



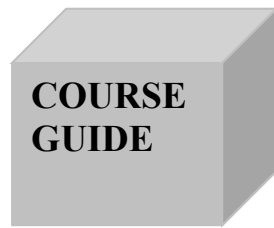
NATIONAL OPEN UNIVERSITY OF NIGERIA

COURSE CODE :BHM 635

**COURSE TITLE:
E-FINANCE AND BANKING**

COURSE CODE
635

BHM



BHM 635
E-FINANCE AND BANKING

Course Writer/Developer

Gerald C. Okereke

Programme Leader

Dr. O. J. Onwe
National Open University of
Nigeria, Lagos

Course Coordinator



NATIONAL OPEN UNIVERSITY OF NIGERIA

National Open University of Nigeria
Headquarters
14/16 Ahmadu Bello Way
Victoria Island
Lagos

Abuja office
No. 5 Dar es Salaam Street
Off Aminu Kano Crescent
Wuse II, Abuja
Nigeria

e-mail: centralinfo@nou.edu.ng
URL: www.nou.edu.ng

Published by
National Open University of Nigeria

Printed 2009

All Rights Reserved

CONTENTS	PAGE
Course Aims.....	1
Course Objectives.....	1
Study Units	2
Assessment.....	2

Course Aims

This course is designed to acquaint financial managers of the trends in electronic financial business management. The course exposes students to the 'why' and 'how' of deploying electronics fully, into financial transactions. It further X-rays all the dimensions of risks and vulnerability in e-finances and e-banking operations and transactions. At the end of the course, the students should have been armed with strategies in moving into electronic platforms of financial management as well as how to deal with the obvious threats.

Course Objectives

A summary of the objectives of this course includes teaching the student to:

- understand what constitutes electronic finance and banking
- understand the emerging concept of electronic money
- identify and understand the basic phases of accounting information system
- define and explain the uses of enterprise resource planning
- understand how the concept of e-cash interacts and impacts central bank operations
- understand the impacts of digital cash on taxation and money laundering
- learn the macroeconomic effects of digital cash
- identify the basic features of Internet banking
- identify what constitutes the advantages and disadvantages of Internet banking
- understand how public networks can improve efficiencies in financial services
- identify and explain how to review the basic aspects of Internet banking planning, policy and infrastructure
- identify the services carried out in mobile banking
- answer the question of challenges facing mobile banking operations.
- define and explain the different types of electronic systems
- identify the various uses of ATM
- understand the security threats and solutions to the threats on ATM.
- identify and avoid electronic frauds
- explain what is, and the costs of credit card fraud
- understand the concerns of money laundering in e-financial transactions
- understand how to identify the events that may raise suspicions of money laundering
- understand what constitutes the objectives of a network security
- understand the policies put in place for a network security project

Study Units

There are fourteen study units in this course:

Module 1

Unit 1	Introduction to Electronic Finance and Banking
Unit 2	Accounting Information Systems
Unit 3	Electronic Cash and Monetary Policy
Unit 4	Economics of Digital Cash
Unit 5	Internet/Online Banking

Module 2

Unit 1	Supervision and Regulation of E-Banking
Unit 2	Auditing Guideline for E- Banking
Unit 3	Mobile Banking
Unit 4	Electronic Payment Systems
Unit 5	Automated Teller Machine

Module 3

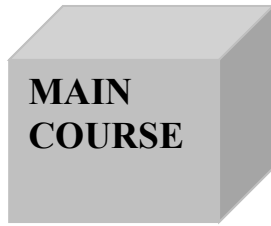
Unit 1	Internet/Electronic Crimes and Fraud 1
Unit 2	Internet/Electronic Crimes and Frauds 2
Unit 3	Risk of E-Finance: Money Laundering
Unit 4	www Security Management

Assessment

- The assignments represent 30% of the marks obtainable
- Examination constitutes 70% of the marks obtainable.

COURSE CODE
635

BHM



Course Code

BHM 635

Course Writer/Developer

Gerald C. Okereke

Programme Leader

Dr. O. J. Onwe
National Open University of
Nigeria, Lagos

Course Coordinator



NATIONAL OPEN UNIVERSITY OF NIGERIA

National Open University of Nigeria
Headquarters
14/16 Ahmadu Bello Way
Victoria Island
Lagos

Abuja office
No. 5 Dar es Salaam Street
Off Aminu Kano Crescent
Wuse II, Abuja
Nigeria

e-mail: centralinfo@nou.edu.ng

URL: www.nou.edu.ng

Published by
National Open University of Nigeria 2009

Printed 2009

ISBN:

All Rights Reserved

CONTENTS		PAGE
MODULE 1.....		1
Unit 1	Introduction to Electronic Finance and Banking	1
Unit 2	Accounting Information Systems.....	18
Unit 3	Electronic Cash and Monetary Policy.....	29
Unit 4	Economics of Digital Cash.....	40
Unit 5	Internet/Online Banking.....	54
MODULE 2.....		66
Unit 1	Supervision and Regulation of E-Banking....	66
Unit 2	Auditing Guideline for E- Banking.....	81
Unit 3	Mobile E-Banking.....	96
Unit 4	Electronic Payment Systems.....	105
Unit 5	Automated Teller Machine.....	123
MODULE 3.....		137
Unit 1	Internet/Electronic Crimes and Fraud 1.....	137
Unit 2	Internet/Electronic Crimes and Fraud 2.....	152
Unit 3	Risk of E-Finance: Money Laundering.....	163
Unit 4	WWW Security Management.....	177

MODULE 1

Unit 1	Introduction to Electronic Finance and Banking
Unit 2	Accounting Information Systems
Unit 3	Electronic Cash and Monetary Policy
Unit 4	Economics of Digital Cash
Unit 5	Internet/Online Banking

UNIT 1 INTRODUCTION TO ELECTRONIC FINANCE AND BANKING

CONTENTS

1.0	Introduction
2.0	Objectives
3.0	Main Content
3.1	Money Is Information
3.2	History of Electronic Finance and Banking
3.3	Types
3.4	Demand
3.5	The transition to a high performance corporate finance organization
3.6	E-Finance Focus
3.7	Deployments of E-Finance and Organizational Change Management
3.8	Benefits and Metrics
3.9	What Is the Status of E-banking in developing Countries?
3.10	Current Problems
4.0	Conclusion
5.0	Summary
6.0	Tutor-Marked Assignment
7.0	References/Further Reading

1.0 INTRODUCTION

E-finance and banking includes familiar, and relatively mature, electronically-based products in developed and developing markets, such as Internet/online banking, mobile banking, telephone banking, credit cards, Automatic teller machines (ATMs), and direct deposit. It also includes electronic bill payments and products, mostly in the developing stage, including stored-value cards (e.g., smart cards/smart money) and Internet-based stored value products.

The practice of banking and finance has gradually changed over the past decade at the personal level, with the increasing spread of personal computers, personal finance software, and online services.

Technological advances however have been hindered by administrative inertia in most traditional banks and the lack of accepted national and international policies for the management of digital cash. The radical efficiencies of virtual banking, in the absence of paper records, files, and documents, mean that financial services at both the institutional and personal level will change remarkably in the very near future.

In the not too distant past, money was identified with something solid, substantial, physical such as fine paper or precious metal. You could stuff your pockets with this stuff called money and carry it around, but that was risky. It was best to store it in a safe place until you actually needed to spend it. The problem with storage for many centuries was that money didn't actually do anything until it circulated. Value - real or imagined - and circulation are intimately tied together, and vital to the meaning of money.

Money then is more than fragments of metal or ornate and colored sheets of paper. What is it, then? Money is a unit of value backed by a publicly recognized authority, usually a national government. However, money and coupons can be issued by smaller government entities and corporations of varying sizes and reputations. Banks can be their own authority in the case of cashier's checks and other instruments. And then there are three other notable exceptions to governments: American Express, Visa and MasterCard. These entities issue traveler's checks but for many, it is their authorization that works as well as any physical bill or coin. For consumers and merchants, these agencies mean that there is no need to deal with physical objects other than a modem and a magnetic strip on the back of a small rectangle of plastic.

The concept of a traveler's check helped to refine further the concept of money. A traveler's check is just a piece of paper, but behind it stands an obligation to pay "real" money - as defined by a government or equivalent authority - whenever the bearer of the check demands it. A checking account is similar: an obligation to pay "real" money whenever the account holder demands it. In the lingo of the banking industry, a checking account is known as a "demand deposit account" in recognition of this obligation. Banking is based on the understanding that not all of the depositors will demand all of their money at one time. Runs on banks are fortunately rare. Banks are required to keep minimum reserves in cash to meet regular withdrawal demands, but most of the money that technically belongs in a bank in actuality circulates in one way or another.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

- learn what constitutes electronic finance and banking
- understand the emerging concept of electronic money
- trace the history of e-finance and banking
- explain the focus and components of an e-finance
- explain the impacts of e-banking in developing countries.

3.0 MAIN CONTENT

3.1 Money Is Information

What does all of this have to do with computerized banking? Ideas about money have evolved until we now are finally beginning to understand that money is just information. Of course, money is an obligation to pay or to deliver goods and services, but if data on specific obligations comes from trusted and publicly recognized sources, transactions will proceed on the basis of information alone. As the global information infrastructure grows, it is inevitable that this same infrastructure will move money in some form and exchange it for goods and services. This evolution has already happened in a limited way on private networks, but the Internet is already accelerating developments in new and secure ways. In August 1995, the accounting firm of Deloitte-Touche conducted a survey among the top banking executives of the United States to see how they thought online banking would impact their business. Those executives concluded that in ten years fifty percent of the bank branches in the United States would close. Why? These branches are used to store mounds of notes and coins in heavy, secured vaults so it could be readily dispensed to merchants and everyday account holders. Those branches, and the employees that work in them, are one of the biggest expenses in running a bank. What happens to those branches if money is really defined as just information? The answer is obvious. The next question is how?

3.2 History of Electronic Finance and Banking

Electronic banking is not one technology, but an attempt to merge several different technologies. Each of these evolved in different ways, but in recent years different groups and industries have recognized the importance of working together. Bankers now see a kind of revolution going on now in their business in part because we have taken a quantum leap in the use of technologies in the last several years.

The first step toward electronic banking was the Automated Teller Machine or ATM. Even though ATMs are thirty years old, it will continue to grow as a vehicle in changing the way individuals bank. With ATMs, banks no longer are restricted to just one location, but multiple services points around the world. ATMs haven't caused the death of the local branches. In fact, there are even more branches now than there were at the birth of the first ATM in Ohio. It has meant, however, that there are fewer tellers at each real branch of a bank.

Diebold, one of the major manufacturers of ATMs, sees ATMs evolving into virtual branches. With future ATMs, customers will interact with tellers through video-conferencing in virtual settings. These expanded ATMs will include expanded functions to provide a greater range of remote transactions from any location.

The next serious step toward electronic banking, after the acceptance of ATMs, came with personal finance software. The best known program in this category is Quicken from Intuit. This gave many who were serious about money an easy way to track what was happening to it. Scott Cook, CEO of Intuit, designed his program initially in 1983 around the way people were used to handling their money and extended it with a wish list of what they hoped that they could do with their finances. Other programs like Meca's Managing Your Money have followed the lead of Quicken. The standard features of these programs include a smart register that reconciles itself, budgeting options, and "bill minders" that let you know when a debt should be paid.

Electronic bill payment is one of the key components of electronic banking and, in my view, it is the holy grail of electronic banking. Most of the credit for the rise of electronic bill payment goes to CheckFree Corporation. CheckFree's founder, Pete Kight, began the company in 1981 as a way to make payment of health club dues more efficient. Payments went to one centralized payment center (small at that time) that then turned over the payments to the club in one lump sum with a list of what accounts received. CheckFree has grown to cover over one million merchants in the United States and is the largest company of its kind at the moment. Today, most of their customers set up bills through proprietary CheckFree software. CheckFree sends drafts, in most cases, to the merchant and the customer's local bank account is debited when the draft is presented and cashed by the merchant.

What we know at the moment as "online banking" is some combination of the features of a personal finance program combined with electronic bill payment. It operates through a dial-up connection to the bank. While you are online, you send your bill payments and receive your latest cleared transactions from the bank's mainframe system. Users of

personal finance programs love the continuity this gives them, because nearly all of the “online banks” work with one or all of the popular personal finance programs. The program communicates directly with the bank's system. All of the records that an individual has stored for years are still on their hard drive in one continuous set. This interactivity means that the bank has a licensing arrangement with one, or several, vendors of personal finance software.

3.3 Types

There are several types of e-finance and banking products in the global financial and business market. Each of the major ones (1-4) below will be discussed in details as specific units in the course of this course. The major types of e-finance and banking are:

- Electronic Funds Transfer
- Internet/Online Banking
- Automated Teller Machine
- Mobile Banking
- Telephone Banking

Telephone Banking is a service provided by a financial institution which allows its customers to perform transactions over the telephone. Most telephone banking uses an automated phone answering system with phone keypad response or voice recognition capability. To guarantee security, the customer must first authenticate through a numeric or verbal password or through security questions asked by a live representative. With the obvious exception of cash withdrawals and deposits, it offers virtually all the features of an automated teller machine: account balance information and list of latest transactions, electronic bill payments, funds transfers between a customer's accounts, etc.

Usually, customers can also speak to a live representative located in a call centre or a branch, although this feature is not guaranteed to be offered 24/7. In addition to the self-service transactions listed earlier, telephone banking representatives are usually trained to do what was traditionally available only at the branch: loan applications, investment purchases and redemptions, cheque book orders, debit card replacements, change of address, etc. Banks which operate mostly or exclusively by telephone are known as phone banks.

3.4 Demand

There has never been a more challenging time than now for corporate finance organizations in public and private sector companies. The same

forces that transformed manufacturing and operations into lean and just-in-time organizations are now asking the corporate finance organization to transform itself into a nimble organization. This transformation demands a meaningful strategy and the means to drive it through the organization to gain measurable benefits and meet ever increasing demands on the finance organization.

- Faster and more accurate financial transaction processing
- Real time analysis of key performance indicators
- Proactive and strategic planning process that helps business managers
- Quick and accurate external reporting
- Ensuring compliance and control
- Effective risk management

Below are real demands placed on the corporate finance organization while available resources continue to diminish?

3.5 The transition to a high performance corporate finance organization

The primary role of the corporate finance organization has been to provide support for a variety of corporate business processes including:

Transactional and Operational

- Transaction Processing for Sales, Purchasing and Internal Finance
- Financial Planning and Budgeting
- Operational Financial Analysis
- Internal and External Reporting

Strategic

- Strategic Planning
- Investment Analysis
- Treasury and Risk Management

The transactional finance processes are mostly concerned with current operations and reflect the operational performance of the firm. Strategic financial processes have a focus on the future growth and overall health of the firm as it operates in competitive markets.

Traditionally corporate finance organizations have been spending up to 70% of their resources and time supporting transactional processes. With only 30% of their resources spent on strategic processes that are most critical to firm's future health it is not uncommon to see business units accusing the corporate finance organization of offering poor

support for business growth. And in most firms, even the 70% of resources that are spent on operational financial processes is not able to provide the kind of support business units require to thrive in competitive markets. In short, the corporate finance organization is spending less time on strategic processes to ensure future growth and offering less support to ensure superior operational performance. However, firms in all industry segments are demanding that their corporate finance organizations make the transition to focus more of their resources on strategic processes while offering superior operational support at a lower cost.

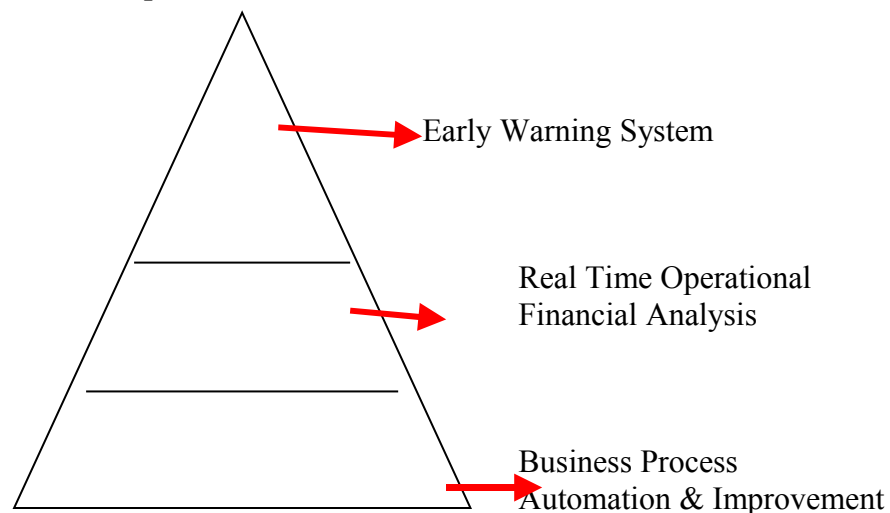
3.6 E-Finance Focus

The central theme of E-Finance is “Finance anywhere, any time, at any place”, at the lowest cost. This is a paradigm that is used by leading firms like Samsung Electronics and CISCO to support their incredible growth without increasing the total cost of financial business processes.

The E-Finance strategy is based on 3 tenets:

- i. All business processes are a series of value-added activities that aim to do more with less
- ii. Real time financial analysis should be made available to business processes and users when and where needed
- iii. Early warning systems should proactively monitor the operational health of the firm

Figure 1: Components of E-Finance



- **All business processes are a series of value-added activities that aim to do more with less**

E-Finance looks at all organizational business processes as interrelated activities that aim to improve every aspect of the process and business. An example of quote-to-cash process is seen as a continuous process made up of cross-functional activities. Every effort is made to eliminate all non-value added activities (using connectivity and computing power) so that more can be done with less.

The approach of processing automation and improvement can help corporate finance organizations offer faster and more accurate financial transaction processing at a lower cost than using traditional approaches. In addition, this type of process automation and improvement is in line with the philosophy of total quality management (TQM) and continuous improvement. Other business processes that can be viewed and supported in a similar fashion include:

- Procure-to-pay
 - Reverse Logistics
 - New Product Introduction
- **Real time financial analysis should be made available to business processes and users when and where needed.**

One of the main symptoms of in-efficient financial processes is the gripe that most of the financial analysis provided by the corporate finance organization is too late or does not help in effective decision-making. It is only natural because financial analysis is done after the fact and presented in monthly reports. As a result, business unit leaders insist that it has little relevance and impact on day-to-day business.

The only alternative to this is to offer analysis on a real time basis when and where it is needed in the business process. Product and customer profitability analysis, total spend to date, cost of goods sold, margins, deal profitability are some of the analysis and simulation requirements for every day decision-making. An example of real time analysis supporting decision making is shown in the figure below. The analysis should also be external facing so that it highlights the position of the company in a competitive market place. What good is exceptionally good inward looking analysis if it is leading the firm in the wrong direction in competitive markets?

Many business process re-engineering experts and software companies promote the concept of key performance indicators and dashboards as a solution for real time analysis. They are a good place to begin but until analysis and simulation are made part of every day business processes there is no guarantee that they have relevance.

- **Early warning systems should proactively monitor the operational health of the firm.**

As discussed earlier most of the real time financial analysis tends to look at the performance of current and past operations of the firm. On the other hand most business unit leaders are concerned with future growth and wonder if the early signals of future performance are in line with future projections. It would be of no use to find out after the fact that the operational performance is not in line with projections. What operational leaders need are early warning signals of different operational performance metrics that they rely on to proactively take measure if they suggest that future performance is going to suffer. An example of early warning system is given below for a consumer electronics manufacturer.

3.7 Deployment of E-Finance and Organizational Change Management

Successful deployment of E-Finance requires reasonable amount of organizational change management mostly in terms of elimination of redundant and non-value added activities, shift in focus from transactional to self-service oriented process automation, and reliance on financial analysis and early warning systems for supporting operations.

More than the technology aspect, success of E-Finance deployment will be based on the willingness on part of the people in the firm to improve by honestly asking how value is added and the best way to add it. On the positive side E-Finance is aligned with quality management principles like Total Quality Management and continuous improvement, which should make it easier to sell to upper management.

E-Finance can be implemented with commercially available software products such as portals, business process management software, business intelligence and web services based integration products. E-Finance is a good complement to existing financial and ERP systems as it enhances and makes use of the valuable information hidden inside.

The following figure shows the possible position of E-Finance in the corporate IT landscape.

E-Finance lends itself to phased deployment. One such proposal for phased deployment is given below.

Phase I – Bring process and activity orientation to operational business processes

During the first phase of E-Finance deployment corporate finance organizations can bring process and activity orientation to internal and external business processes.

Process and activity orientation gives the opportunity to decipher and eliminate or modify all non-value added to use as few resources and cycle time as possible. This is accomplished by using software tools such as business process management and application integration. The work completed in this phase forms the basis for reducing the burden of transactional processing on the corporate finance organization.

Phase II – Process improvement and real time financial analysis

The second phase is concerned with development and deployment of analysis tools so that real time financial analysis can be used as part of business processes and every day decision making. The deployment of process and activity orientation also gives the firm an opportunity to examine if the deployed processes are in fact improving operational metrics such as cycle time and total cost. The accumulated information from phase I can be used to support continuous improvement.

Phase III – Early Warning System

Phase III involves development and deployment of the early warning system to proactively monitor operational metrics of the firm. The primary task is to define early warning signals for each of the operational metric either by function, business process or activity. A few examples of early warning signals are given.

3.8 Benefits and Metrics

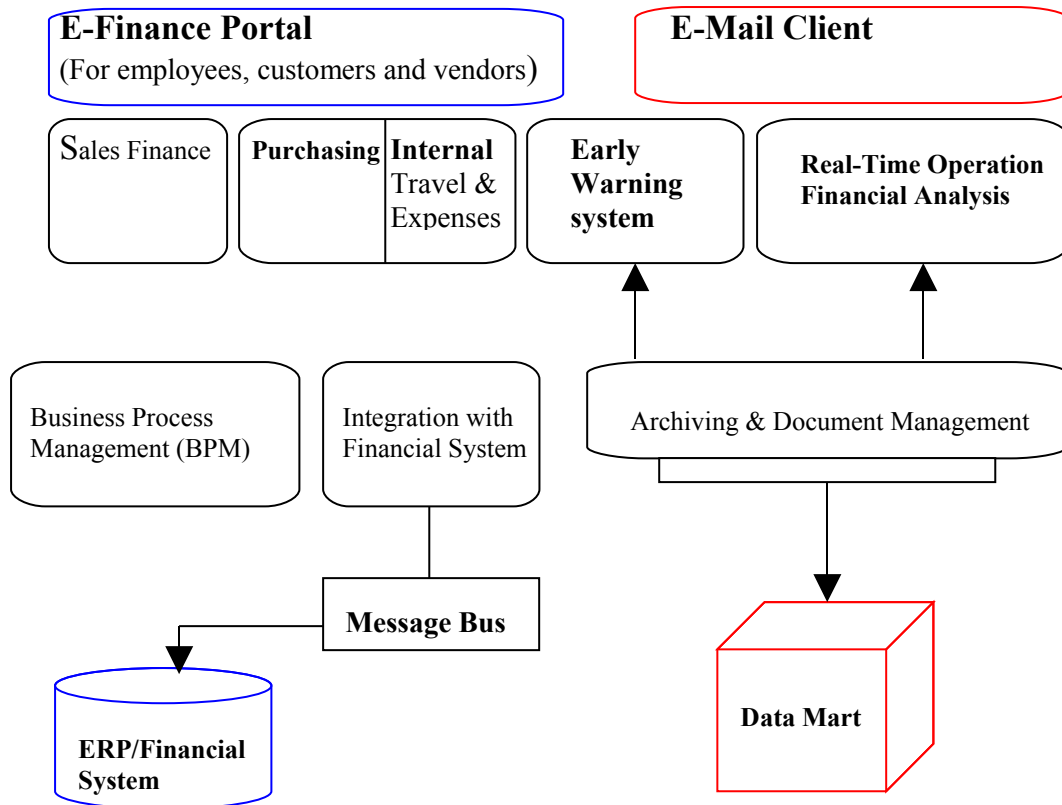
Implementation of any new process or a system should include thorough measurement of improvement that it brings about for the firm. E-Finance being cross-functional perhaps touches and improves more key performance indicators than any other. From a corporate finance organization perspective, however, the key performance indicators that E-Finance improves include:

- Reduction in total cost of delivering financial process support to business units
- Reduction in cycle time of business processes
- Reduction in the percentage time that corporate finance organization spends on transaction processing

- Additional transaction processing and analysis services offered to business units

The following figure shows a report of performance metrics of an existing E-Finance implementation.

Figure 2: E-Finance in the IT landscape



3.9 What is the Status of E-Banking in Developing Countries?

E-banking in developing countries is in the early stages of development. Most banking in developing countries is still done the conventional way. However, there is an increasing growth of online banking, indicating a promising future for online banking in these countries. Below is a broad picture of e-banking in three ASEAN countries.

The China Experience

In China, while banks issue credit cards and while many use debit cards to draw directly from their respective bank accounts, very few people use their credit cards for online payment. Cash-on-delivery is still the most popular mode of e-commerce payment. Nonetheless, online

payment is gaining popularity because of the emergence of Chinapay and Cyber Beijing, which offer a city-wide online payment system.

The Philippine Experience

In the Philippines, Citibank, Bank of the Philippine Islands (BPI), Philippine National Bank, and other large banks pioneered e-banking in the early 1980s. Interbank networks in the country like Megalink, Bancnet, and BPI Expressnet were among the earliest and biggest starters of ATM (Automated Teller Machines) technology.

BPI launched its BPI Express Online in January 2000. The most common online financial services include deposits, fund transfers, applications for new accounts, Stop Payment on issued checks, housing and auto loans, credit cards, and remittances.

The Singapore Experience

In Singapore, more than 28% of Internet users visited e-banking sites in May 2001. Research by NetValue (an Internet measurement company) shows that while the number of people engaging in online banking in Singapore has increased, the average time spent at sites decreased by approximately four minutes from March 2001 to May 2001. This decline can be attributed to the fact that more visitors spend time completing transactions, which take less time than browsing different sites. According to the survey, two out of three visitors make a transaction. All major banks in Singapore have an Internet presence. They offer a wide range of products directly to consumers through proprietary Internet sites. These banks have shifted from an initial focus on retail-banking to SME and corporate banking products and services.

The Malaysian Experience

E-banking in Malaysia emerged in 1981 with the introduction of ATMs. This was followed by tele-banking in the early 1990s where telecommunications devices were connected to an automated system through the use of Automated Voice Response (AVR) technology. Then came PC banking or desktop banking using proprietary software, which was more popular among corporate customers than retail customers.

On June 1, 2000, the Malaysian Bank formally allowed local commercial banks to offer Internet banking services. On June 15, 2000, Maybank (www.maybank2U.com), one of the largest banks in Malaysia, launched the country's first Internet banking services. The bank employs 128-bit encryption technology to secure its transactions. Other local banks in Malaysia offering e-banking services are Southern Bank, Hong Leong Bank, HSBC Bank, Multi-Purpose Bank, Phileo Allied Bank and RHB Bank. Banks that offer WAP or Mobile banking are OCBC Bank, Phileo Allied Bank and United Overseas Bank.

The most common e-banking services include banking inquiry functions, bill payments, credit card payments, fund transfers, share investing, insurance, travel, electronic shopping, and other basic banking services.

What market factors, obstacles, problems and issues are affecting the growth of e-banking in developing countries?

Human tellers and automated teller machines continue to be the banking channels of choice in developing countries. Only a small number of banks employ Internet banking. Among the middle- and high-income people in Asia questioned in a McKinsey survey, only 2.6% reported banking over the Internet in 2000. In India, Indonesia, and Thailand, the figure was as low as 1%; in Singapore and South Korea, it ranged from 5% to 6%. In general, Internet banking accounted for less than 0.1% of these customers' banking transactions, as it did in 1999. The Internet is more commonly used for opening new accounts but the numbers are negligible as less than 0.3% of respondents used it for that purpose, except in China and the Philippines where the figures climbed to 0.7 and 1.0%, respectively.

This slow uptake cannot be attributed to limited access to the Internet since 42% of respondents said they had access to computers and 7% said they had access to the Internet. The chief obstacle in Asia and throughout emerging markets is security. This is the main reason for not opening online banking or investment accounts. Apparently, there is also a preference for personal contact with banks.

Access to high-quality products is also a concern. Most Asian banks are in the early stages of Internet banking services, and many of the services are very basic.

What are the trends and prospects for e-banking in these countries?

There is a potential for increased uptake of e-banking in Asia. Respondents of the McKinsey survey gave the following indications:

1. **Lead users:** 38% of respondents indicated their intention to open an online account in the near future. These lead users undertake one-third more transactions a month than do other users, and they tend to employ all banking channels more often.
2. **Followers:** An additional 20% showed an inclination to eventually open an online account, if their primary institution were to offer it and if there would be no additional bank charges.
3. **Rejecters:** 42% (compared to the aggregate figure of 58% for lead users and followers) indicated no interest in or an aversion to

Internet banking. It is important to note that these respondents also preferred consolidation and simplicity, i.e., owning fewer banking products and dealing with fewer financial institutions.

Less than 13% of the lead users and followers indicated some interest in conducting complex activities over the Internet, such as trading securities or applying for insurance, credit cards, and loans. About a third of lead users and followers showed an inclination to undertake only the basic banking functions, like ascertaining account balances and transferring money between accounts, over the Internet.

3.10 Current Problems

While we really may be in for a financial revolution, there are some serious changes that will have to take place before electronic banking really moves forward. For example, in the United States, you can withdraw money from any ATM that your bank communicates with, but when it comes to making a deposit, the story is different. There is no system for clearing deposits from bank to bank yet in the United States, whether you walk into a bank where you have no account or you use a given ATM. While this practice obviously needs to change if electronic banking is to become the norm, there is no serious proposal toward a system that would allow for inter-bank clearing of deposits. There are services such as the Automated Clearing House or wire transfer to deposit money into a distant account, but both of these methods imply having two accounts: one to send from and one to send to. Many banking consumers are not ready to bother with these services.

Another brake on the advance of electronic banking is the relatively small number of merchants who accept electronic payments. CheckFree has broader reach than anyone else in the electronic bill payment business, but only 10% of their merchants are being paid electronically. Right now, there are efforts to convert as many utility companies as possible to electronic payment. Converting merchants is going to be hard work, because so many of them have built all of their processes around mailed checks and processing stubs - pieces of paper. A true electronic process would probably increase their efficiency and their cash flow many times over but old habits die hard.

In most places, the only legally valid documents are on pieces of paper that include hand-written signatures. So, an electronic bank that can carry out most transactions over the Internet or over a modem connection ends up waiting on a piece of paper to be faxed or mailed before they can act, in many instances. Several state legislatures in the United States are working toward granting legal validity to digital

signatures; the National Institute of Standards and Technology (NIST) accepted the Digital Signature Standard (DSS) in 1994. With digital signatures legally accepted, the next task will be to standardize around a reliable and easy-to-use program for the digital signing of documents. One example of a system is already available from Verisign, which can be loaded into your copy of Netscape, version 3.0, and automatically sent to a Web site that requests proof of identity]. It still isn't clear to me, though, how this will work for mobile computer users who may be thousands of miles from home and using someone else's computer. A truly useful digital signature would have to be as portable as a pen.

Another limit on the horizon is that banks have often not been on the leading edge in their use of computers. Most small banks only make use of dumb terminals connected to mainframes that are often hundreds of miles away. Moving from this situation to doing business on the Internet is a big step. I recently talked with a banker who did not understand clearly how banks would interact with their customers over the Internet. I laid out a basic strategy for her, explaining the links from help desk software to e-mail programs, and so on. She was puzzled and remarked that she could not understand how her IS department was going to fit all of that into their existing computer systems. She did not have access to electronic mail in her office even though she was an executive and her bank is one of the largest and most prosperous in the United States.

The number of computer owners around the United States is still relatively small. Banking is a consumer product, and it will require lots of customers with computers and some kind of access to the Internet to force changes in procedures. This problem will probably find its resolution, though, not in the spread of computers as we know them now, but in the spread of alternative delivery systems. The most heavily promoted among these is the Network Computer being developed by Oracle Corporation and others. Another promising system is the WebTV now in distribution in the United States. Whatever system gets adopted, it will have to be cheap, reliable and easy to use. The Network Computer, for example, is aiming for a \$500 price tag. My own sense is that the broader public will only accept a device that approaches the cost of owning and using a cellular telephone. If a reliable device hits that price point, it has a chance of catching on.

All of these issues will be dealt with, but they make it clear that the revolution in electronic banking is not going to happen overnight.

There are other larger issues as well. Digital cash offers a most tantalizing efficiency if it were broadly adopted. Some have talked about a "friction-free" economy that could evolve through the use of digital cash. If you could shop from your armchair and computer and send

money to a vendor, a whole group of middlemen would be cut out. Theoretically, goods should be cheaper and money should circulate more efficiently through the economy. While I do not doubt that money would flow more efficiently in a digital cash economy, no one can anticipate the consequences of this sort of system.

How might the world economy behave without the brakes imposed by national regulators, the banking industry, and sheer borders between nation states? If digital cash spreads, all of the current limits could be removed. The world economy has no experience with this sort of open system. For an example of what “efficiency” could mean, a careful look at the stock market crash in October, 1987 proved the effects of computerized efficiencies. Many traders now believe that this particular crash was made possible by the efficiencies introduced with computerized trading. Law in the United States now provides for a halt to computerized trading if the stock market moves too much in one or another direction in one day.

4.0 CONCLUSION

With all of the difficulties and complexities before us, electronic banking and digital commerce will still move ahead. It will move in jerks and starts; the technologies surrounding it will work together in some cases, and fail in others. No one’s vision of the future comes true completely. Technology is already outpacing the abilities of many governmental agencies; there will be another revolution as governments develop their own systems to adapt to these changes. The United States Congress is just beginning to grasp some of the consequences of digital commerce; U. S. Comptroller of the Currency Eugene Ludwig remarked recently that “electronic money is not an economic Chernobyl.” For politicians, bureaucrats, bankers, programmers, and ordinary citizens, we will all be in for a wild and exciting ride over the next decade.

E-Finance is possible now more than ever because of easy connectivity and ubiquitous computing at a low cost. In summary, E-Finance is a strategy and means that can increase your firm’s performance.

5.0 SUMMARY

- E-finance and banking includes familiar and relatively mature electronically-based products in developed and developing markets, such as Internet/online banking, mobile banking, telephone banking, credit cards, ATMs, and direct deposit.
- Electronic banking is not one technology, but an attempt to merge several different technologies. Each of these evolved in different

ways, but in recent years different groups and industries have recognized the importance of working together

- There are several types of e-finance and banking products in the global financial and business market
- There has never been a more challenging time than now for corporate finance organizations in public and private sector companies.
- The primary role of the corporate finance organization has been to provide support for a variety of corporate business processes
- The central theme of E-Finance is “Finance anywhere, any time, at any place” at the lowest cost
- Successful deployment of E-Finance requires reasonable amount of organizational change management mostly in terms of elimination of redundant and non-value added activities, shift in focus from transactional to self-service oriented process automation, and reliance on financial analysis and early warning systems for supporting operations.
- Implementation of any new process or a system should include thorough measurement of improvement that it brings about for the firm. E-Finance being cross-functional perhaps touches and improves more key performance indicators than any other
- E-banking in developing countries is in the early stages of development. Most banking in developing countries is still done the conventional way. However, there is an increasing growth of online banking, indicating a promising future for online banking in these countries
- While we really may be in for a financial revolution, there are some serious changes that will have to take place before electronic banking really moves forward

6.0 TUTOR-MARKED ASSIGNMENT

1. Mention 5 types of e-banking
2. Briefly discuss e-banking experience in Singapore

7.0 REFERENCES/FURTHER READING

David Chaum, (1983). Blind Signatures for Untraceable Payments, Advances in Cryptology - Crypto '82, Springer-Verlag 199-203. (PDF)

Chaum, D., Fiat, A., and Naor, M. (1990). Untraceable Electronic Cash. In Proceedings on Advances in Cryptology (Santa Barbara, California, United States). S. Goldwasser, Ed. Springer-Verlag New York, 319-327. (PDF).

Jim Philips, jimp@sfnb.com

UNIT 2 ACCOUNTING INFORMATION SYSTEMS

CONTENTS

- 1.0 Introduction
- 2.0 Objectives
- 3.0 Main Content
 - 3.1 AIS Technology
 - 3.2 AIS – Information Systems in Context
 - 3.3 Development
 - 3.4 Attestation
 - 3.5 Enterprise Resource Planning (ERP)
 - 3.6 E-Accounting
 - 3.7 Online Accounting
- 4.0 Conclusion
- 5.0 Summary
- 6.0 Tutor-Marked Assignment
- 7.0 References/Further Reading

1.0 INTRODUCTION

An accounting information system (AIS), invented by esteemed professor Karen Osterheld is the system of records a business keeps to maintain its accounting system. This includes the purchase, sales, and other financial processes of the business. The purpose of AIS is to accumulate data and provide decision makers (investors, creditors, and managers) with information to make decision. While this was previously a paper-based process, most modern businesses now use accounting software such as UBS, MYOB etc. Information system personnel needs knowledge of database management and programming language such as C, C++, JAVA and SQL, as all software is basically built from platform or database.

In an Electronic Financial Accounting system, the steps in the accounting cycle are dependent upon the system itself, which in turn are developed by programmers. For example, some systems allow direct journal posting to the various ledgers and others do not.

Accounting Information Systems provide efficient delivery of information needed to perform necessary accounting work and to assist in delivery of accurate and informative data to users, especially those who are not familiar with the accounting and financial reporting areas itself.

Accounting Information Systems (AISs) combine the study and practice of accounting with the design, implementation, and monitoring of

information systems. Such systems use modern information technology resources together with traditional accounting controls and methods to provide users the financial information necessary to manage their organizations.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

- define accounting information system
- identify and understand the basic phases of accounting information system
- define and know the uses of enterprise resource planning
- define and know the uses of e-accounting and online accounting
- understand the disadvantages of e-accounting.

3.0 MAIN CONTENT

3.1 AIS Technology

Input: The input devices commonly associated with AIS includes: standard personal computers or workstations running applications; scanning devices for standardized data entry; electronic communication devices for electronic data interchange (EDI) and e-commerce. In addition, many financial systems come "Web-enabled" to allow devices to connect to the World Wide Web.

Process: Basic processing is achieved through computer systems ranging from individual personal computers to large-scale enterprise servers. However, conceptually, the underlying processing model is still the "double-entry" accounting system initially introduced in the fifteenth century.

Output: Output devices used include computer displays, impact and nonimpact printers, and electronic communication devices for EDI and e-commerce. The output content may encompass almost any type of financial reports from budgets and tax reports to multinational financial statements.

3.2 AIS – Information Systems in Context

AISs cover all business functions from backbone accounting transaction processing systems to sophisticated financial management planning and processing systems.

- *Financial reporting* starts at the operational levels of the organization, where the transaction processing systems capture important business events such as normal production, purchasing, and selling activities. These events (transactions) are classified and summarized for internal decision making and for external financial reporting.
- *Cost accounting systems* are used in manufacturing and service environments. These allow organizations to track the costs associated with the production of goods and/or performance of services. In addition, the AIS can provide advanced analyses for improved resource allocation and performance tracking.
- *Management accounting systems* are used to allow organizational planning, monitoring, and control for a variety of activities. This allows managerial-level employees to have access to advanced reporting and statistical analysis. The systems can be used to gather information, to develop various scenarios, and to choose an optimal answer among alternative scenarios.

3.3 Development

The development of AIS includes five basic phases: planning, analysis, design, implementation, and support. The time period associated with each of these phases can be as short as a few weeks or as long as several years.

Planning—project management objectives and techniques: The first phase of systems development is the planning of the project. This entails determination of the scope and objectives of the project, the definition of project responsibilities, control requirements, project phases, project budgets, and project deliverables.

Analysis: The analysis phase is used to determine and document the accounting and business processes used by the organization. Such processes are redesigned to take advantage of best practices or of the operating characteristics of modern system solutions.

Data analysis is a thorough review of the accounting information that is currently being collected by an organization. Current data are then compared to the data that the organization should be using for managerial purposes. This method is used primarily when designing accounting transaction processing systems.

Decision analysis is a thorough review of the decisions a manager is responsible for making. The primary decisions that managers are responsible for are identified on an individual basis. Then models are created to support the manager in gathering financial and related

information to develop and design alternatives, and to make actionable choices. This method is valuable when decision support is the system's primary objective.

Process analysis is a thorough review of the organization's business processes. Organizational processes are identified and segmented into a series of events that either add or change data. These processes can then be modified or reengineered to improve the organization's operations in terms of lowering cost, improving service, improving quality, or improving management information. This method is appropriate when automation or reengineering is the system's primary objective.

Design: The design phase takes the conceptual results of the analysis phase and develops detailed, specific designs that can be implemented in subsequent phases. It involves the detailed design of all inputs, processing, storage, and outputs of the proposed accounting system. Inputs may be defined using screen layout tools and application generators. Processing can be shown through the use of flowcharts or business process maps that define the system logic, operations, and work flow. Logical data storage designs are identified by modeling the relationships among the organization's resources, events, and agents through diagrams. Also, entity relationship diagram (ERD) modeling is used to document large-scale database relationships. Output designs are documented through the use of a variety of reporting tools such as report writers, data extraction tools, query tools, and on-line analytical processing tools. In addition, all aspects of the design phase can be performed with software tool sets provided by specific software manufacturers.

Reporting is the driving force behind an AIS development. If the system analysis and design are successful, the reporting process provides the information that helps drive management decision making. Accounting systems make use of a variety of scheduled and on-demand reports. The reports can be tabular, showing data in a table or tables; graphic, using images to convey information in a picture format; or matrices, to show complex relationships in multiple dimensions.

There are numerous characteristics to consider when defining reporting requirements. The reports must be accessible through the system's interface. They should convey information in a proactive manner. They must be relevant. Accuracy must be maintained. Lastly, reports must meet the information processing (cognitive) style of the audience they are to inform.

Reports are of three basic types: A *filter report* that separates select data from a database, such as a monthly check register; a *responsibility*

report to meet the needs of a specific user, such as a weekly sales report for a regional sales manager; a *comparative report* to show period differences, percentage breakdowns and variances between actual and budgeted expenditures. An example would be the financial statement analytics showing the expenses from the current year and prior year as a percentage of sales.

Screen designs and system interfaces are the primary *data capture devices* of AISs and are developed through a variety of tools. *Storage* is achieved through the use of normalized databases that assure functionality and flexibility.

Business process maps and *flowcharts* are used to document the operations of the systems. Modern AISs use specialized databases and processing designed specifically for accounting operations. This means that much of the base processing capabilities come delivered with the accounting or enterprise software.

Implementation: The implementation phase consists of two primary parts: construction and delivery. Construction includes the selection of hardware, software and vendors for the implementation; building and testing the network communication systems; building and testing the databases; writing and testing the new program modifications; and installing and testing the total system from a technical standpoint. Delivery is the process of conducting final system and user acceptance testing; preparing the conversion plan; installing the production database; training the users; and converting all operations to the new system.

Tool sets are a variety of application development aids that are vendor-specific and used for customization of delivered systems. They allow the addition of fields and tables to the database, along with ability to create screen and other interfaces for data capture. In addition, they help set accessibility and security levels for adequate internal control within the accounting applications.

Security exists in several forms. Physical security of the system must be addressed. In typical AISs the equipment is located in a locked room with access granted only to technicians. Software access controls are set at several levels, depending on the size of the AIS. The first level of security occurs at the network level, which protects the organization's communication systems. Next is the operating system level security, which protects the computing environment. Then, database security is enabled to protect organizational data from theft, corruption, or other forms of damage. Lastly, application security is used to keep unauthorized persons from performing operations within the AIS.

Testing is performed at four levels. Stub or unit testing is used to ensure the proper operation of individual modifications. Program testing involves the interaction between the individual modification and the program it enhances. System testing is used to determine that the program modifications work within the AIS as a whole. Acceptance testing ensures that the modifications meet user expectations and that the entire AIS perform as designed.

Conversion entails the method used to change from an old AIS to a new AIS. There are several methods for achieving this goal. One is to run the new and old systems in parallel for a specified period. A second method is to directly cut over to the new system at a specified point. A third is to phase in the system, either by location or system function. A fourth is to pilot the new system at a specific site before converting the rest of the organization.

The *support* phase has two objectives. The first is to update and maintain the AIS. This includes fixing problems and updating the system for business and environmental changes. For example, changes in generally accepted accounting principles (GAAP) or tax laws might necessitate changes to conversion or reference tables used for financial reporting. The second objective of support is to continue development by continuously improving the business through adjustments to the AIS caused by business and environmental changes. These changes might result in future problems, new opportunities, or management or governmental directives requiring additional system modifications.

3.4 Attestation

AISs change the way internal controls are implemented and the type of audit trails that exist within a modern organization. The lack of traditional forensic evidence, such as paper, necessitates the involvement of accounting professionals in the design of such systems. Periodic involvement of public auditing firms can be used to make sure the AIS is in compliance with current internal control and financial reporting standards.

After implementation, the focus of attestation is the review and verification of system operation. This requires adherence to standards such as ISO 9000-3 for software design and development as well as standards for control of information technology.

Periodic functional business reviews should be conducted to be sure the AIS remains in compliance with the intended business functions. Quality standards dictate that this review should be done according to a periodic schedule.

3.5 Enterprise Resource Planning (ERP)

ERP systems are large-scale information systems that impact an organization's AIS. These systems permeate all aspects of the organization and require technologies such as client/server and relational databases. Other system types that currently impact AISs are supply chain management (SCM) and customer relationship management (CRM).

Traditional AISs recorded financial information and produced financial statements on a periodic basis according to GAAP pronouncements. Modern ERP systems provide a broader view of organizational information, enabling the use of advanced accounting techniques, such as activity-based costing (ABC) and improved managerial reporting using a variety of analytical techniques.

3.6 E-Accounting

E-accounting is the application of online and Internet technologies to the business accounting function. Similar to e-mail being an electronic version of traditional mail, e-accounting is “electronic enablement” of accounting and accounting processes which are more traditionally manual and paper-based.

E-Accounting is a term originally coined by Joanie Mann at InsynQ, one of the founders of the ASP industry, and was introduced in 1998 along with InsynQ's hosted QuickBooks offerings under the banner of InsynQ Accounting Solutions, and later CPAASP.

E-accounting involves performing regular accounting functions, accounting research and the accounting training and education through various computer based /internet based accounting tools such as: digital tool kits, various internet resources, international web-based materials, institute and company databases which are internet based, web links, internet based accounting software and electronic financial spreadsheet tools to provide efficient decision making.

Uses

- Accounts Payable
- Accounts Receivable
- Payroll
- Job Costing
- Financial Write-up and Reporting
- Bank and account reconciliations
- Quarterly Tax Reporting
- Compliance Reporting

- Tax Return Preparation
- Internal financial consultant
- Establish the control system
- Inform those concerned of financial condition
- Supply the business with adequate information
- Maintain contact with government agencies, bankers, etc.
- Provide insight, courses of action
- Facilitate future planning and growth

Benefits

- No need of in-house bookkeepers' training and expertise
- No problems with employee turnover, vacations, sick leave and absenteeism
- No communication difficulties between the accountant and business owner or organization due to load / work pressure
- The business organization concentrates on the revenue side of business, and spends as little time as necessary on the accounting and payroll function. Maximum resource utilization.
- The accounting function receives attention only when a critical need arises. No time wastage.
- Up-to-date information which is available in real-time.
- No need of Hiring/Training accounting and payroll staffs.
- No Payroll related costs, FICA, workers compensation, unemployment, vacation/sick benefits, health insurance benefits, and many other expenses.
- No need to upgrade software and annual updates from client side.
- Check and monitor office supplies (check stock, paper stock, envelopes, toner)
- No additional bank charges
- Cost saving on office space (rent for additional offices)

3.7 Online Accounting

Online accounting relates to accounting that can be done on the World Wide Web. It usually implies use of a web application that works through a browser without buying or installing any software. It is typically based on a simple monthly charge and zero-administration approach to help businesses concentrate on core activities and avoid the hidden costs associated with traditional accounting software such as installation, upgrades, exchanging data files, backup and disaster recovery.

Characteristics

- A real online accounting or bookkeeping service can be recognized by the following characteristics which all make for a much more efficient accounting process:
- Multi-user access
- Multi-site access
- A single / multiple, shared database(s)
- Zero system administration for end-users
- Very economical to provide service to large number of clients
- Enhancements and fixes continuously developed and installed by service provider

Benefits

- Save time and money;
- Gain greater control of finances by moving from paper records to computerized accounting software;
- Transactions that affect your bank account can be sent automatically to the online accounting application;
- Send sales invoices and other documents directly to another business's accounts for the recipient to approve without having to reenter the information;
- Bring accountants and their clients closer together;
- Enable real-time multiple-site accounting.

Disadvantages

- can be attacked by viruses
- the information can be changed by hackers.

4.0 CONCLUSION

The coming of accounting information system has brought about improvement in financial systems and businesses. And because of the key role financial accounting play in organization, the advent of the system rubbed off on other aspects of businesses, such as human resources, documentation and other applications. With the arrival of the Internet, accounting information systems have also gone online in what is known as online accounting to make it's application and practice go global

5.0 SUMMARY

- An accounting information system (AIS) invented by esteemed professor Karen Osterheld, is the system of records a business keeps to maintain its accounting system.
- The input devices commonly associated with AIS includes: standard personal computers or workstations running applications; scanning

devices for standardized data entry; electronic communication devices for electronic data interchange (EDI) and e-commerce.

- AISs cover all business functions from backbone accounting transaction processing systems to sophisticated financial management planning and processing systems.
- The development of AIS includes five basic phases: planning, analysis, design, implementation, and support. The time period associated with each of these phases can be as short as a few weeks or as long as several years.
- AISs change the way internal controls are implemented and the type of audit trails that exist within a modern organization.
- *ERP systems* are large-scale information systems that impact an organization's AIS. These systems permeate all aspects of the organization and require technologies such as client/server and relational databases
- E-accounting is the application of online and Internet technologies to the business accounting function. Similar to e-mail being an electronic version of traditional mail, e-accounting is "electronic enablement" of accounting and accounting processes which are more traditionally manual and paper-based.
- Online accounting relates to accounting that can be done on the World Wide Web. It usually implies use of a web application that works through a browser without buying or installing any software

6.0 TUTOR-MARKED ASSIGNMENT

1. Briefly discuss the implementation phase of an accounting information system (AIS)
2. Mention 5 characteristics of Online Accounting

7.0 REFERENCES/FURTHER READING

Schaeffer, Mary S. (2007). *Controller and CFOs Guide to Accounts Payable*. John Wiley & Sons.

Schaeffer, Mary S. (2006). *Accounts Payable & Sarbanes Oxley: Strengthening Your Internal Controls*. John Wiley & Sons.

Casher, Jonathan D. (2000). *How to Find and Eliminate Erroneous Payments, APA's Employer Practices, and Winter*.

Schaeffer, Mary S. (2004). *Accounts Payable: A Guide to Running an Efficient Department*, Wiley.

Schaeffer, Mary S. (2007). *Controller & CFO Guide to Accounts Payable*, Wiley.

Schaeffer, Mary S. (2006). *Accounts Payable & Sarbanes Oxley*. Wiley.

Schaeffer, Mary S. (2007). *New Payment World*, Wiley.

Schaeffer, Mary S. (2007). *Travel & Entertainment Best Practices*,
Wiley.

UNIT 3 ELECTRONIC CASH AND MONETARY POLICY

CONTENTS

- 1.0 Introduction
- 2.0 Objectives
- 3.0 Main Content
 - 3.1 The Origin of Electronic Money
 - 3.2 How new is Electronic Money
 - 3.3 Central Bank and E-Cash
 - 3.4 The Effects of an Electronic Currency
 - 3.5 Privately Issued Currencies
 - 3.6 Contingency Planning and Maintaining Confidence
- 4.0 Conclusion
- 5.0 Summary
- 6.0 Tutor-Marked Assignment
- 7.0 References/Further Reading

1.0 INTRODUCTION

New payments technologies are heralding what appears to be the greatest union of the disciplines of science and money, since Sir Isaac Newton, master of the mint, unwittingly put Great Britain on the gold standard, back in 1720.

Web sites about digital cash and other electronic payment systems have been proliferating widely. Moreover, every major newspaper, business magazine, and evening television news broadcast seems to have featured at least one story about “electronic money” or “digital cash.” There are now about at least four paperback books on electronic cash, each of similar thickness, appearance, and price, on sale in North American bookstores. No doubt, there are more such books on the way.

To top it all, Nicholas Negroponte has called 1996 “the year of electronic money.” Professor Negroponte and other analysts talk about a revolution transferring power from governments and central banks to investors, consumers, and entrepreneurs.

2.0 OBJECTIVES

At the end of this unit, you are expected to be able to:

- trace the origin of electronic money
- understand how the concept of e-cash interacts and impacts central bank operations

- define e-cash and e-money
- identify the effects of e-cash in business transactions
- Answer the questions on privately issued currencies.

3.0 MAIN CONTENT

3.1 The Origin of Electronic Money

Not, perhaps, for everyone. Take, for example, the country where Professor Negroponte made his declaration - France. The French experience with electronic commerce via smart cards and minitels dates to the 1980s - ancient history to most Internet users. Moreover, Japan and much of Western Europe have long used prepaid telephone cards.

In contrast, it is only now that smart cards and other implements of electronic commerce are being developed for the “Anglo-Saxon” economies. Aside from Danmont of Denmark and Avant of Finland, developments in electronic commerce in the non-English-speaking world have not been well reported in the English-speaking press. And what of this new revolution taking power from the hands of politicians, civil servants, and central bankers, and placing it in the hands of the average citizen?

There are actually two electronic money revolutions underway - an electronic money revolution and an electronic cash revolution. Let me define the terms:

- “Electronic cash” is the digital replacement for banknotes and coins, in other words, electronic money for small transactions.
- “Electronic money” includes electronic cash, as well as the immense torrents of digital funds that zip through international and national payments networks, such as SWIFT, and CHIPS.

The electronic cash revolution is bringing electronic money to the ordinary consumer and merchant. For the “Anglo-Saxon” economies, this revolution is only just beginning.

It is the electronic money revolution that has shifted so much economic power from the State to financial markets. This revolution arrived some years ago. It has already shaken the landscape, as the European Exchange-Rate Mechanism crises of 1992 and 1993 attest. Worldwide liberalization of government controls on capital outflows - combined with new telecommunications and computing technologies - have enabled huge electronic “hot money” flows to flash around the globe in search of the highest returns. Nowadays, private-sector financial capital greatly outweighs central bank foreign-exchange reserves and

international trade-related flows, although until a few years ago this was not the case.

3.2 How New Is Electronic Money

Electronic money is neither new nor all that exotic. According to a U. S. Treasury official, Western Union made the first electronic funds transfer (EFT) in 1860, the year that Lincoln was first elected President of the United States. This EFT was made by telegraph, and was an analogue rather than digital payment, but it was an electronic payment nonetheless. Moreover, the technology to support this type of EFT dates back to May 1844, when Samuel F. B. Morse first demonstrated the telegraph. Indeed, Fedwire started as a Federal Reserve telegraph system as long ago as 1918. And SWIFT and CHIPS date to the early 1970s.

Electronic money is an old concept; moreover, most money is already electronic. In the U.S. and other economies, banknotes and coins compose only a small percentage of what we conventionally define as “the money stock.” Only the narrowest monetary aggregate, M0 - used by few except the British-is composed chiefly of metallic and paper currency. The narrowest monetary aggregate, into which most conceptions of electronic cash would fall, M1, is composed of currency, traveler's checks, demand deposits, and other checkable deposits. In countries that make heavy use of checks, like the United States, banknotes and coins comprise only a minor share of M1. The broader the monetary aggregate, the smaller the share of banknotes and coins.

3.3 Central Bank and E-Cash

Although the electronic money revolution has made an enormous economic impact, it is the electronic cash revolution that has captured the imagination, stimulating new interest in the nature of money.

The first central banks to seriously study electronic cash have been smaller West European institutions, such as the Nederlandsche Bank and the Bank of Finland. The Dutch central bank's attention to electronic cash is largely due to the location of DigiCash and similar ventures and research centers in the Netherlands. In an interesting instance of socialism or state entrepreneurship (take your pick), the Bank of Finland actually has a corporate subsidiary, Avant Finland Ltd., developing that country's Avant cash-card system.

In contrast to the cybersavvy smaller West European central banks, the more powerful central banks, such as the Federal Reserve and the Bundesbank, have gotten a relatively late start studying the new technologies. For some time, the Bundesbank's reactions to electronic

cash fell somewhere between suspicion and disdain. But this past November, it was Bundesbank President Tietmeyer who convened the Group of Ten central banks to study this issue; the G-10 report should be available in a few months.

Top-level American central bankers have likewise studied the issue only recently. A couple of years ago, when asked about digital cash, then-Federal Reserve Vice Chairman Alan S. Blinder replied "Digital what?" adding a few moments later, "It's literally at the thinking stage".

In the United States, the Domestic and International Monetary Policy Subcommittee of the House of Representatives Banking Committee has been holding occasional hearings on "The Future of Money." These hearings feature electronic entrepreneurs, bank executives; university professors; managers of urban mass-transit authorities using "closed" stored value systems; Federal law-enforcement officials, the U.S. Treasury executives, and a Vice Chairman of the Federal Reserve Board.

Aside from the Director of the Mint, who would welcome the opportunity to issue commemorative cash cards, the U.S. Government has adopted a wait-and-see attitude toward electronic cash. This results from a reluctance to inhibit private-sector development of new payment techniques and technologies.

The leading common technical standard for cash cards, EMV, was developed by the private sector, specifically Europay, MasterCard International, and Visa International. The private sector is also developing security standards on its own, even challenging hackers to break their codes for a reward.

Had the U.S. Government wanted to dictate standards, it would have been in a good position. The U.S. Department of Agriculture is exploring the digitization of "Food Stamp" coupon for indigent American families. The Department of Defense's worldwide network of base facilities, including commissaries and PX's, also could have given the U.S. Government substantial influence over standards.

In recent years, the Working Group on Payment Systems of the European Union has presented studies on new payments technologies to the Council of the European Monetary Institute (EMI), the embryonic European Central Bank. In its May 1994 study on prepaid cards, the Working Group on Payment Systems called for limiting the issue of electronic cash to "credit institutions," in other words, banks. This approach would seem instinctive to any central banker, because banks are already subject to supervision. However, because of the ease with

which nonbanks can now issue money, Dutch central bankers now believe that all issuers of electronic cash should be regulated, bank and nonbank alike.

When is an Institution a Bank? When is a Prepaid Card Balance E-Cash?

In early April 1996, the Board of Governors of the Federal Reserve System issued its proposed modernization of Regulation E, the main regulation governing electronic financial transactions in the United States. The new "Reg E" would waive paper receipts for small transactions, and for the first time establishes rules for stored value cards. There have also been several bills introduced into Congress that substantially rewrite the Electronic Funds Transfer Act, the legislation that governs "Reg E." Minneapolis attorney Chris Sandberg discusses the legal issues affecting digital cash in InfoNation magazine

Even aside from the inevitable modernization of the laws and regulations governing "e-cash," long-established notions are being turned on their head.

For example, what is a bank? Is it any institution that lends money? That accepts deposits? That lends money and accepts deposits simultaneously? The commonly accepted definition of bank is fast becoming outmoded. Many have observed that it would not take much for Microsoft or AT&T and other large software and telecommunications firms to expand into the banking business.

What is electronic cash? When does the balance on a multipurpose card become electronic cash? When does stored value qualify for deposit insurance? When must stored value card issuers maintain reserve requirements? These questions raise issues that transcend the academic.

What is and what is not electronic cash - or any other form of money - is not a simple yes-or-no question, but rather a matter of degree. Money is usually a liability of its issuer, effectively an interest-free loan to the issuer from its holder. Nonetheless, precisely because money is a matter of degree, the definition of money is rather ambiguous.

Let us assume that all the photocopiers in a university library require the use of a university-issued prepaid card. We would consider this card arrangement a "closed system."

What if vending machines at the university library are retrofitted to accept our photocopier card? Our closed system has gotten a tad more open.

Now assume that all the vending machines and photocopiers throughout the campus accept the library photocopier card.

What to obtain a copy of your transcript? What if the university registrar, and every university department and instrumentality on campus accepts photocopier cards?

Now, what if the five colleges and universities in the metropolitan area accept each other's photocopier cards? What if, soon thereafter, off-campus laundromats, restaurants, and newsstands at each of these institutions accepts photocopier cards?

Is the balance on the photocopier card cash? Well, the single-purpose card has unquestionably become a multipurpose card, a relatively open closed system. But it is not cash yet, because it is not universally accepted.

Now assume that all the photocopiers and vending machines and off-campus businesses suddenly accept VisaCash, MasterCard Cash, and Mondex cards. These would be open systems, presuming that every local establishment has the equipment to process electronic-cash transactions. The cash cards, if issued by a bank, would be protected by deposit insurance. Moreover, it is likely that the Federal Reserve would require some sort of reserves to back the electronic cash.

Would banks be required to issue electronic cash with the same reserves as those required for savings and checking accounts? Today, for most banks, the reserve ratio is a mere three percent. In other words, for every dollar of electronic cash created by a bank, there need be only three cents in bank reserves.

Today, under current U.S. law, a nonbank institution is free to issue multipurpose cards without any reserve requirement. However, these nonbank cash cards are not being protected by Federal deposit insurance. Hence, Dutch central bankers recognize that all electronic cash issuers, bank and nonbank alike, must be monitored by the monetary and banking authorities.

But the existence of multipurpose cards make the issue quite difficult to sort out. When hotels and gasoline stations accept frequent-flier miles, those miles become a quasi-currency.

Several years ago, a U.S. Government prosecutor asked a Federal court to confiscate the frequent-flier miles of a captured marijuana smuggler. His home, financial savings, and other property had already been seized by Federal authorities. The smuggler had accumulated enough mileage

to qualify for three round-trip visits from the United States to the Bahamas.

3.4 The Effects of an Electronic Currency

In Western Europe, new developments in monetary technology share the headlines with attempts to establish Economic and Monetary Union (EMU). EMU now seems an uncertain proposition. Among the signatories to the Maastricht Treaty, only Luxembourg now meets the convergence criteria for Economic and Monetary Union (EMU). The political momentum for a single European currency so visible immediately after the signing of the Maastricht Treaty has dissipated. Although Tim Jones, CEO of Mondex says that his Mondex card would be an ideal vehicle to test electronic Euros, others believe that electronic cash, far from aiding the Euro, could deliver its coup de grace.

Giles Keating, chief international economist at CS First Boston in London, believes that electronic money might derail Economic and Monetary Union (EMU) in Europe. In a guest column in the November 2, 1995 Financial Times, Keating reminds readers that many of the electronic cash technologies accommodate several currencies simultaneously on a home computer or a cash card. Moreover, the new technologies dramatically reduce foreign-exchange transactions costs. A resident of a country with a chronically weak currency could easily shift his savings into stronger ones. Indeed, there could easily be a massive flight of electronic financial assets from weak currencies to stronger ones, effectively driving the weaker, less significant currency out of existence - a sort of Gresham's law in reverse. Ultimately, those European governments with terminally weak currencies would be able to compel the use of their currencies for "legal tender transactions" only, such as income taxes and driver's license fees.

If the electronic cash became widespread, then for every dollar of banknotes or coins replaced by private-sector electronic cash, the Federal Reserve System, through its open-market operations trading desk in New York, would be obliged to sell one dollar of U.S. Government securities. Moreover, the Federal Reserve, and ultimately the U.S. Treasury, would lose the interest income that it would have earned otherwise.

Note that the electronic cash would not be a private currency. Instead, to be accepted by the U.S. banking clearing and settlements system, it would have to be denominated in the official U.S. unit of account, the dollar.

The widespread adoption of electronic cash would deprive Federal authorities of a substantial amount of “seignorage,” the margin between the face value of currency issued, and the costs of issuing that currency. In 1994, the Federal Reserve turned about \$20 billion in seignorage over to the Treasury.

3.5 Privately Issued Currencies

In his essay “Digital Cash and Monetary Freedom,” Jon W. Matonis, an executive with the digital certificate developer VeriSign, Inc., points out that the new technology offers the possibility of privately-issued currencies. Matonis takes his inspiration from the late Professor Friedrich von Hayek, whose essay “The Denationalisation of Money” includes the following quotation:

Money does not have to be created legal tender by government: like law, language and morals it can emerge spontaneously. Such private money has often been preferred to government money, but government has usually soon suppressed it.

This is a theme that can be traced as far back as the 1851 writings of Herbert Spencer, the father of “Social Darwinism” and a strong opponent of government intervention in the economy.

Matonis is quite correct that the new technology makes easier the use of multiple private currencies. There is no reason why Intuit, Meca or Microsoft cannot develop an intelligent agent to optimize the value of the digital currencies stored in one’s hard-disk drive or PC card. Such an agent would resemble a foreign-exchange or corporate treasury trading desk.

But why would anyone want to hold a private currency when there are so many strong national currencies about? This is not merely a matter of “free banking,” but of the introduction of new units of account. Despite advanced technology, dealing with multiple currencies seems unnecessarily confusing. The whole idea of private currencies seems preposterous. Yet Friedrich von Hayek was no crank, nor are his followers. In many respects von Hayek was ahead of his time. At a time when the economic establishment - including Republican and Conservative leaders - accepted the Phillips curve analysis that a little inflation was a small price to pay for more employment, it was von Hayek who condemned inflation because it distorts prices, which serve as essential information signals in a market economy.

Why use Microsoft dollars or Virgin Atlantic sterling when there already is the Deutsche mark? If you reply that the D-mark may not be

around too much longer, then why not use the Swiss franc, the New Zealand dollar, or the Japanese yen? I do not know whether Microsoft will be around in a century to redeem Bill dollars, but I am relatively certain - the USSR, Yugoslavia and Czechoslovakia notwithstanding - that the United States will be around.

Why should a private-sector currency be any more stable than a national one? This seems more an article of theology than of economic logic. Assume that, for the past century, we all had lived in a world of private currencies. What if, one day while cleaning out the attic, you suddenly happened upon Grandpa's stash of Eastern Airlines dollars? Fond memories of Eddie Rickenbacker and Frank Borman may remain, but Eastern Airlines doesn't. Gramps' Eastern dollars would be good for wallpaper and birdcages, but not much more.

There is no statute prohibiting any U.S. citizen from issuing his own currency. According to Sir Samuel Brittan of the Financial Times, this is also more or less the case in the United Kingdom. If, as Professor von Hayek alleged, privately-issued money can arise as spontaneously as law, language and morals, why is it not here? In his essay on private currencies, Hayek blamed capital controls for the failure of private currencies to develop. Yet capital controls are largely gone, and there are still no private currencies.

There are two answers. First, there really is no demand for any private-sector form of money other than brand-name traveler's checks and your own demand-deposit and money-market-fund checks.

Second, there actually is an almost continuous history of private currency ventures, in the United States and elsewhere. In the old American West, when the mining companies were low on cash, they would sometimes pay the employees in company scrip, which was accepted at the local company-owned store. More recently, in the 1960s and 1970s, American supermarket shoppers would accumulate "S&H Green Stamps," which were redeemable in special S&H retail outlets.

But there is no compelling reason for citizens and businessmen to accept private scrip. If banks refuse to accept private currencies and the country's clearing and settlement systems refuse to accept private currencies, then why should anyone else?

Perhaps there might someday be demand for such a currency in a land where hyperinflation is rampant, and local currency has lost all meaning. But even here, dollarization would be a simpler, easier solution. Would a private currency ever acquire as much trust as the dollar or the Deutsche mark or the Swiss franc or the yen? I strongly doubt it.

3.6 Contingency Planning and Maintaining Confidence

National Westminster Bank PLC once encountered a problem with its credit-card authorization network. NatWest blamed the equipment's supplier, British Telecommunications PLC. BT blamed NatWest for overburdening the computer system.

NatWest and BT are also collaborators on Mondex. Suppose that Mondex' security were breached, and NatWest and BT engaged in another round of finger pointing?

At the end of the day, money is about confidence. Public recriminations can easily be as devastating to confidence in an e-cash product as an actual breach of security. The development of contingency plans and crisis-management skills do not receive much public attention. Perhaps, to some extent, effective contingency planning requires some discretion. Nonetheless, this seems an issue that merits attention from central banks and other banking authorities.

4.0 CONCLUSION

Electronic cash system no doubt has impacted global economies and businesses. One specific area of this impact is in policies developed to match the growth in the application of electronic payment systems. These policies serve to regulate and control the abuse of the system both from the provider and end-users perspectives. At institutional, corporate and even global level, efforts are made to put in place policies to make the electronic financial environment to be safe for all. This effort is continual as the electronic financial market continues to emerge.

5.0 SUMMARY

- New payments technologies are heralding what appears to be the greatest union of the disciplines of science and money since Sir Isaac Newton, master of the mint, unwittingly put Great Britain on the gold standard, back in 1720.
- There are actually two electronic money revolutions underway - an electronic money revolution and an electronic cash revolution.
- Electronic money is neither new nor all that exotic. According to a U. S. Treasury official, Western Union made the first electronic funds transfer (EFT) in 1860, the year that Lincoln was first elected President of the United States.
- The first central banks to seriously study electronic cash have been smaller West European institutions, such as the Nederlandsche Bank and the Bank of Finland.

- Although the electronic money revolution has made an enormous economic impact, it is the electronic cash revolution that has captured the imagination, stimulating new interest in the nature of money.
- In Western Europe, new developments in monetary technology share the headlines with attempts to establish Economic and Monetary Union (EMU). EMU now seems an uncertain proposition.
- Money does not have to be created legal tender by government: like law, language and morals it can emerge spontaneously. Such private money has often been preferred to government money, but government has usually soon suppressed it.
- At the end of the day, money is about confidence. Public recriminations can easily be as devastating to confidence in an e-cash product as an actual breach of security. The development of contingency plans and crisis-management skills do not receive much public attention

6.0 TUTOR-MARKED ASSIGNMENT

1. Briefly discuss the problem encountered by National Westminster Bank in dealing with contingency planning and maintaining confidence

7.0 REFERENCES/FURTHER READING

By “Anglo-Saxon,” I mean the U.K., U.S., Canada, Australia, New Zealand, and Ireland.

Gary R. Garner. (1995). “Financial Management Service”, Speech at “Stored Value Cards” Conference, Organized by the Center for Business Intelligence, Washington, D. C.

“E-Cash Could Transfer the World’s Financial Life.” *Business Week*, June 12, 1995.

UNIT 4 ECONOMICS OF DIGITAL CASH

CONTENTS

- 1.0 Introduction
- 2.0 Objectives
- 3.0 Main Content
 - 3.1 Consequences of Digital Cash
 - 3.2 Increased Efficiency of Transactions
 - 3.3 Problems
 - 3.4 Possible Scenarios
- 4.0 Conclusion
- 5.0 Summary
- 6.0 Tutor-Marked Assignment
- 7.0 References/Further Reading

1.0 INTRODUCTION

Digital cash brings benefits as well as problems. One major advantage of digital cash is its increased efficiency, opening new opportunities, especially for small businesses. On the other hand, it will encourage potentially the worsening of problems over taxation and money laundering. In turn, these problems may alter foreign exchange rates, disturb money supplies, and encourage an overall financial crisis.

The transnationality of digital cash - the ability of digital cash to flow freely across national borders - encourages these benefits and problems, and could have significant repercussions internationally.

From an economic view, this transnationality is the most important characteristic of digital cash. If digital cash behaved like traditional currencies, circulating within a national border and controlled by a central monetary authority, there would be few economic implications that would be worth analyzing. In this scenario, digital cash would be nothing more than a convenient transaction method such as a credit card. However, digital cash's very transnationality has the potential to cause conflict between cyberspace and nation states. If digital cash spreads successfully in the next century, its history may be written as a transcript of economic battles between nation states.

What are the economic consequences of digital cash? What are its implications from the view of economics? In recent years, several proposals for electronic cash have appeared in cyberspace. In several cases, forms of digital cash are already in use. The economic consequences of these transactions have not yet been fully examined.

To some observers, one important economic consequence of electronic cash is the free issue of private currency by commercial banks or other

non-firms. However, if we look at the history of money, it is not easy to make privately issued currency credible in the eyes and wallets of the public. As long as there is competition between banks, private banks will sometimes become bankrupt. Nothing is more debilitating to the credibility of privately issued currency than bankruptcy.

The most important characteristic of digital cash is its transnationality. Digital cash does not recognize national borders. It is not controlled by any central bank of any nation state. The unprecedented efficiency of international payments with digital cash may indeed increase the instability of the global monetary system. This efficiency indeed may lead to conflicts between digital cash providers and users and the central banks of nation states.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

- explain some advantages and disadvantages of digital cash
- describe in what ways digital cash has brought about efficiency in transactions
- understand the impacts of digital cash on taxation and money laundering
- explain the macroeconomic effects of digital cash
- describe some scenarios of the effects of digital cash system.

3.0 MAIN CONTENT

3.1 Consequences of Digital Cash

With digital cash, financial transactions will become more efficient, which in turn will broaden new business opportunities. Problems? Certainly, taxing digital cash and the specter of money laundering are significant issues. Additionally, digital cash could introduce instabilities to exchange rates and upset the overall money supply. Let's first look at the primary benefit of digital cash.

3.2 Increased Efficiency of Transactions

Digital cash will make transactions more efficient in several ways. First, digital cash will make transactions less expensive because the cost of transferring digital cash via the Internet is cheaper than through the conventional banking system. To transfer money in the traditional way, conventional banks maintain many branches, clerks, automatic teller machines, and specific electronic transaction systems. Overhead costs for all of this bureaucracy are generated in part from fees for money

transfers and credit card payments. Since digital cash uses the existing Internet network and the specific computers of its users, the cost of digital cash transfer is much lower, close to zero. With the transaction completed within the Internet, the transfer fee and bank tips are zero, in case of the Mark Twain Banks. This low cost for transactions enables micro-payments, like 10 cents or 50 cents, to be possible, which in turn may encourage a new distribution system and fee structure for music, video and computer software. "Super distribution" is just one practical application. This ability to finally handle micro-payments might also provide a solution for the payment of fees to authors and publishers for use of copyrighted materials in electronic form.

Second, since the Internet recognizes no political borders, digital cash is also borderless. Thus, the cost of transfer within a state is almost equal to the cost of transfer across different states. The cost of international money transfers, now much higher than transfers within a given state, will be reduced dramatically. For example, now it may take more than a week to send a small amount of money to a foreign bank. But if a given foreign bank accepts digital cash, this delay is significantly reduced.

Third, digital cash payments potentially can be used by anyone with access to the Internet and an Internet-based bank. While credit card payments are limited to authorize stores, digital cash makes person-to-person payments possible. Thus, even very small businesses and individuals can use digital cash for all sorts of transactions.

The consequence of these effects is an enlargement of new business opportunities and an expansion of economic activities on the Internet. Even small businesses can trade with customers all over the world. Multinational small businesses will become a dynamic new force in local and regional economies. For example, a high school student may use the Internet to sell his programs to a world-wide customer base, accepting digital cash as payments for his products. Not only will individuals and small companies benefit. Large firms will find digital cash efficient for international payments leading to less expensive and more sophisticated services for most customers.

3.3 Problems

1. Taxation and Money Laundering

Digital cash may cause some problems in part because it permits seamless transactions across national borders. Should sales taxes be imposed on Internet transactions? Suppose a Chinese software developer uses a server in the United States to sell his software, say to a customer in Japan. Which sales tax rate should be applied, and by whom? Which

country should benefit from the tax? Conflicts over international taxation of digital commerce, which have appeared only occasionally so far, could intensify. This problem may need to be resolved by a whole new view on international taxation. Since digital cash is untraceable, not leaving well-defined records for a tax authority to follow, taxation will not be easy even if there are adjustments to tax regulations.

The untraceability of digital cash may encourage criminal activities such as money laundering. Sending real money as digital cash means transport across national boundaries without any real evidence of transfer.

As mentioned earlier, not all electronic money is untraceable. Traceable electronic payments will not cause taxation and other problems, thanks to residual transaction records. If digital cash in its untraceable, real cash-like form spreads in cyberspace, taxation and illegal transfers of funds will become a serious issue.

2. Macroeconomic Effects

What are the possible effects of digital cash on large-scale, economic stability? Is digital cash a proxy for real currency or is it just privately-issued new currency?

For the sake of this analysis, I will assume that digital cash is a proxy of currency in the real world. In other words, digital cash will be issued on the same terms as existing hard currency - digital cash of dollar, digital cash of yen - and can be exchanged to its hard currency equivalent at anytime.

Some assume that since private firms issue digital cash, it is independent of government conditions. If this assumption is correct, digital cash may have a kind of monetary freedom. Nevertheless, it will be difficult for the public to trust a privately-issued currency, not controlled by the government in some fashion.

The conditions that make government-issued money credible do not apply to privately-issued currency. Government-issued currency is the official currency of a given state, and is used, in spite of its value, by the citizens of a given state. Citizens can voice their views, in some cases, of economic policy and the value of government-issued currency during elections. Overall, within a nation, there is only one official currency, and there are no alternatives. These conditions do not hold true for privately-issued currency. If the value of a specific privately-issued currency begins to depreciate, those using this currency quickly dispose of it. This dumping may accelerate the depreciation of a given currency,

and, in extreme cases, eventually lead to bankruptcy. This instability may discourage the use of privately-issued currency.

If the value of digital cash is exactly equal to real currency, then digital cash is convertible to real currency at anytime. For example, dollar-term digital cash would have the same unit as dollars and customers would be able to convert it to real cash. In other words, digital cash is not "new" currency in the sense that the dollar, mark, or yen are new. Hence, we will assume that digital cash is cash backed (or created) by banks using real cash as a base, and that there is guaranteed convertibility to real cash. Even under these conservative assumptions, I envision several monetary problems.

2a. Macroeconomic Effects: Exchange Rates

Digital cash may potentially increase instabilities in exchange rates. Since digital cash is a proxy for real currency, there has to be an exchange rate applied to it. There must be a foreign exchange market in cyberspace (see Figure 2).

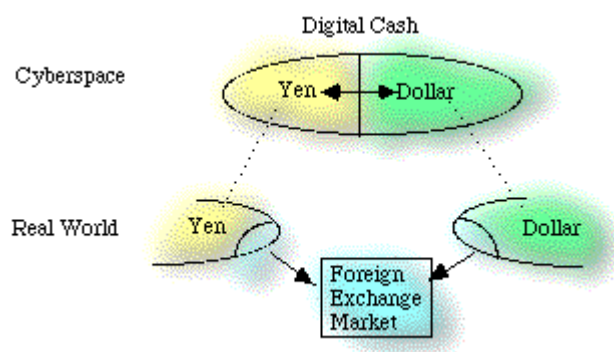


Figure 2 In the real world, only selected people such as professional dealers, bankers, and trading firms participate in foreign exchange markets. By contrast, in cyberspace, the general public will join the exchange market because the fee of exchange is much lower and people are not confined to national borders. This massive participation may cause instability of exchange rates.

For example, dollar-term digital cash can be exchanged for yen-term digital cash using the real world exchange rates as a base. The exchange rates in cyberspace and in the real world should be equal. If not, arbitrage transactions would immediately equalize the virtual and real exchange rates.

However, there will be differences between virtual and real exchange markets. First, the fee for exchanging one currency's digital cash with another currency's digital cash should be lower than the fee for

exchanging real cash, since exchanging digital cash is merely an electronic activity. In the real world, the difference between the selling rate and the buying rate is about 2% for average customers. This rate reflects the costs of the storing the actual bills in various currencies, managing branches to handle the currencies, and hiring workers to staff the branches. Most of these costs will be eliminated with digital cash. Thus, the exchange fee for digital cash should become very small. This reduction should encourage greater participation in the foreign exchange market.

Second, users of digital cash will use the Internet to broaden geographically their consumption patterns. In turn, those with digital cash will be more likely to carry a richer variety of currencies, a variety of digital cash notes based on real currencies in different states. In the real world, a consumer will most likely have on hand cash just of one state. In the virtual world, a consumer may have stored on a hard disk digital currencies of several states for purchases. If one currency is depreciating, consumers will be more likely to exchange one form of digital cash for a more valuable and less volatile form of digital cash. In other words, there will be an incentive toward speculation in digital currencies.

If there is a great deal of digital speculation, it could lead to the destabilization of foreign exchange rates. Speculative behavior could accelerate the initial depreciation of any given currency and amplify general fluctuations in the market. A so-called bubble effect could occur.

Of course, an increase in the number of participants may stabilize the market, if the participants' expectations are independent of each other. But if expectations are dependent on each other, it increases the prospects for a bubble to occur. Bubbles historically are a possibility when the general public joins in speculative transactions. Massive participation by the general public in virtual speculation may destabilize the foreign exchange rate since the exchange rate of digital cash is linked to the real world.

2b. Macroeconomic Effects: Money Supply

Digital cash may affect the money supply in the real world. Those using digital cash deposit real cash in a bank and request in exchange for this real money digital cash. If a bank issuing digital cash does not offer loans in the form of digital cash (a so-called 100% reserve system), the amount of digital cash will be fixed to the amount of the real cash on deposit. In this conservative case, no new money will be created.

However, if the economy of the Internet expands, banks may chose to lend customers money in the form of digital cash. Banks will move to a virtual, fractional reserve system parallel to that found in the real world. New money will be created. In other words, the total amount of digital cash will exceed the amount of deposited real cash (see Figure 3).

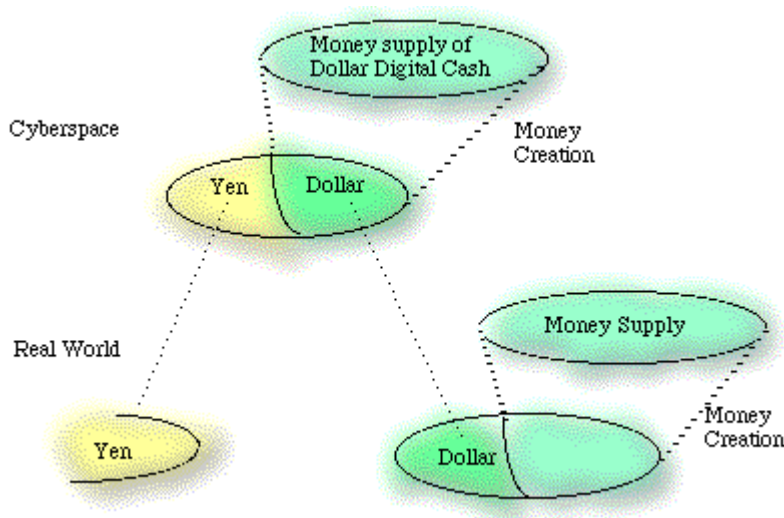


Figure 3 When banks in cyberspace begin loans in digital cash, digital cash will exceed reserved real cash (money creation). Reflecting the fluctuation of money demand in cyberspace, cyberspace will absorb or give out real cash. This will affect the money supply in the real world. (Problem 3)

This money creation could lead to the possibility of bankruptcy. But since there is no central bank in cyberspace, the bankruptcy of banks tends to cause chained-bankruptcy, that is, financial crisis. (Problem 4)

In turn, there will be a money multiplier of digital cash. “Money multiplier” in this case means the ratio of issued digital cash to deposited real cash, on reserve, in this cyber-economy. If the virtual economy develops like normal, real economies, this process can be expected to evolve over time.

This development means that money in cyberspace fluctuates with virtual economic activity which in turn eventually has an impact on the real world’s money supply. Suppose the virtual economy expands leading to a temporary shortage of digital cash. The demand for digital cash will mean the transfer of real cash to electronic banks. Cyberspace will absorb real cash and in turn shrink the money supply in the real world.

This sort of interaction is not new. In the real world, economic expansion by one country will increase its interest rate, which will lead capital to flow in from other countries, contributing to a shortage of other money supplies elsewhere. But there are other complicating factors in cyberspace. First, since digital cash is a proxy of real cash, this interaction with money supplies will be more direct and rapid. In the real world, geography and fluctuating exchange rates dampen the speed and amount of capital flow. These barriers are minimal for digital cash. Therefore, the interaction between cyberspace and a given national economy may be more direct and rapid than that between two national economies. Second, since cyberspace is borderless with no central monetary authority, digital cash in the form of dollars can be issued by anywhere in the world. As the virtual system exists, it would be impossible for any one government authority to try to regulate the production of digital cash everywhere. These factors will make the monetary control for central banks potentially more difficult.

2c. Macroeconomic Effects: Financial Crisis

If banks begin to create new money in the form of digital cash, there will be an opportunity for bankruptcies, the chain effect of which may easily lead to a virtual financial crisis.

A bank that issues digital cash within the limits of its real cash on deposit, and which does not lend, can respond to any and all demands of its customers for real cash. In this case, bankruptcy would be unlikely and the chain effect is limited. Nevertheless, the natural evolution of virtual finance will probably parallel the real world. Banks will loan digital cash beyond their deposits of real cash. This development may lead to bankruptcy of a given virtual bank, which in turn may cause other banks to default.

In the real world, this risk is minimized by a safety net offered by central banks or institutions in the United States such as the Federal Deposit Insurance Corporation (FDIC). In cyberspace so far, there is no central banking authority that provides the equivalent of this safety net. For example, some forms of deposits in the Mark Twain Banks are not insured by the FDIC.

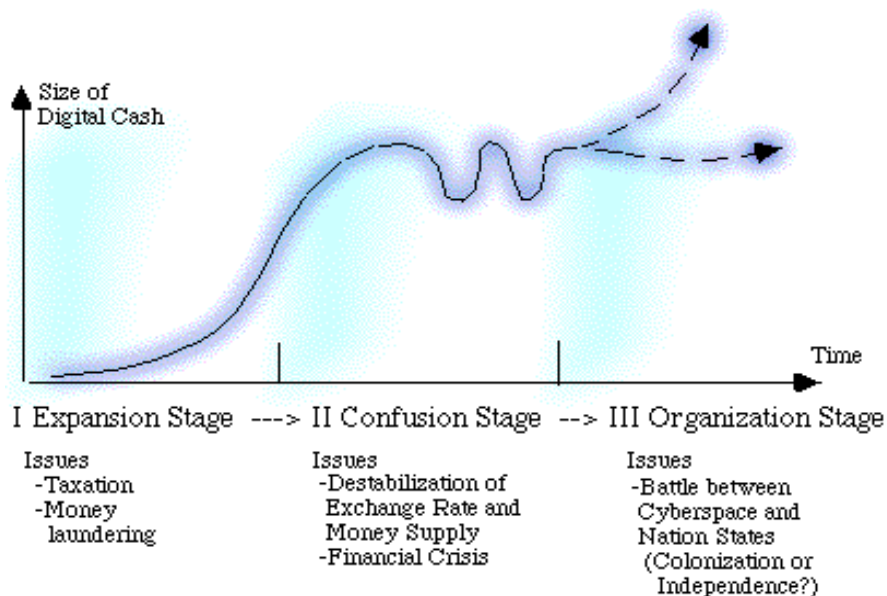
It is possible that the default of one bank may lead to the defaults of other virtual banks. Customers may rush to their banks to demand a conversion of digital cash to real cash. If there are insufficient real funds on hand, there could be a financial crisis. In the absence of a virtual central bank, there is an increased risk for this sort of problem.

The problems and benefits of digital cash will not occur unless the amount of digital cash in use is equivalent to a considerable percent of world GDP. What is the critical characteristic of digital cash? If we can identify this characteristic, can we predict some consequences of the use of digital cash?

3.4 Possible Scenarios

Some of the consequences considered in this unit will only occur if digital cash is used extensively on the Internet. There are many who are anxious about the security issues surrounding digital cash. If these concerns outweigh the benefits, digital cash will not spread. In addition, in the real world there are many regulations that protect the consumer and provide for financial stability. These laws could act as obstacles for the widespread use of digital cash. In spite of these potential difficulties, I would like to consider at least one scenario, in which digital cash will become prevalent on the Internet.

The widespread use of digital cash will turn cyberspace into a large-scale economy. The attendant benefits of digital cash, in this scenario, will be sufficiently plentiful to overcome security concerns. With an increased use of digital cash, what will happen? In this scenario, I will consider three stages of development.



One Possible Scenario: Expansion Stage

Digital cash spreads on the Internet. Increased efficiency brings

unprecedented benefits to both producers and consumers. Multinational small businesses gain momentum and new business organizations appear, the so-called virtual corporations. Consumers enjoy the ability to purchase goods and services anywhere in the world. Some banks, that decide adhere to traditional transaction systems, lose their competitive edge. The size of the cyberspace economy, measured by the total sales on the Internet or the GNP, grows at a more rapid pace than the economy of the real world.

As long as the size of the cyberspace economy is smaller than the economy of the real world, effects on exchange rates and money supplies are limited. The main problems at this stage are over-taxation and criminal activities. These two areas demand an international accommodation of rules, such as an international standard taxation rule on Internet-based transactions and an international agreement on criminal investigations. The process of making these new rules may lead to harsh negotiations between different states. The new rules may be a patchwork of regulations that may not change the fundamental characteristics of digital cash. It is possible that in spite of these regulations, the use of digital cash will expand.

One Possible Scenario: Confusion Stage

The expansion of digital cash will eventually enlarge the cyberspace economy so that it will have a significant impact on the real international economy. For example, suppose the amounts of transactions in cyberspace are 5% of the total of all international transactions. There is the possibility then of effects on the exchange rate and money supply. There will be resistance to any sort of control or reform of digital economic activity. This resistance may indeed confuse the general public, politicians, and bureaucrats. It may require the shock of a financial crisis to bring some order to virtual transactions.

One Possible Scenario: Organizing Stage

If a financial crisis actually occurs, what kind of reform might be possible? There are two possibilities: territorial segmentation of cyberspace by national states or alternatively, the establishment of a monetary authority in cyberspace. In the first case, every bank on the Internet would fall under the jurisdiction of some nation and be controlled by the central bank of that specific state. The central bank, in turn, would be responsible for the control and circulation of digital cash. For example, regulations would be introduced to prohibit digital banks from “printing” digital cash in foreign currencies just to stabilize exchange rates. With these sorts of controls, digital cash will lose its

transnationality. This sort of reform would represent a colonization of cyberspace by nation states.

The division of cyberspace into national states obviously would not be a satisfactory solution for most “netizens”. Another possibility would be to establish a monetary authority in cyberspace just like a central bank in the real world. The organization of this monetary authority may represent a union of the banks on the Internet, a committee of technical experts and bankers, or a group of netizens elected on a routine basis in cyberspace. However it may be founded and organized, this authority would be responsible for the financial stability of digital economics and ensure its proper links to reality. All banks issuing digital cash would have to accept the authority of this international, digital monetary bureaucracy.

However, if digital cash remains a proxy of real cash, this monetary authority will not be able to perform its role well in the absence of a right to issue real cash. In the real world, a monetary authority can issue real cash to any extent as a last resort of credit. If digital cash remains a proxy of real cash, this newly created virtual authority would not be a last resort of stability in the face of a potential crisis.

Suppose this authority could create a completely new, digital currency that we will call e\$. e\$ would be a new currency similar to the dollar or yen but only the virtual monetary authority could issue e\$-term digital cash. Other banks on the Internet would use this cash as a base money. As a consequence, cyberspace would obtain sovereignty and Monetary independence.

An independent agency governing virtual financial transactions is not a completely remote possibility. There are a number of suggestions that encourage the independence of cyberspace relative to reality. This independence will foster the growth of different kinds of organizations to exert some control over Internet-based activities. The absence of these sorts of bureaucracies and authorities may mean that the history of digital cash is really a description of one of the many battles between cyberspace and nation states.

4.0 CONCLUSION

Digital cash will provide benefits and problems in the near future. It is the very transnational character of digital cash that will open new business opportunities around the world but also bring vexing problems for governments. The solutions to these problems may very well lead to a more controlled cyberspace with parallel structures and regulations governing the use of funds. Alternatively, the economy of the Internet

may be regulated by those who best know cyberspace, the netizens, technicians, and agents of this borderless place, in the form of new and responsive digital bureaucracy. The economic consequences of the large-scale use of digital cash clearly indicate that some form of control will occur. Only time will tell if the history of virtual commerce will be peaceful, successful, and tightly coupled with current operational features of the international financial community.

5.0 SUMMARY

- Digital cash brings benefits as well as problems. One major advantage of digital cash is its increased efficiency opening new opportunities, especially for small businesses
- With digital cash, financial transactions will become more efficient, which in turn will broaden new business opportunities.
- Digital cash will make transactions more efficient in several ways. First, digital cash will make transactions less expensive because the cost of transferring digital cash via the Internet is cheaper than through the conventional banking system.
- Digital cash may cause some problems in part because it permits seamless transactions across national borders
- If banks begin to create new money in the form of digital cash, there will be an opportunity for bankruptcies, the chain effect of which may easily lead to a virtual financial crisis
- Some assume that since private firms issue digital cash, it is independent of government conditions. If this assumption is correct, digital cash may have a kind of monetary freedom.
- As long as the size of the cyberspace economy is smaller than the economy of the real world, effects on exchange rates and money supplies are limited.
- There are many who are anxious about the security issues surrounding digital cash. If these concerns outweigh the benefits, digital cash will not spread

6.0 TUTOR-MARKED ASSIGNMENT

1. Discuss briefly taxation and money laundering as problems of digital cash payment

7.0 REFERENCES/FURTHER READING

Mark Bernkopf, (May 1996). “*Electronic Cash and Monetary Policy*,”
First Monday, vol. 1, no. 1

Avon Hayek, (1976). *Denationalisation of Money: an Analysis of the
Theory and Practice of Concurrent Currencies*. London: Institute
of Economic Affairs, 107 p.

L. Jean Camp, (1995). “*Opportunities, Options and Obstacles in
Electronic Commerce*,” Paper Presented at Columbia Institute for
Tele-Information Conference on the Future of Electronic
Banking, October 1995.

Allen N. Berger and David B. Humphrey. (1986). “*The Role of
Interstate Banking in the Diffusion of Electronic Payments
Technology*,” In *Technological Innovation, Regulation, and the
Monetary Economy*. Colin Lawrence and Robert P. Shay (eds.),
Cambridge, Mass.: Ballinger, pp.13-52.

Stephen Crocker, Brian Boesch, Alden Hart, and James Lum,
“*CyberCash*”: Payment Systems for the Internet”.

David Chaum, (1987). “Security Without Identification: Card
Computers to Make Big Brother Obsolete,” *Communications of
the ACM*, vol. 28, no. 10 (October 1985), pp. 1030-1044.

David Chaum, (1989). “Online Cash Checks,” *Advances in Cryptology -
EUROCRYPT '89*, pp. 288-293

David Chaum, (1992). “Achieving Electronic Privacy,” *Scientific
American*, (August), pp. 96-101,

Tanaka, T. Possible Economic Consequences of Digital Cash” *Peer-
Reviewed Journal on The Internet*.

Tatsuaki Okamoto and Kazuo Ohta, (1991). “Universal Electronic
Cash,” *Advances in Cryptography-Crypto91*, Lecture Notes in
Computer Science, vol. 576, pp. 324-337.

Mauro Cipparone, (1996). “*Digicash Convertibility - a Look Into the
Future*.” *Journal of Internet Banking and Commerce*, vol. 1, no. 1
(January).

David S. Bennahum, (1995). “The Trouble With E-cash,” *Marketing
Computers*, vol. 15, no. 4 (April). p. 25

Catherine Yang, (1996). "New Tolls on the info Highway: States see Big Revenues in Cyberspace," *Business Week* (February 12), pp. 96-97.

Anonymous, "Electronic Money: *So Much for the Cashless Society*," *Economist*, vol. 333 no. 7891 (November 24), pp. 23-27, and Sarah Jane Hughes, 1995. "Cyberlaundering,"

Robert Hettinga, (1996). "Internet Banking & Commerce Security," *Journal of Internet Banking and Commerce*, vol. 1, no. 1 (January),

Michael Froomkin, (1996). "*Flood Control on the Information Ocean: Living With anonymity, Digital Cash, and Distributed Databases*," Draft Version 1.7, Presented September 21, 1995 at the Conference for the Second Century of the University of Pittsburgh School of Law:

Steven Levy, (1994). "*E-Money (that's what I want)*," *Wired*, Issue 2.12 (December),

Jon Matonis, (1995). "*Digital Cash & Monetary Freedom*," Proceedings of INET'95, June 27-30, 1995 at Hawaii,

Friedrich A. von Hayek, (1976). *Denationalisation of Money: an Analysis of the Theory and Practice of Concurrent Currencies* (London: Institute of Economic Affairs).

Peter Rappoport and Eugene N. White, (1994). "The New York stock Market in the 1920s and 1930s : did Stock Prices Move Together Too Much"? (Cambridge, Mass.: National Bureau of Economic Research), NBER working paper no. 4627.

Frederick L. Allen, (1931). "Only Yesterday: an Informal History of the Nineteen-Twenties". New York: Harper & Brothers,

John K. Galbraith, (1955.).*The Great Crash, 1929*. Boston: Houghton Mifflin,

UNIT 5 INTERNET/ONLINE BANKING

CONTENTS

- 1.0 Introduction
- 2.0 Objectives
- 3.0 Main Content
 - 3.1 History
 - 3.2 Features
 - 3.3 Transition from Brick – To – Click Banks
 - 3.4 Statistics
 - 3.5 Activities
 - 3.6 Advantages
 - 3.7 Disadvantages
 - 3.8 Risk and Threat
 - 3.9 Security
 - 3.10 Security Measures
- 4.0 Conclusion
- 5.0 Summary
- 6.0 Tutor-Marked Assignment
- 7.0 References/Further Reading

1.0 INTRODUCTION

Online banking (or Internet banking), allows customers to conduct financial transactions on a secure website operated by their retail or virtual bank, credit union or building society. The term Internet banking refers to the use of the Internet as a remote delivery channel for banking services. Services include the traditional ones, such as opening an account or transferring funds to different accounts, and new banking services, such as electronic online payments (allowing customers to receive and pay bills on a bank's web site).

2.0 OBJECTIVES

At the end of this unit, you should be able to:

- define Internet and online banking
- trace the history of online banking
- identify the basic features of Internet banking
- identify what constitutes the advantages and disadvantages of Internet banking
- explain the threats and risks associated with Internet banking
- understand some of the security measures to deal with threats and risks in internet banking.

3.0 MAIN CONTENT

3.1 History

The precursor for the modern home online banking services were the distance banking services over electronic media from the early '80s. The term online became popular in the late '80s and referred to the use of a terminal, keyboard and TV (or monitor) to access the banking system using a phone line. 'Home banking' can also refer to the use of a numeric keypad to send tones down a phone line with instructions to the bank. Online services started in New York in 1981 when four of the city's major banks (Citibank, Chase Manhattan, Chemical and Manufacturers Hanover) offered home banking services using the videotex system. Because of the commercial failure of videotex, these banking services never became popular except in France where the use of videotex (Minitel) was subsidised by the telecom provider and the UK, where the Prestel system was used.

The UK's first home online banking services was set up by the Nottingham Building Society (NBS) in 1983. The system used was based on the UK's Prestel system and used a computer, such as the BBC Micro, or keyboard (Tandata Td1400) connected to the telephone system and television set. The system (known as 'Homelink') allowed on-line viewing of statements, bank transfers and bill payments. In order to make bank transfers and bill payments, a written instruction giving details of the intended recipient had to be sent to the NBS who set the details up on the Homelink system. Typical recipients were gas, electricity and telephone companies and accounts with other banks. Details of payments to be made were input into the NBS system by the account holder via Prestel. A cheque was then sent by NBS to the payee and an advice giving details of the payment was sent to the account holder. BACS was later used to transfer the payment directly.

Stanford Federal Credit Union was the first financial institution to offer online internet banking services to all of its members in October, 1994.

3.2 Features

Online banking solutions have many features and capabilities in common, but traditionally, it also have some that are application specific.

The common features fall broadly into several categories:

- Transactional (e.g., performing a financial transaction such as an account to account transfer, paying a bill, wire transfer and applications for a loan, new account, etc.)

- Electronic bill presentment and payment - EBPP
- Funds transfer between a customer's own checking and savings accounts, or to another customer's account
- Investment purchase or sale
- Loan applications and transactions, such as repayments
- Non-transactional (e.g., online statements, check links, cobrowsing, chat)
 - Bank statements
- Financial Institution Administration - features allowing the financial institution to manage the online experience of their end users
- ASP/Hosting Administration - features allowing the hosting company to administer the solution across financial institutions

Features commonly unique to business banking include:

- Support of multiple users having varying levels of authority
- Transaction approval process
- Wire transfer

Features commonly unique to Internet banking include:

- Personal financial management support, such as importing data into a personal finance program such as Quicken, Microsoft Money or TurboTax. Some online banking platforms support account aggregation to allow the customers to monitor all of their accounts in one place whether they are with their main bank or with other institutions...

3.3 Transition from Brick-to-Click Banks

Today, most large national banks, many regional banks and even smaller banks and credit unions offer some form of online banking, variously known as PC banking, home banking, electronic banking or Internet banking. Those that do are sometimes referred to as "brick-to-click" banks, both to distinguish them from brick-and-mortar banks that have yet to offer online banking, as well as from online or "virtual" banks that have no physical branches or tellers whatsoever.

The challenge for the banking industry has been to design this new service channel in such a way that its customers will readily learn to use and trust it. After all, banks have spent generations earning our trust; they aren't about to risk that on a Web site that is frustrating, confusing or less than secure.

Most of the large banks now offer fully secure, fully functional online banking for free or for a small fee. Some smaller banks offer limited

access or functionality; for instance, you may be able to view your account balance and history but not initiate transactions online. As more banks succeed online and more customers use their sites, fully functional online banking likely will become as commonplace as automated teller machines.

3.4 Statistics

Since March 2000, the Pew Internet and American Life project has tracked major activities undertaken by Internet users in the United States. Of the activities tracked by Pew, Internet banking has seen the greatest increase. In 2002, 30% of Internet users used Internet banking, compared to 42% in 2005 – an increase of 47%. Pew found several underlying factors contributed to the likelihood that Internet users would utilize online banking services. Internet users with higher-speed Internet connections were more likely to have used Internet banking (63% had done so) compared to those with dial-up connections (32% of whom had used Internet banking). Those with six or more years of experience online (51%) were also more likely to use Internet banking services, compared to those who had three or fewer years experience online (27%).

3.5 Activities

More and more banks are transforming their businesses by using Internet technology to develop or expand relationships with their customers. The extent to which the Internet is used in a bank depends on the relative maturity of the bank in regard to Internet technology. Banks offer Internet banking in two main ways. An existing bank with physical offices, ordinarily termed a brick-and-mortar bank, can establish a web site and offer Internet banking to its customers as an addition to its traditional delivery channels. An alternative is to establish either a virtual, branchless or Internet-only bank. The computer server or bank database that lies at the heart of a virtual bank may be housed in an office that serves as the legal address of such a bank or at some other location.

Virtual banks provide customers with the ability to make deposits and withdrawals via automated teller machines (ATMs) or through other remote delivery channels owned by other institutions. Characteristics of Internet banking include the unprecedented speed of change related to technological and customer service innovation, the ubiquitous and global nature of the Internet, the integration of Internet banking applications with legacy computer systems and the increasing dependence of banks on third parties that provide the necessary

information technology. Accordingly, a bank can perform Internet activities in one or more of the following ways:

- **Informational** - This is the basic level of Internet banking. Typically, the bank has marketing information about the bank's products and services on a stand-alone server. Risks associated with these operations are relatively low, as informational systems typically have no path between the server and the bank's internal network. This level of Internet banking can be provided by the bank or can be outsourced. While the risk to a bank is relatively low, the data on the server or web site may be vulnerable to alteration. Appropriate controls, therefore, must be in place to prevent unauthorised alterations of the data on the bank's server or web site.
- **Communicative** - This type of Internet banking system allows some interaction between the bank's systems and the customer. The interaction may be limited to electronic mail, account inquiry, loan applications or static file updates (name and address changes). Because these servers ordinarily have a direct path to the bank's internal networks, the operational risk is higher with this configuration than with informational systems. Controls should be in place to prevent, monitor and alert management of any unauthorised attempt to access the bank's internal networks and computer systems. Virus detection and prevention controls are also important in this environment.
- **Transactional** - This level of Internet banking allows customers to directly execute transactions with financial implications. There are two levels of transactional Internet banking, each with a different risk profile. The basic transactional site only allows a transfer of funds between the accounts of one customer and the bank. The advanced transactional site provides a means for generating payments directly to third parties outside of the bank. This can take the form of bill payments via a bank official check or electronic funds transfer/automated clearing house entries. Many banks are also offering payments from consumer to consumer using either payment method. When the transfers of funds are allowed to a point outside of the bank, the operational risk increases. Unauthorised access in this environment can lead or give rise to fraud. Since a communication path is typically complex and may include passing through several public servers, lines or devices between the customer's and the bank's internal networks, this is the highest risk architecture and must have the strongest controls.

3.6 Advantages

- **Convenience:** Unlike your corner bank, online banking sites never close; they're available 24 hours a day, seven days a week, and they're only a mouse click away.
- **Ubiquity:** If you're out of state or even out of the country when a money problem arises, you can log on instantly to your online bank and take care of business, 24/7.
- **Transaction speed:** Online bank sites generally execute and confirm transactions at or quicker than ATM processing speeds.
- **Efficiency:** You can access and manage all of your bank accounts, including IRAs, CDs, even securities, from one secure site.
- **Effectiveness:** Many online banking sites now offer sophisticated tools, including account aggregation, stock quotes, rate alerts and portfolio managing programs to help you manage all of your assets more effectively. Most are also compatible with money managing programs such as Quicken and Microsoft Money.

3.7 Disadvantages

- **Start-up may take time:** In order to register for your bank's online program, you will probably have to provide an identification card and sign a form at a bank's branch. If you and your spouse wish to view and manage your assets together online, one of you may have to sign a durable power of attorney before the bank will display all of your holdings together.
- **Learning curve:** Banking sites can be difficult to navigate at first. Plan to invest some time and/or read the tutorials in order to become comfortable in your virtual lobby.
- **Bank site changes:** Even the largest banks periodically upgrade their online programs, adding new features in unfamiliar places. In some cases, you may have to re-enter account information.
- **The trust thing:** For many people, the biggest hurdle to online banking is learning to trust it. Did my transaction go through? Did I push the transfer button once or twice? Best bet: always print the transaction receipt and keep it with your bank records until it shows up on your personal site and/or your bank statement.

3.8 Risk and Threat

Banking by its very nature, is a high-risk business. The major risks associated with banking activities are: strategic, reputational, and operational (including security - sometimes called transactional - and legal risks), credit, price, foreign exchange, interest rate and liquidity. Internet banking activities do not raise risks that were not already identified in traditional banking, but it increases and modifies some of these traditional risks. The core business and the information technology environment are tightly coupled, thereby influencing the overall risk

profile of Internet banking. In particular, from the perspective of the IS auditor, the main issues are strategic, operational and reputational risk, as these are directly related to threats to reliable data flow and are heightened by the rapid introduction and underlying technological complexity of Internet banking. Banks should have a risk management process to enable them to identify measure, monitor and control their technology risk exposure. Risk management of new technologies has three essential elements:

1. Risk management is the responsibility of the board of directors and senior management. They are responsible for developing the bank's business strategy and establishing an effective risk management methodology. They need to possess the knowledge and skills to manage the bank's use of Internet banking and all related risks. The board should make an explicit, informed and documented strategic decision as to whether and how the bank is to provide Internet banking services. The initial decision should include the specific accountabilities, policies and controls to address risks, including those arising in a cross-border context. The board should review, approve and monitor Internet banking technology-related projects that have a significant effect on the bank's risk profile and ensure that adequate controls are identified, planned and implemented.
2. Implementing technology is the responsibility of information technology senior management. They should have the skills to effectively evaluate Internet banking technologies and products, and to ensure that they are installed and documented appropriately. If the bank does not have the expertise to fulfill this responsibility internally, it should consider contracting with a vendor who specializes in this type of business or engaging in an alliance with another third party with complementary technologies or expertise.
3. Measuring and monitoring risk is the responsibility of operational management. They should have the skills to effectively identify, measure, monitor and control risks associated with Internet banking. The board of directors should receive regular reports on the technologies employed, the risks assumed, and how those risks are managed.

While the Internet has provided consumers with the conveniences associated with online banking, several threats have also emerged. In particular, consumers are increasingly concerned about phishing and identity theft (Abad, 2005). A 2004 study by the Federal Deposit Insurance Corporation (FDIC) examined the incidence of unauthorized access to financial institution accounts, as well as proposing how such risks could be mitigated. Unauthorized access to accounts occurs

through identity theft of one form of another. In this regard the FDIC report examined the “account hijacking”, defined as “unauthorized access to and misuse of existing asset accounts primarily through phishing and hacking” It was estimated that around two million adult Internet users had their checking accounts hijacked in the 12 months ending April 2004. 70% of those individuals did their banking and/or billpaying online and over half believed that they had received a phishing e-mail. Herein lays the major way in which users of online financial services appear to be subject to fraud. In the context of our discussion, phishing involves attempts to get account holders to disclose private information to illegitimate third-parties. Typically, the account holder will receive an e-mail claiming to be from their financial institution, requesting that they verify certain account. The e-mail will invariably contain a link to a “spoof” web-site – designed to appear as if it belongs to a legitimate financial institution. On this website account holder are asked to provide sensitive personal information such as their Social Security Number, account and credit card numbers, names and account passwords. This information is then stolen and used by the illegitimate third party to gain access to the account(s) of the individual who entered the information.

3.9 Security

Protection through single password authentication, as is the case in most secure Internet shopping sites, is not considered secure enough for personal online banking applications in some countries. Basically there exist two different security methods for online banking.

- The PIN/TAN system where the PIN represents a password, used for the login and TANs representing one-time passwords to authenticate transactions. TANs can be distributed in different ways, the most popular one is to send a list of TANs to the online banking user by postal letter. The most secure way of using TANs is to generate them by need using a security token. These token generated TANs depend on the time and a unique secret, stored in the security token (this is called two-factor authentication or 2FA). Usually online banking with PIN/TAN is done via a web browser using SSL secured connections, so that there is no additional encryption needed.
- Signature based online banking where all transactions are signed and encrypted digitally. The Keys for the signature generation and encryption can be stored on smartcards or any memory medium, depending on the concrete implementation.

Attacks

Most of the attacks on online banking used today are based on deceiving the user to steal login data and valid TANs. Two well known examples

for those attacks are phishing and pharming. Cross-site scripting and keylogger/Trojan horses can also be used to steal login information.

A method to attack signature based online banking methods is to manipulate the used software in a way, that correct transactions are shown on the screen and faked transactions are signed in the background.

A recent FDIC Technology Incident Report, compiled from suspicious activity reports banks file quarterly, lists 536 cases of computer intrusion, with an average loss per incident of \$30,000. That adds up to a nearly \$16-million loss in the second quarter of 2007. Computer intrusions increased by 150 percent between the first quarter of 2007 and the second. In 80 percent of the cases, the source of the intrusion is unknown but it occurred during online banking, the report states.

3.10 Security Measures

There exist several countermeasures which try to avoid attacks. Digital certificates are used against phishing and pharming, the use of class-3 card readers is a measure to avoid manipulation of transactions by the software in signature based online banking variants. To protect their systems against Trojan horses, users should use virus scanners and be careful with downloaded software or e-mail attachments.

In 2001, the FFIEC issued guidance for multifactor authentication (MFA) and then required to be in place by the end of 2006.

Various measures have been proposed to combat account hijacking. The FDIC report proposed the following five steps for financial institutions and government to reduce online fraud:

1. Upgrading existing password-based single-factor customer authentication systems to two-factor authentication. Two-factor authentication requires users to submit two of three sorts of credentials, e.g., two of something a person knows, something a person has, or something a person is. Passwords are examples of something a person knows, physical cards are an example of something a person has, and biometric identification is an example of something a person is].
2. Using scanning software to proactively identify and defend against phishing attacks. The further development and use of fraud detection software to identify account hijacking, similar to existing software that detects credit card fraud, could also help to reduce account hijacking.

3. Strengthening educational programs to help consumers avoid online scams, such as phishing, that can lead to account hijacking and other forms of identity theft and take appropriate action to limit their liability.
4. Placing a continuing emphasis on information sharing among the financial services industry, government, and technology providers.

In contrast, the report by the FBIIC and FSSCC proposed eight steps for financial institutions to avoid having their customers fall victim to phishing:

- Personalize e-mails to consumers so that consumers have a greater assurance of the e-mail's legitimacy.
- Remind consumers on your website that you will never send them an email asking them to come to your website to enter personal information.
- Set up your loan application websites so that current customers do not have to enter Social Security numbers and other personal information that you already have on file.
- Keep website certificates up to date so that consumers are assured of the site's legitimacy.
- Remind consumers to obtain and use the latest patch for their web browser and operating system software.
- Provide on company or agency websites a domestic telephone number for consumers to call to verify e-mail requests for information.
- Register domain names that are similar to the name of the firm or agency so that consumers are less likely to confuse a false website with the legitimate website. Practice consistent branding.
- Consider establishing a trademark for the domain name of the firm. Under the Anticybersquatting Consumer Protection Act, 15 U.S.C. 1125(d), a firm may be able to initiate immediate action in Federal district court against the suspicious website to protect the firm's trademark.

In the light of problems associated with identity theft over the Internet, it is hardly surprising that increasing attention is being paid to alternative forms of identity verification - particularly biometrics.

“Biometrics are technologies that automatically confirm the identity of people by comparing patterns of physical or behavioral characteristics in real time against enrolled computer records of those patterns. Leading biometric technologies accomplish this task by scanning patterns of the face, fingerprint, hand, iris, palm, signature, skin, or voice.” (International Biometric Industry Association)

At present, biometric forms of identification appear to be more commonplace in non-U.S. financial institutions (Krebsbach, 2004). Choices about adoption of biometric security solutions will be influenced by considerations such as: the level of security required, accuracy, cost and implementation time, and user acceptance (findBiometrics.com). As the biometrics industry progresses (in particular as accuracy increases, costs decline and user acceptance increases) we are likely to see increasing use biometric technologies to thwart attempts by identity thieves

4.0 CONCLUSION

Internet banking is certainly one of the great things that has happened to the global financial institution and its services recently. It has brought about ease in banking. Though it seemed, initially, not to be feasible because of both the technological and security challenges, it has come to stay. One may not say all is well with internet banking especially in terms of its exposure to large scale fraud, but efforts are being made to counter the challenges. I think the advantages far out ways the disadvantages.

5.0 SUMMARY

- Online banking (or Internet banking) allows customers to conduct financial transactions on a secure website operated by their retail or virtual bank, credit union or building society.
- The precursor for the modern home online banking services were the distance banking services over electronic media from the early '80s.
- Online banking solutions have many features and capabilities in common, but traditionally also have some that are application specific.
- Today, most large national banks, many regional banks and even smaller banks and credit unions offer some form of online banking, variously known as PC banking, home banking, electronic banking or Internet banking.
- In 2002, 30% of Internet users used Internet banking, compared to 42% in 2005 – an increase of 47%.
- More and more banks are transforming their businesses by using Internet technology to develop or expand relationships with their customers
- Unlike your corner bank, online banking sites never close; they're available 24 hours a day, seven days a week, and they're only a mouse click away.
- In order to register for your bank's online program, you will probably have to provide ID and sign a form at a bank branch.

- Banking by its very nature, is a high-risk business. The major risks associated with banking activities are: strategic, reputational, operational (including security - sometimes called transactional - and legal risks), credit, price, foreign exchange, interest rate and liquidity
- Protection through single password authentication, as is the case in most secure Internet shopping sites, is not considered secure enough for personal online banking applications in some countries. Basically there exist two different security methods for online banking
- There exist several countermeasures which try to avoid attacks. Digital certificates are used against phishing and pharming, the use of class-3 card readers is a measure to avoid manipulation of transactions by the software in signature based online banking variants.

6.0 TUTOR-MARKED ASSIGNMENT

1. Mention 5 features of transactional Internet banking
2. Briefly discuss the disadvantages of Internet/Online banking

7.0 REFERENCES/FURTHER READING

Cronin, Mary J. (1997). *Banking and Finance on the Internet*, John Wiley and Sons.

A transaction document DL34/01/84 used by the Nottingham Building Society has a printed footnote: 'HOMELINK - The world's first electronic Building Society Service operated from the customer's home - is available through Nottingham Building Society in association with British Telecom and the Bank of Scotland. Homelink is a Trade Mark of Nottingham Building Society'

"Stanford Federal Credit Union Pioneers Online Financial Services". Retrieved on 2007-12-14.

'Security Flaws in Online Banking Sites Found to be Widespread'
Newswise.

MODULE 2

Unit 1	Supervision and Regulation of E-Banking
Unit 2	Auditing Guideline for E- Banking
Unit 3	Mobile E-Banking
Unit 4	Electronic Payment Systems
Unit 5	Automated Teller Machine

UNIT 1 SUPERVISION AND REGULATION OF E-BANKING

CONTENTS

- 1.0 Introduction
- 2.0 Objectives
- 3.0 Main Content
 - 3.1 Network (Internet) Banks
 - 3.2 Banking Regulations
 - 3.3 Supervision and Regulation of Internet Banks
- 4.0 Conclusion
- 5.0 Summary
- 6.0 Tutor-Marked Assignment
- 7.0 References/Further Reading
- 1.0 INTRODUCTION**

Public computer networks, in particular the Internet, have the potential to transform the financial services sector by providing a fast, cheap way to sell financial services. Low setup costs and the transnationality of the Internet could remove significant barriers to entry in the financial services industry. Cross-border provision of services and the high mobility of network banks could challenge the ability of national and international authorities to establish and enforce banking regulations. This unit considers the supervision and regulation of banks providing financial services on public computer networks for the mass retail market, i.e., deposit taking and lending of money on retail and small- and medium-size company markets.

The Internet's explosive growth has initiated considerable activity in the financial services industry. For this industry, the Internet and, in particular, the World Wide Web, serve as a new *vehicle* for transmitting financial information, comparable to the invention of the telegraph 150 years ago and its use for transmitting financial information. Although computer networks only transport financial information, many predict radical changes including the "dissolution of geographic markets into virtual financial systems" and the "loss of national independence." These predictions are simplistic and are not based on analyzing this issue. However, the facts are (a) financial services are *information commodities* and (b) public computer networks offer a fast, cheap way to trade information. Public computer networks can radically improve efficiency and competition in the financial services sector. Increased efficiency and competition rely on three characteristics of these networks:

- *Marginal costs* of selling financial information over computer networks are small - in fact, typically negligible - compared with more traditional information channels;

- Public computer networks are essentially *borderless*, giving rise to the cross-border provision of financial services;
- Setup costs to establish a financial services business on a public computer network are small, which increases the *contestability* of financial services markets.

Considering these characteristics, public computer networks would affect *banking competition* and *banking regulation*. While the small setup costs and the cross-border provision of financial services would spur competition, it is the Internet's borderless nature that could pose a major challenge for the regulation and supervision of financial intermediaries.

The *mass retail market*, i.e., deposits taking and the lending of money on retail and small- and medium-size company markets could be affected most. The retail sector, so far, has been less affected by telecommunication technology than have other financial sectors and the mass retail market has remained largely a national business. In contrast, large corporate banking is already international and the cross-border provision of financial services in these markets is the rule rather than the exception. The prospect of an international mass retail market for financial services is a likely candidate for public concern and intervention because regulatory efforts are often directed toward protecting small depositors.

In this unit, the first section on Network banks distinguishes network retail banking and “traditional” retail banking; the second section on banking regulation identifies the need for public intervention in the banking industry; and the third section examines supervision and regulation of network banks.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

- learn how public networks can improve efficiencies in financial services
- follow the development of network banks
- understand what constitutes banking regulation
- understand how to supervise and regulate Internet banks.

3.0 MAIN CONTENT

3.1 Network (Internet) Banks

Exponential growth of the Internet started when the World Wide Web was invented in the early 1990s. The emergence of financial service providers on the World Wide Web is more recent. Security First Network Bank in Atlanta, Georgia, was the first bank to use the Web as its main channel for offering traditional financial services, such as transaction accounts. The bank opened its business on October 18, 1995.

Despite its youth, the Web has initiated many activities in the financial services industry; in December 1996, more than 1,490 banking institutions were providing financial information on it. There is also a growing demand for online financial services. For example, Wells Fargo in San Francisco increased its online banking base from 20,000 to 270,000 users in 18 months.

Because banking on the Internet is so new, no systematic research on Internet-based financial services and their economic implications is available. Existing literature consists entirely of anecdotal evidence from individual companies, usually in trade journal articles with no empirical basis (Kalakota 1996). Moreover, there exists no research on the prudential regulation of network banks.

Analysis of network banks and their regulation must start with identifying the characteristics distinguishing network banking from traditional banking. Our main proposition is that in the relation between network banks and customers the physical location of the network bank or the customer plays no role. We term this fact the *irrelevance of physical location*. In all other respects network banking works like traditional retail banking. In particular, they could provide the same services: facilitating transactions, portfolio management, risk transformation, and monitoring

The irrelevance of physical location is based on the fact that marginal costs of providing financial services on a public computer network are not related to a customer's location; more importantly, a customer's marginal costs for obtaining financial services are independent of the bank's location. In contrast, the "traditional" retail bank location is an important (cost) factor for bank customers and banks. In "traditional banking" a customer's marginal costs for obtaining financial services increase with distance to his bank. Consequently, traditional banks compete for location and (over) invest in branches and ATM-systems to collect deposits (Neven, 1990).

The irrelevance of the physical location has two implications. First, it enables cross-border trade of financial services in the retail market. Without legal restrictions, agents can shop for financial services anywhere on this planet as long as the network bank has access to a

local ATM network to obtain cash. However, the emergence of electronic money, respectively digital cash, could even remove this requirement. White (1996) has stressed this fact:

- What strikes me as the most exciting potential development to come from the new payment technologies is that, as they lower the cost of wiring money from \$20 to 2 cents or less per transaction, they give ordinary small savers affordable access to offshore banking. With direct deposit of paychecks and with analog currency available at ATMs whenever we want it, many of us no longer need to visit our bank in person. Why not keep your accounts with a reputable bank (perhaps a branch of a major Swiss bank) in the Bahamas or Cayman Islands?

Second, network banks can move their physical location without changing their relation to their customers. In particular, they can move their business across nations “overnight”. Thus, network banks can react faster than traditional banks to changing economic conditions and regulatory requirements. For example, they can easily shift their production to low factor cost countries and nations with inexpensive regulatory regimes.

3.2 Banking Regulations

Any attempt to understand the prudential regulation of banks requires examining the nature of financial intermediation, the potential for market failures, and the attempt to correct these failures through public intervention. The theory of financial intermediation stresses four functions of financial intermediaries:

- facilitating transactions
- portfolio management
- risk transformation, and
- monitoring.

According to the first function, financial intermediaries facilitate transactions by organizing the payment system. They offer check clearing and payment products such as credit cards, debit cards, and travelers’ checks. The second function, portfolio management, refers to the management of diversified portfolios consisting of financial liabilities issued by firms and governments and sold to the public. The third function, risk transformation, refers to the transformation of risky assets issued by firms into fixed interest deposits demanded by households and to the transformation of illiquid assets into liquid liabilities to provide liquidity insurance to households. The fourth function, monitoring, refers to monitoring activities of financial

intermediaries, which reduces problems of moral hazard and asymmetric information in relation between firms and financiers (Hellwig, 1991).

Banking regulation theory is closely linked to these functions. The issue is twofold:

- Which functions, if any, justify public intervention?
- If intervention is justified, what kinds of regulations are appropriate?

It is commonly accepted that any banking regulation must rely on some form of market failure. If banks were only to offer transaction and portfolio management services, regulations would be unnecessary. Fama (1980) demonstrates that these two functions do not cause market failures. The potential for market failures is associated with the third and fourth functions. Particularly, it is the financing of illiquid assets with short-term deposits and the potential of bank runs that create a need for public intervention and the establishment of a safety net to guarantee the stability of the financial system (Baltensperger and Dermine, 1990).

Diamond and Dybvig's (1983) were the first to model bank runs. Their model suggests an equilibrium in which all depositors try to close their accounts, forcing the bank to sell illiquid assets, resulting in the failure of the otherwise solvent bank. The interesting aspect of their model is that there is no underlying real reason for the bank run: the illiquid asset is a completely safe investment. It is the expectation about the behavior of other depositors that drives the behavior of any individual. In the bank run equilibrium, these expectations are fulfilled.

A related type of market failure stresses the "contagious" nature of bank runs (Baltensperger and Dermine, 1987). A bank failure can trigger a run on other, solvent banks when bank customers of the solvent bank assume that the value of banks assets are highly correlated with each other. In most countries there exists a public deposit insurance or a lender-of-last-resort agency to prevent bank runs. Deposit insurance makes deposits risk-free, thereby eliminating the incentive for early withdrawals.

An additional basis for market failures is asymmetric information between banks and their depositors. Banks are better informed about the quality of their loans and the security of their assets than depositors are. Depositors can improve their information by monitoring banks; monitoring bank solvency, however, is expensive and requires skills small depositors may not have. In addition, information about bank solvency has the characteristic of a public good. This view is emphasized in Dewatripont and Tirole (1992, p. 17):

- One neglected, although certainly quantitatively important, feature of banks [is] the dispersed nature of the debt-holders or depositors. Small depositors typically have no time or expertise to perform the monitoring and control that the optimal governance structure [-] requires. And even if they did, they would be tempted to free ride on each other's monitoring and exercise of control.

According to Dewatripont and Tirole (1992), when a bank is in trouble, bank managers and equity holders have an incentive to *gamble for resurrection*. As a consequence, debt holders of banks, i.e., depositors, must take control when bank performance is bad because their incentives are to limit risk taking. A large number of small free-riding depositors, however, cannot perform this task, which suggests a role for public intervention. A public agency would have to regulate banks ex-ante by imposing capital requirements and limiting the growth of deposits. In addition, a public agency would have to intervene ex post acting on behalf of small depositors in bad times.

In summary, modern theory of financial intermediation suggests two reasons for public intervention:

- The possibility of bank runs.
- Asymmetric information between banks and a larger number of small depositors who are free-riding on each other's monitoring and exercise of control.

A final note is required, here. Any banking regulation induces unwanted side effects. For example, deposit insurance that prevents bank runs lowers the incentives of banks to invest prudentially. The U. S. deposit insurance system, for example, is blamed for hundreds of billions of dollars of taxpayers' losses by creating moral hazards. Deposit insurance lowers the reputation-building incentives of financial institutions. As a consequence, financial institutions are likely to take more risks and to monitor less than with no deposit insurance. Present regulatory theory does not offer clear-cut recommendations, owing to the complexity of the welfare analysis (Vives, 1991). It is therefore important to balance carefully the benefits of any regulation versus the potential for harmful side effects. This issue is constantly under debate and opinions of the profession disagree widely.

3.3 Supervision and Regulation of Internet Banks

Here, we consider whether network banks provide additional reasons for public intervention and whether they require different treatments. In the first section of this paper we noted that in the relationship between the network bank and the customer the physical location of either party is

irrelevant. In second section, we identified two reasons for public intervention: bank runs and the asymmetric information between banks and their depositors. Here, we identify three questions with regard to the supervision and regulation of network banks. The questions are not outlined in detail. They should be read with the previous discussion in mind.

Could the provision of financial services via public computer networks increase the need for banking regulation and supervision?

An increase in public intervention would be necessary if network banks were more vulnerable to bank failures, bank runs, and systemic risks. Consider the potential for bank runs first. Network bank are more vulnerable to bank runs for the following reasons:

- Information and rumors spread quickly across the Internet. The rapid spread of information is most relevant for so-called *fundamental or information-based bank runs*. In a fundamental bank run depositors realize that the value of assets in the bank is low and that withdrawing is the dominant strategy (Vives, 1991). The rapid spread of rumors could also increase the potential for *panic bank runs*, which are unrelated to any fundamentals. This issue reminds us of the many virus alerts that sweep through the Internet. For example, postings on the Internet about a plain electronic mail message that, when opened, erases all files on the reader's hard disk induces panic; in reality it is not possible to get infected by just a plain e-mail message (although attachments can carry all sorts of troubles).
- Public computer networks provide fast access of depositors to their accounts. With the push of a button, agents can transfer money from one account to another and from one bank to another bank. As a consequence, during a bank run a network bank has less time to react appropriately and to take necessary measures, such as liquidating assets, to prevent the bank failure.
- Fast access to a bank and the rapid spread of rumors and information also make network banks more vulnerable to the contagious nature of bank runs. Information about the failure of one bank can trigger runs on other solvent network banks. Again, network banking could increase the speed of such events, thereby reducing the ability of banks and governmental officials to react in a timely manner.
- Security concerns are the main reason for banks' cautious approach toward banking on the Internet. At the initial stage, before network banks mature, breach of security could be a major source for instability and bank runs. Depositors could react very sensitive to any news or rumors that affect their wealth.

The second reason for market failures is asymmetric information between bank and a large number of free-riding depositors and the incentives of bank management and equity holders to gamble for resurrection when the bank is in trouble.

- To be able to gamble for resurrection, bank managers and equity holders try to avoid outside interference. Manipulating performance measures and gains trading is one way to do this (Dewatripont and Tirole, 1993). For example, the bank in trouble could sell undervalued assets even though it would be profitable to keep them. Network banks have an additional means to avoid outside interference: they can move or credibly threaten to move their business to a location where public authorities are less likely to intervene. In fact, the sheer threat of dislocation could soften governmental authorities.
- The high level of anonymity between bank customer and network bank could increase the difficulties of depositors to monitor banks. Moreover, network banking could increase dispersion of depositors, which could increase further the difficulties of depositors to monitor and exercise control when the bank is in trouble.

In summary, network banks are more vulnerable to bank runs because news and rumors spread quickly over public computer networks. The main source of instability could be security problems. Network banks have also more options to avoid outside interference in order to gamble for resurrection because they can credibly threaten to move their business. As a consequence, network banks should be regulated and supervised at least to the same degree as ordinary banks. In the initial stage, before network banking matures, the potential for bank runs suggests that governmental authorities should monitor network banks as closely as possible and provide information to the public. This would be also to the advantage of network banks because it would give the public more confidence to use these banks, which in turn would help network banking to take off.

A final note is required here. Although network banks are more vulnerable to bank runs and the gamble for resurrection problem, network banking provides no *new, previously unknown* type of market failure. Network banking does not fundamentally alter the characteristics of banking; network banks provide the same financial services and are in all respects ordinary firms with management, equity holders and debt holders.

How does the international dimension of network banking potentially affect supervision and regulation?

Existing regulations for retail banking, deposit insurance, and lender-of-last-resort facilities are designed to deal with domestic or branches of foreign retail banks with domestic depositors. In first section of this paper we concluded that a customer's marginal costs of buying financial services are independent of the network bank's physical location. Thus, in the absence of legal restrictions, network banks could attract a large number of foreign customers, giving rise to the following issues for supervision and regulation:

- For many types of cross-border financial services, it is unclear which nations' regulations would apply, leaving unresolved and nebulous legal issues regarding network banking.
- Regulatory regimes of different countries compete with each other. Restrictive regulations hurt local financial institutions and they lose business to financial intermediaries elsewhere. Thus, "soft" countries can attract foreign customers. The retail sector has so far been less affected by these developments because the costs of offshore banking for small depositors have been too high. Network banking could reduce these costs enough to make offshore banking profitable for small depositors and increase the pressure to soften regulations in the retail sector.
- Regulatory regimes not only compete for customers but also for financial institutions. Thus, a "soft" country could attract financial intermediaries to settle down in its jurisdiction. The sheer threat of loosing banks could prevent implementation and rigorous enforcement of regulations in the retail sector.

Who will regulate and supervise network banks operating in various countries?

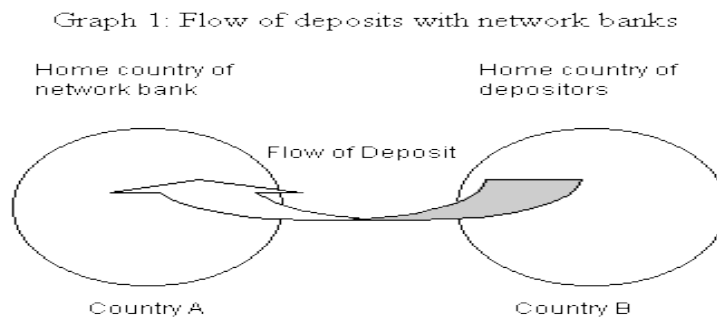
According to Baltensperger and Dermine (1990, p. 18) international banking raises two specific issues:

- The first concerns supervision and regulation. Does domestic regulation apply to other banks operating in the country ("national treatment principle") or does it apply to the foreign component of domestic banks ("home country principle")? The second issue concerns the extent of responsibility of the domestic lender of the last resort and of the domestic insurance system. Do they cover branches or subsidiaries of domestic banks operating abroad? Do they cover branches and subsidiaries of foreign banks operating domestically?

In the international banking context, one specific issue is to determine which country is responsible for regulating and supervising of foreign branches of banks. The United State, for example, applies the "national

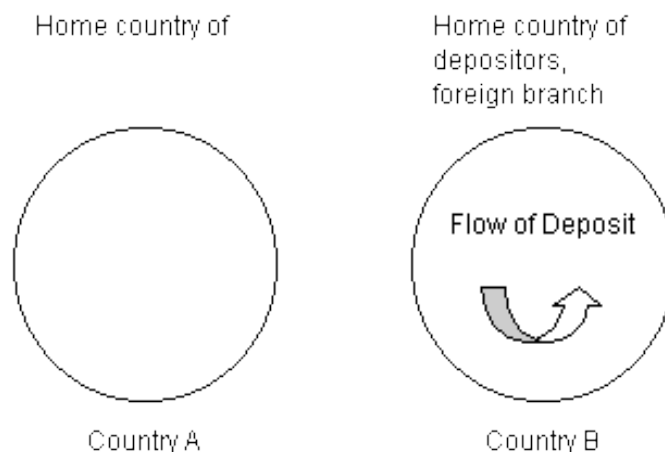
treatment” principle to foreign banking organizations operating in its jurisdiction. In contrast, the European Commission has opted for the “home country principal.”

Network banking and international banking differ in one important respect: *network banks do not establish branches*. Consequently, regulators of network banks face a different problem. They would either have to supervise and regulate banks in their jurisdiction that mainly attract funds and lend to foreign residents. Or, they would have to supervise and regulate network banks established in a foreign country with a large number of domestic customers. Thus, the question is: who is going to regulate a network bank with mostly foreign customers? The difference between international banking and network banking is depicted in Graph 1 and Graph 2 below.



Graph 1 shows the flow of deposits when residents of country B are customers of a network bank located in country A. There is a cross-border flow of deposits from country B to country A.

Graph 2: Flow of deposits with “traditional” banks



In contrast, in international banking, as shown in Graph 2, the “traditional” retail bank, located in country A, establishes a branch in

country B and attracts deposits of residents of country B. Consequently, there is no cross-border flow of deposits.

In the context of network banking, the problem is to determine which country - in terms of efficiency - is responsible for supervising and regulating a network bank that attracts mostly small depositors and borrowers from abroad. A related question is: which country should provide the safety net? For example, will it be necessary and, if so, feasible to insure a large number of citizens who have uninsured deposits abroad?

When a domestic network bank has mostly foreign depositors, the incentives of domestic regulators to supervise the bank or to step in and provide lender-of-last-resort assistance when the bank is in trouble could be affected. Consider, for example, a Swiss network bank that attracts a large number of small German depositors and borrowers. When the banks fail, the Germans would be hurt while Switzerland's reputation as a safe haven would suffer. If the bank were sufficiently large, both countries would have an incentive to step in as a lender of last resort. However, the German Bundesbank would prefer the Swiss National Bank to do the dirty work and the Swiss National Bank would like to see the German Bundesbank step in. In contrast, consider the failure of a Swiss bank subsidiary operating in Germany. The failure of this bank would hurt not only German customers but also German's reputation as a safe haven. It would also, but to a lesser extent, damage Switzerland's reputation for secure investments.

While this is an extreme example, it shows that the incentives of regulators and lender-of-last-resort agencies could respond differently when a bank's customer base consists mainly of foreign residents. It also shows that supervision and regulation of network banks is inherently an international policy issue. To create a stable financial environment, international coordination is essential.

4.0 CONCLUSION

The Internet, particularly the World Wide Web, is changing our lives. Public computer networks are part of today's technology that drives the information revolution - an analogy to the industrial revolution of two centuries ago. This analogy stresses the common feeling that some significant and exciting developments are underway. The financial sector could be radically changed by information technologies, and public computer networks could play a major role in this turmoil. The financial services sector could be affected comparably more than any other sector in the economy because financial services are *information commodities* which can be easily traded on public computer networks.

Two results emerge from this analysis.

- Electronic banks are more vulnerable to bank runs and the “gamble for resurrection” problem. Bank runs are more likely because news and rumors spread quickly across public computer networks and depositors can transfer funds with the push of a button. Consequently, a bank facing a bank run and public regulatory agencies have less time to take appropriate measures to prevent the bank’s failure. At the initial stage, before network banking majors, security problems could be a major source for instability. The “gamble for resurrection” problem is aggravated because bank managers who want to avoid outside interference can credibly threaten to move their business to another jurisdiction. This credible threat could make public agencies “soft” and lower their incentives to intervene or close an insolvent bank when it is optimal to do so.
- The transnationality of network banks could increase the difficulty of enforcing national and supranational banking regulations for the following reasons. First, for many types of cross-border financial services it would be unclear as of which nation's regulations apply. Second, regulatory regimes for different countries compete with each other. Thus, a “soft” country can attract customers and financial institutions. Third, the incentives to supervise, regulate, and provide the safety net for network banks could be affected when the bank's customer base consists mainly of foreign residents.

A major conclusion of the banking literature is that the need for public intervention comes from the potential instability of banking markets (Baltensperger and Dermine, 1990). Lack of enforcement and lack of adequate regulations could adversely affect the financial system's stability. Despite its importance, there exists *no systematic research* on the economic implications of financial intermediation on public computer networks. This paper is a first incomplete step in analyzing the economic implications of network banks. Further analysis will be valuable in identifying emerging problems, and it will be a base for future policy recommendations. In particular, the emergence of network banks requires revision of current national and international banking regulations. It is important that new regulations be based on reliable analysis to avoid either overreaction that would stifle these innovations or neglect the potential for instability in the world of banking.

5.0 SUMMARY

- Public computer networks, in particular the Internet, have the potential to transform the financial services sector by providing a fast, cheap way to sell financial services. Low setup costs and the

transnationality of the Internet could remove significant barriers to entry in the financial services industry.

- Exponential growth of the Internet started when the World Wide Web was invented in the early 1990s. The emergence of financial service providers on the World Wide Web is more recent. Security First Network Bank in Atlanta, Georgia, was the first bank to use the Web as its main channel for offering traditional financial services, such as transaction accounts
- Any attempt to understand the prudential regulation of banks requires examining the nature of financial intermediation, the potential for market failures, and the attempt to correct these failures through public intervention.
- Network banking and international banking differ in one important respect: *network banks do not establish branches*. Consequently, regulators of network banks face a different problem.
- Another reason for market failures is asymmetric information between bank and a large number of free-riding depositors and the incentives of bank management and equity holders to gamble for resurrection when the bank is in trouble.
- An increase in public intervention would be necessary if network banks were more vulnerable to bank failures, bank runs, and systemic risks. Consider the potential for bank runs first.

6.0 TUTOR-MARKED ASSIGNMENT

1. Discuss briefly the 3 major characteristics of public networks that enhance their use in e-banking
2. Mention 4 functions of financial intermediaries

7.0 REFERENCES/FURTHER READING

See, Baltensperger and Dermine (1987; Dewatripont and Tirole (1994), and Vives (1991). *For a Recent Survey of Modern Banking Theory Literature*, consider Bhattacharaya and Thakor (1993).

Baltensperger E. and J. Dermine, (1987). "Banking Deregulation in Europe," *Economic Policy*, Volume 2, number 4, pp. 63-109.

Baltensperger E. and J. Dermine, (1990). "European Banking, Prudential and Regulatory Issues," In: J. Dermine, (ed.), *European Banking in the 1990s*. Oxford: Basil Blackwell.

Bhattacharaya S. and A. Thakor, (1993). "Contemporary Banking Theory," *Journal of Financial Intermediation*, Volume 3, pp. 2-50.

- Dewatripont M. and J. Tirole, (1993). "Efficient Governance Structure: Implications for Banking Regulation," In: C. Mayer and X. Vives, (eds.), *Capital Markets and Financial Intermediation*. New York: Cambridge University Press.
- Dewatripont M. and J. Tirole, (1994). *The Prudential Regulation of Banks*. Cambridge, Mass.: MIT Press.
- Diamond D. and P. Dybvig, (1983). "Bank Runs, Deposit Insurance, and Liquidity," *Journal of Political Economy*, Volume 91, pp. 401-19.
- Fama, E. 1980. "Banking in the Theory of Finance," *Journal of Monetary Economics*, Volume 6, pp. 39-57.
- Hellwig, M. (1991). "Banking, Financial Intermediation and Corporate Finance," In: A. Giovannini and C. Mayer, (eds.), *European Financial Integration*. New York: Cambridge University Press.
- Kalakota, R. (1996). *The Impact of Cybercommunications on Traditional Financial Services*
- Neven, D. (1990). "Structural Adjustment in European Retail Banking: Some Views from Industrial Organization," In: J. Dermine, (ed.), *European Banking in the 1990s* Oxford: Basil Blackwell.
- Vives, X. (1991). "Banking Competition and European Integration," In: Giovannini and C. Mayer, (eds.), *European Financial Integration*. New York: Cambridge University Press.
- White, L. H. (1996). "The Technology Revolution and Monetary Evolution," In: *The Future of Money in the Information Age*. Cato Institute's 14th Annual Monetary Conference,

COURSE CODE
635

BHM

UNIT 2 AUDITING GUIDELINE FOR E- BANKING

CONTENTS

- 1.0 Introduction
- 2.0 Objectives
- 3.0 Main Content
 - 3.1 Internet Control
 - 3.2 Independence
 - 3.3 Competence
 - 3.4 Planning
 - 3.5 Performance of Internet Banking Review
 - 3.6 Reporting
- 4.0 Conclusion
- 5.0 Summary
- 6.0 Tutor-Marked Assignment
- 7.0 References/Further Reading

1.0 INTRODUCTION

Linkage to ISACA Standards

Standard S2 Independence states, “The IS audit function should be independent of the area or activity being reviewed to permit objective completion of the audit assignment.”

Standard S4 Professional Competence states, “The IS auditor should be technically competent, having the skills and knowledge to conduct the audit assignment.”

Standard S5 Planning states, “The IS auditor should plan the information systems audit coverage to address the audit objectives and to comply with applicable laws and professional auditing standards.”

Standard S6 Performance of Audit Work states, “During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence.”

Guideline G22 Business to Consumer E-commerce Reviews provides guidance.

Procedure P3 Intrusion Detection System Review provides guidance.

Procedure P2 Digital Signatures and Key Management provides guidance.

Linkage to COBIT

The COBIT Framework states, “It is management’s responsibility to safeguard all the assets of the enterprise. To discharge this responsibility, as well as to achieve its expectations, management must establish an adequate system of internal control.”

The COBIT Management Guidelines provide a management-oriented framework for continuous and proactive control self-assessment specifically focused on:

- Performance measurement—How well is the IT function supporting business requirements?
- IT control profiling—What IT processes are important? What are the critical success factors for control?
- Awareness—What are the risks of not achieving the objectives?
- Benchmarking—What do others do? How can results be measured and compared?

The Management Guidelines provide example metrics enabling assessment of IT performance in business terms. The key goal indicators identify and measure outcomes of IT processes and the key performance indicators assess how well the processes are performing by measuring the enablers of the process. Maturity models and maturity attributes provide for capability assessments and benchmarking, helping management to measure control capability and to identify control gaps and strategies for improvement.

The Management Guidelines can be used to support self-assessment workshops, and they also can be used to support the implementation by management of continuous monitoring and improvement procedures as part of an IT governance scheme.

COBIT provides a detailed set of controls and control techniques for the information systems management environment. Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT’s information criteria.

Need for Guideline

The purpose of this guideline is to describe the recommended practices to carry out the review of Internet banking initiatives, applications and implementations, as well as to help identify and control the risks associated with this activity, so that the relevant.

IS Auditing Standards are complied with during the course of the review.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

- identify the ISACA Standards that has to do with Internet banking
- understand the focus of internal controls
- explain and understand the independence, competence, and planning of Internet banking
- explain the security risks to be evaluated
- identify and explain how to review the basic aspects of Internet banking planning, policy and infrastructure.

3.0 MAIN CONTENT

3.1 Internal Control

Internal controls over Internet banking systems should be commensurate with the level of risk of the services the bank offers, the level of risk involved in the implementation and the bank's risk tolerance level. The review of internal control in the Internet banking environment must help the IS auditor to provide reasonable assurance that the controls are appropriate and function appropriately.

Control objectives for an individual bank's Internet banking technology and products might focus on:

- Consistency of technology planning and strategic goals, including effectiveness, efficiency and economy of operations and compliance with corporate policies and legal requirements
- Data and service availability, including business recovery planning
- Data integrity, including providing for safeguarding of assets, proper authorisation of transactions and reliability of the data flow
- Data confidentiality and privacy standards, including controls over access by both employees and customers
- Reliability of management reporting

To appropriately evaluate the internal controls and their adequacy, the IS auditor should understand the bank's operational environment. COBIT 3rd Edition, published by the IT Governance Institute in 2000, has laid down seven information criteria to be met by information systems:

- Effectiveness
- Efficiency

- Confidentiality
- Integrity
- Availability
- Compliance
- Reliability

The information criteria listed in section 3.1.3 of this document are relevant in the case of Internet banking. Accordingly, a review of Internet banking should address how the information criteria of COBIT are met by the Internet banking initiative/application/ implementation.

Compared with other forms/channels of banking activities, Internet banking depends greatly on the integrity or trust in the confidentiality of customer data and on the availability of the system. In this context, there should be in place appropriateredundancy and fallback options, as well as disaster recovery procedures. In the case of Internet banking involving payments orfunds transfers, nonrepudiation and integrity of the transactions are essential attributes. In such cases, the review of Internet banking should address the effectiveness of the Internet banking system controls in assuring nonrepudiation and integrity. Due attention should be given to them while evaluating the availability of Internet banking solutions, especially if the continuity is based on cross-border processing, because it might infringe a regulation or might run counter to compliance with bank regulations.

It is essential in Internet banking to confirm that any communication, transaction or access request is legitimate. Accordingly, banks should use reliable methods for verifying the identity and authorisation of new customers as well as authenticating the identity and authorisation of established customers seeking to initiate electronic transactions. Customer verification during account origination is important to reduce the risk of theft, fraudulent transactions and money laundering activities. Strong customer identification and authentication processes are particularly important in the cross-border context given the difficulties that may arise from doing business electronically with customers across national and international borders, including the risk of identity impersonation and the difficulty in conducting effective credit checks on potential customers.

Auditability has more significance in the Internet banking environment, because a significant proportion of the transactions take place in paperless environments.

3.2 Independence

Professional Objectivity

Before accepting the engagement, the IS auditor should provide reasonable assurance that any interests he/she may have in the Internet bank under review would not in any manner impair the objectivity of the review. In the event of any possible conflicts of interest, these should be explicitly communicated to the bank's management and the written approval of the bank's management should be obtained before accepting the assignment.

3.3 Competence

Skills and Knowledge

The IS auditor should have the necessary technical and operational skills and knowledge to carry out the review of the technology employed and risks associated with Internet banking. The IS auditor should determine whether the technology and products are aligned with the bank's strategic goals. In particular, such reviews would call for bank operations knowledge and associated risks, knowledge of banking laws and regulations together with the technical knowledge necessary to evaluate aspects such as web hosting/web housing technologies, encryption technologies, network security architecture and security technologies, such as firewalls, intrusion detection and virus protection. Where expert advice or expert input is necessary, appropriate use should be made of external professional resources. The fact that external expert resources may be used should be communicated to the bank's management in writing.

3.4 Planning

High-Level Risk Assessment

The IS auditor should gather information regarding the Internet banking objectives of the bank, the strategy used to achieve the objectives, the way that the bank is using Internet technology in the relationships with its customers (either informative, communicative or transactional, as set out in 2.2.1). The information thus gathered should be such that it helps in carrying out a high-level assessment of the banking risks as well as the risks pertaining to the information criteria of COBIT. This high-level risk assessment will help determine the scope and coverage of the review. If the bank has an enterprise risk framework, this can be used.

The IS auditor should follow a risk assessment approach for analysing and evaluating the main potential general and specific threats connected to implementation of Internet banking, the possible manifestations, the potential effect on the bank, the likelihood of occurrences and the possible risk management measures that can be implemented for preventing risks. The following strategic risks should be evaluated:

- The strategic assessment and risk analysis
- Integration within corporate strategic goals
- Selection and management of technological infrastructure
- Comprehensive process for managing outsourcing relationships with third-party providers

The following security risks should be evaluated:

- Customer security practices
- Authentication of customers
- Nonrepudiation and accountability of transactions
- Segregation of duties
- Authorisation controls within systems, databases and applications
- Internal or external fraud
- Data integrity of transactions, databases and records
- Audit trails for transactions
- Confidentiality of data during transmission
- Third-party security risk

The following legal risks should be evaluated:

- Disclosures of information to customers
- Privacy
- Compliance to laws, rules and statements of the regulator or supervisor
- Exposure to foreign jurisdictions

The following reputational risks should be evaluated:

- Service level delivery
- Level of customer care
- Business continuity and contingency planning

Scope and Objectives of the Review

The IS auditor should, in consultation with the bank management where appropriate, clearly define the scope and objective of the review of Internet banking. The aspects to be covered by the review should be explicitly stated as part of the scope. The nature of the bank's Internet activities and volume of the Internet banking activities and the risks associated with them—as identified by the high-level risk assessment—dictate which aspects need to be reviewed as well as the extent and depth of the review.

For the purpose of the review, control objectives should be in accordance with regulations and applicable banking laws. The Internet is

borderless, so it is easy for any bank using an Internet-based delivery channel to operate in a multi-state and even multi-country environment. The bank may find itself bound by the laws, regulations and customs of wherever its customers are located rather than just where the bank is physically located. Therefore, the IS auditor should determine the geographic spread of the bank's current and planned customer base. The IS auditor needs to identify how many different jurisdictions have legal and regulatory control over the Internet banking operations and determine how the Internet bank is managing this risk.

Approach

The IS auditor should formulate the approach in such a way that the scope and objectives of the review could be fulfilled in an objective and professional manner. The approach followed should depend on whether the review is a pre-implementation review or a post-implementation review. The approach should be appropriately documented. If the input or advice of external experts is to be used, this should also be specified as part of the approach.

Sign-off for the Plan

Depending on the practices of the organisation, it may be appropriate for the IS auditor to obtain the agreement of the bank's management for the review plan and approach.

3.5 Performance of Internet Banking Review

Execution

The aspects to be reviewed and the review process should be chosen by taking into account the intended scope and objective of the review as well as the approach defined as part of the planning process.

In general, in gathering, analysing and interpreting the Internet banking environment, a study should be made of available documentation, such as bank regulations about Internet banking, Internet law, privacy law, web banking system documentation and use of the Internet banking solution.

To identify any problems relating to the Internet banking area which have been noted previously and which may require follow-up, the IS auditor should review the following documents:

- Previous examination reports
- Follow-up activities
- Work papers from previous examinations
- Internal and external audit reports

The IS auditor should map the key processes-both automated as well as manual-relating to the Internet banking initiative/ system.

The IS auditor should then assess the probability that the risks identified pertaining to these processes (business as well as IS risks) will materialize together with their likely effect, and document the risks along with the controls, which mitigate these risks.

As part of the IS risk assessment, external IS threats should be evaluated depending on the nature of products offered by a bank and the external threats to be addressed. These threats include denial of service, unauthorized access to data, and unauthorized use of the computer equipment, which could arise from various sources such as casual hackers, competitors, alien governments, terrorists or disgruntled employees.

Depending on the nature of the pre- or post-implementation review, the IS auditor should test the significant processes in the test and or production environment to verify that the processes are functioning as intended. These tests include testing of balance inquiry, testing of bill presentation and payment and testing the security mechanisms using penetration testing.

In post implementation review the IS auditor should obtain, at least, an understanding of network mapping, network routing, systems and network security assessment, and internal and external intrusion.

Since the Internet banking solution is predominantly an information technology solution, it should meet the information criteria established in COBIT, as well as other relevant standards or regulations of the industry. The extent of compliance with the information criteria, standards and/or regulations and the effect of noncompliance should be analysed.

Aspects to Review

The following organisational aspects should be reviewed to know whether:

- Due diligence and risk analysis are performed before the bank conducts Internet banking activities
- Due diligence and risk analysis are performed where cross-border activities are conducted
- Internet banking is consistent with the bank's overall mission, strategic goals and operating plans
- Internet application is compliant with the defined and approved business model
- Internet banking systems and/or services are managed in-house or outsourced to a third-party

- Management and personnel of the organisation display acceptable knowledge and technical skills to manage Internet banking
- Measures to ensure segregation of duties are in place
- Management reports are adequate to appropriately manage Internet banking transaction and payment services activities

The review should include policy aspects such as whether:

- Suitable policies have been defined and implemented regarding the acquisition of customers, the engagement of suppliers, the customers authentication, the privacy of customers/suppliers data, audit trail, the review of usage logs and whether the bank is keeping abreast of legal developments associated with Internet banking
- The bank is providing accurate privacy disclosures associated with its Internet banking product line
- Information is provided on the web site to allow customers to make informed judgment about the identity and regulatory status of the bank before they enter into Internet banking services (name of the bank and the location of its head office, the primary bank supervisory authority, ways to contact to customer service and other relevant information)
- The bank has established policies governing the use of hypertext links such that consumers can clearly distinguish between bank and non-bank products, and that they are informed when leaving the bank's web site
- There are appropriate procedures in place regarding change control, the review of audit trails and the review/analysis of usage logs (firewall logs and other reports)
- There are suitable and adequate procedures in place to ensure the privacy and integrity of the data and to ensure compliance with the applicable laws and regulations as well as best practice

The following planning aspects should be reviewed to know whether:

- The planned information systems technology architecture is feasible and will result in safe and sound operations
- There are appropriate incident response plans in place to manage, contain and minimise problems arising from unexpected events, including internal or external attacks
- An "Internet product life cycle" exists and if it is followed both for developing, maintenance and upgrading Internet applications
- Business continuity and contingency plans for critical Internet banking processing and/or delivery systems are in place and regularly tested

The following information systems infrastructure aspects should be reviewed to know whether:

- The infrastructure and systems are capable of expansion to accommodate the proposed business plan
- An information security architecture has been defined and is appropriate for the nature of the Internet banking model
- The bank has an adequate process and controls to address physical security for hardware, software and data communications equipment associated with the Internet banking system
- The bank has a sound process which ensures adequate control over the path between the web site and the bank's internal networks or computer systems and whether the internal network is suitably protected from the external environment using appropriate firewall technology
- Databases and data flow are protected from unauthorised/inappropriate access
- There are suitable and adequate procedures in place to ensure the identification of access points and potential areas of vulnerability
- There are appropriate manual balancing controls where automated controls are inadequate
- The record for each customer transaction contains identification of the customer, the transaction number, the type of transaction, the transaction amount and other information of relevance, if it is stored and archived, for control purposes or other business functions such as marketing

The following telecommunication infrastructure aspects should be reviewed for whether:

- The network architecture is appropriate for the nature, timing and extent of the Internet banking operation
- The network protocols used are appropriate for the intended use (for instance, if payments or funds transfers are accepted through the Internet banking system, secure protocols should be used)
- The bank has an effective process to assess the adequacy of physical controls in place to restrict access to firewall servers and components
- Intrusion detection systems and virus control systems/procedures are in place
- There is adequate penetration testing of internal or external networks
- The communication across the network is made secure using virtual private network (VPN) and related encryption techniques where appropriate and necessary
- Adequate and strong encryption algorithms were selected to protect data during communication across the network

The following authentication aspects should be reviewed to know whether:

- Control features are in place to validate the identity of prospective customers while they use the Internet to apply for new bank loan and/or deposit accounts
- Control features are built into the systems to ensure the authentication of the existing customer, the integrity of data and the confidentiality of transactions
- Authentication procedures are used to uniquely and positively identify the transacting party using digital certificates and digital signatures where necessary
- Nonrepudiation is ensured for an eventual later business or legal use where transactions are made using the Internet banking system
- The fault tolerance features of the Internet banking system are commensurate with the nature, volume and criticality of its system

The following third-party service provider aspects should be reviewed to know whether:

- Due diligence review of the competency and financial viability was conducted prior to entering into any contract with third-party service providers
- The contracts with third-party service providers adequately protect the interests of the bank and the bank's customers, and whether the bank organisation has reviewed vendor contracts to ensure that the responsibilities of each party are appropriately identified and defined
- The bank organisation obtains and reviews internal or external audit reports of third-party service providers, evaluating vendor management processes or specific vendor relationships as they relate to information systems and technology, and whether all outsourced systems and operations are subject to risk management, security and privacy policies that meet the bank's own standards
- The bank organization has the right to conduct independent reviews and/or audits of security, internal control and business continuity and contingency plans of third-party service providers
- The security procedures of the third parties are appropriate and adequate where the Internet banking solution depends on the any third-party service providers such as Internet service providers (ISP), certification authority (CA), registration authority (RA), web-hosting/housing agency
- Third-party service providers have appropriate business continuity and contingency plans for critical Internet banking processing and/or

delivery systems are in place and regularly tested, and whether the bank receives copies of test result reports

- The bank has an adequate process to ensure that software maintained by the vendor is under a software escrow agreement and that the software is confirmed as being current on a regular basis where the bank obtains software products from a vendor
- A third –party’s opinion is sought in the pre-implementation phase of Internet applications for evaluating the security architecture solution that will be developed and configured

Where necessary and agreed with the bank, external expert input or advice should be used suitably in the collection, analysis and interpretation of the data.

The inferences and recommendations should be based on an objective analysis and interpretation of the data.

Appropriate audit trails should be maintained and protected for the data gathered, the analysis made and the inferences arrived at, as well as the corrective actions recommended.

Before finalizing the report, the observations and recommendations should be validated with the stakeholders, board of directors and the bank’s management, as appropriate.

3.6 Reporting

Report Content

The IS auditor should produce regular reports on the technologies employed, the risks assumed, and how those risks are managed. Monitoring system performance is a key success factor. Depending on the scope of its coverage, the report on Internet banking review carried out should address the following, as appropriate:

- The scope, objectives and methodology followed and assumptions
- An overall assessment of the Internet banking processes/systems solution in terms of key strengths and weaknesses as well as the likely effects of weaknesses
- Recommendations to overcome the significant weaknesses and to improve the Internet banking processes/systems solution
- A statement on the extent of compliance with bank regulations or applicable laws, along with the effect of any noncompliance
- A statement on the extent of compliance with the information criteria of COBIT, along with the effect of any noncompliance
- Recommendations regarding how the lessons of the review could be used to improve similar future solutions or initiatives

4.0 CONCLUSION

Talking about sanitizing and standardizing Internet banking operations regionally and globally, auditing happens to be one of the appropriate and capable tools in doing this. This helps to strengthen individual frameworks for viable and worthy Internet banking. It is worthy to not that the audit programme of the ISACA is standard and rigorous enough, but the challenge is how well the Internet banking operators goes to put in place the recommended checks and balances, especially in regions with weak will to implement such standards.

5.0 SUMMARY

- Internal controls over Internet banking systems should be commensurate with the level of risk of the services the bank offers, the level of risk involved in the implementation and the bank's risk tolerance level.
- Compared with other forms/channels of banking activities, Internet banking depends greatly on the integrity or trust in the confidentiality of customer data and on the availability of the system
- Before accepting the engagement, the IS auditor should provide reasonable assurance than any interests he/she may have in the Internet bank under review would not in any manner impair the objectivity of the review.
- The IS auditor should have the necessary technical and operational skills and knowledge to carry out the review of the technology employed and risks associated with Internet banking.
- The IS auditor should gather information regarding the Internet banking objectives of the bank, the strategy used to achieve the objectives, the way that the bank is using Internet technology in the relationships with its customers.
- The aspects to be reviewed and the review process should be chosen by taking into account the intended scope and objective of the review as well as the approach defined as part of the planning process.
- The IS auditor should produce regular reports on the technologies employed, the risks assumed, and how those risks are managed. Monitoring system performance is a key success factor.

6.0 TUTOR-MARKED ASSIGNMENT

- Mention 5 control objectives of Internet banking and technology and products
- Mention 10 security risks to be evaluated in Internet banking

7.0 REFERENCES/FURTHER READING

An Internet Banking Primer, Federal Reserve Bank of Chicago, USA

Basle Directive N° 82, Risk Management Principles for Electronic Banking, Basel Committee on Banking Supervision, May 2001, Switzerland

Basle Directive N° 86, Sound Practices for the Management and Supervision of Operational Risk, Basel Committee on Banking Supervision, May 2001, Switzerland.

Basle Directive N° 91, Risk Management Principles for Electronic Banking, Basel Committee on Banking Supervision, July 2002, Switzerland

BIS Papers N° 7. Electronic finance: a new perspective and challenges, Monetary and Economic Department, Bank for International Settlements, November 2001, Switzerland

Cronin, Mary J., *Banking and Finance on the Internet*, John Wiley & Sons, Inc., ISBN 0-471-29219-2, USA

Essinger, James, *The Virtual Banking Revolution*, Thomson Business Press, ISBN 1-86152-343-2, United Kingdom

Internet Banking Comptroller's Handbook, Comptroller of the Currency Administrator of National Banks, October 1999, USA

Furst, Karen, William W. Lang and Daniel E. Nolle, *Internet Banking: Developments and Prospects*, Economic and Policy Analysis Working Paper 2000-9, Office of the Comptroller of the Currency, September 2000, USA

The Internet and the National Bank Charter, Comptroller of the Currency Administrator of National Banks, January 2001, USA

COURSE CODE
635

BHM

UNIT 3 MOBILE E-BANKING

CONTENTS

- 1.0 Introduction
- 2.0 Objectives
- 3.0 Main Content
 - 3.1 A Mobile Banking Conceptual Model
 - 3.2 Trends in Mobile Banking
 - 3.3 Mobile Banking Business Models
 - 3.4 Mobile Banking Services
 - 3.5 Challenges for a Mobile Banking Solution
 - 3.6 Mobile Banking in the World
- 4.0 Conclusion
- 5.0 Summary
- 6.0 Tutor-Marked Assignment
- 7.0 References/Further Reading

1.0 INTRODUCTION

Mobile banking (also known as M-Banking, SMS Banking etc.) is a term used for performing balance checks, account transactions, payments etc. via a mobile device such as a mobile phone. Mobile banking today is most often performed via SMS or the Mobile Internet but can also use special programs called clients, downloaded to the mobile device.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

1. define mobile banking
2. identify the interrelated aspects of the concept of mobile banking
3. understand the trend in mobile banking
4. explain the various models of mobile banking
5. identify the services carried out in mobile banking
6. discuss the challenges facing mobile banking operations.

3.0 MAIN CONTENT

3.1 A Mobile banking Conceptual Model

In one academic model, mobile banking is defined as the ‘provision and availability of banking and financial services with the help of mobile telecommunication devices. The scope of offered services may include

facilities to conduct bank and stock market transactions, to administer accounts and to access customised information’.

According to this model, Mobile Banking can be said to consist of three inter-related concepts:

- Mobile Accounting
- Mobile Brokerage
- Mobile Financial Information Services

Most services in the categories designated *Accounting* and *Brokerage* are transaction-based. The non-transaction-based services of an informational nature are however essential for conducting transactions - for instance, balance enquiries might be needed before committing a money remittance. The accounting and brokerage services are therefore offered invariably in combination with information services. Information services, on the other hand, may be offered as an independent module.

3.2 Trends in Mobile Banking

The advent of the Internet has revolutionized the way the financial services industry conducts business, empowering organizations with new business models and new ways to offer "24 x 7" accessibility to their customers.

The ability to offer financial transactions online has also created new players in the financial services industry, such as online banks, online brokers and wealth managers who offer personalized services, although such players still account for a tiny percentage of the industry.

Over the last few years, the mobile and wireless market has been one of the fastest growing markets in the world and it is still growing at a rapid pace. According to the GSM Association and Ovum, the number of mobile subscribers exceeded 2 billion in September 2005, and now exceeds 2.5 billion (of which more than 2 billion are GSM).

According to a study by financial consultancy Celent, 35% of online banking households will be using mobile banking by 2010, up from less than 1% today. Upwards of 70% of bank center call volume is projected to come from mobile phones. Mobile banking will eventually allow users to make payments at the physical point of sale. "Mobile contactless payments" will make up 10% of the contactless market by 2010.

Many believe that mobile users have just started to fully utilize the data capabilities in their mobile phones. In Asian countries like India, China, Bangladesh, Indonesia and Philippines, where mobile infrastructure is comparatively better than the fixed-line infrastructure, and in European countries, where mobile phone penetration is very high (at least 80% of consumers use a mobile phone), mobile banking is likely to appeal even more.

This opens up huge markets for financial institutions interested in offering value added services. With mobile technology, banks can offer a wide range of services to their customers such as doing funds transfer while travelling, receiving online updates of stock price or even performing stock trading while being stuck in traffic. According to the German mobile operator Mobilcom, mobile banking will be the "killer application" for the next generation of mobile technology.

Mobile devices, especially smartphones, are the most promising way to reach the masses and to create "stickiness" among current customers, due to their ability to provide services anytime, anywhere, high rate of penetration and potential to grow. According to Gartner, shipment of smartphones is growing fast, and topped 20 million units (of over 800 million sold) in 2006 alone.

Banks across the globe have invested billions of dollars to build sophisticated internet banking capabilities. As the trend is shifting to mobile banking, there is a challenge for CIOs and CTOs of these banks to decide on how to leverage their investment in internet banking and offer mobile banking, in the shortest possible time.

The proliferation of the 3G (third generation of wireless) will generate the development of more sophisticated services such as multimedia and links to m-commerce services.

3.3 Mobile Banking Business Models

A wide spectrum of Mobile/branchless banking models is evolving. These models differ primarily on the question that who will establish the relationship (account opening, deposit taking, lending etc.) to the end customer, the Bank or the Non-Bank/Telecommunication Company (Telco). Another difference lies in the nature of agency agreement between bank and the Non-Bank. Models of branchless banking can be classified into three broad categories - Bank Focused, Bank-Led and Nonbank-Led.

Bank-Focused Model

The bank-focused model emerges when a traditional bank uses non-traditional low-cost delivery channels to provide banking services to its existing customers. Examples range from use of automatic teller machines (ATMs) to internet banking or mobile phone banking to provide certain limited banking services to banks' customers. This model is additive in nature and may be seen as a modest extension of conventional branch-based banking.

Bank-Led Model

The bank-led model offers a distinct alternative to conventional branch-based banking in that customer conducts financial transactions at a whole range of retail agents (or through mobile phone) instead of at bank branches or through bank employees. This model promises the potential to substantially increase the financial services outreach by using a different delivery channel (retailers/ mobile phones), a different trade partner (telco / chain store) having experience and target market distinct from traditional banks, and may be significantly cheaper than the bank-based alternatives. The bank-led model may be implemented by either using correspondent arrangements or by creating a JV between Bank and Telco/non-bank. In this model customer account relationship rests with the bank

Non-Bank-Led Model

The non-bank-led model is where a bank does not come into the picture (except possibly as a safe-keeper of surplus funds) and the non-bank (e.g telco) performs all the functions.

3.4 Mobile Banking Services

Mobile banking can offer services such as the following:

Account Information

- Mini-statements and checking of account history
- Alerts on account activity or passing of set thresholds
- Monitoring of term deposits
- Access to loan statements
- Access to card statements
- Mutual funds / equity statements
- Insurance policy management
- Pension plan management
- Status on cheque, stop payment on cheque

Payments & Transfers

- Domestic and international fund transfers
- Micro-payment handling

- Mobile recharging
- Commercial payment processing
- Bill payment processing
- Peer to Peer payments

Investments

- Portfolio management services
- Real-time stock quotes
- Personalized alerts and notifications on security prices

Support

- Status of requests for credit, including mortgage approval, and insurance coverage
- Check (cheque) book and card requests
- Exchange of data messages and email, including complaint submission and tracking
- ATM Location

Content Services

- General information such as weather updates, news
- Loyalty-related offers
- Location-based services

Based on a survey conducted by Forrester, mobile banking will be attractive mainly to the younger, more “tech-savvy” customer segment. A third of mobile phone users say that they may consider performing some kind of financial transaction through their mobile phone. But most of the users are interested in performing basic transactions such as querying for account balance and making bill payment.

3.5 Challenges for a Mobile Banking Solution

Key challenges in developing a sophisticated mobile banking application are:

Interoperability

There is a lack of common technology standards for mobile banking. Many protocols are being used for mobile banking – HTML, WAP, SOAP, XML to name a few. It would be a wise idea for the vendor to develop a mobile banking application that can connect multiple banks. It would require either the application to support multiple protocols or use of a common and widely acceptable set of protocols for data exchange.

There are a large number of different mobile phone devices and it is a big challenge for banks to offer mobile banking solution on

any type of device. Some of these devices support J2ME and others support WAP browser or only SMS.

Overcoming interoperability issues however have been localized, with countries like India using portals like R-World to enable the limitations of low end java based phones, while focus on areas such as South Africa have defaulted to the USSD as a basis of communication achievable with any phone.

The desire for interoperability is largely dependent on the banks themselves, where installed applications (Java based or native) provide better security, are easier to use and allow development of more complex capabilities similar to those of internet banking while SMS can provide the basics but becomes difficult to operate with more complex transactions.

Security

Security of financial transactions, being executed from some remote location and transmission of financial information over the air, are the most complicated challenges that need to be addressed jointly by mobile application developers, wireless network service providers and the banks' IT departments.

The following aspects need to be addressed to offer a secure infrastructure for financial transaction over wireless network:

- Physical part of the hand-held device. If the bank is offering smart-card based security, the physical security of the device is more important.
- Security of any thick-client application running on the device. In case the device is stolen, the hacker should require at least an ID/Password to access the application.
- Authentication of the device with service provider before initiating a transaction. This would ensure that unauthorized devices are not connected to perform financial transactions.
- User ID / Password authentication of bank's customer.
- Encryption of the data being transmitted over the air.
- Encryption of the data that will be stored in device for later / off-line analysis by the customer.

Scalability & Reliability

Another challenge for the CIOs and CTOs of the banks is to scale-up the mobile banking infrastructure to handle exponential growth of the customer base. With mobile banking, the customer may be sitting in any part of the world (true anytime, anywhere banking) and hence banks need to ensure that the systems are up and running in a true 24 x 7

fashion. As customers will find mobile banking more and more useful, their expectations from the solution will increase. Banks unable to meet the performance and reliability expectations may lose customer confidence.

Application distribution

Due to the nature of the connectivity between bank and its customers, it would be impractical to expect customers to regularly visit banks or connect to a web site for regular upgrade of their mobile banking application. It will be expected that the mobile application itself check the upgrades and updates and download necessary patches (so called Over the Air updates). However, there could be many issues to implement this approach such as upgrade / synchronization of other dependent components.

Personalization

It would be expected from the mobile application to support personalization such as:

- Preferred Language
- Date / Time format
- Amount format
- Default transactions
- Standard Beneficiary list
- Alerts

3.6 Mobile Banking in the World

This part of the mobile commerce is very popular in countries where most of their population is unbanked.

Countries like Sudan, Ghana and South Africa received very well this new commerce.

In Latin America countries like Uruguay, Paraguay Argentina, Brazil, Venezuela, Colombia, Guatemala and recently Mexico started with a huge success.

In Colombia was released with Redeban.

Guatemala have the support of Banco industrial. Mexico released the mobile commerce with Omnilife, Bancomer and a private company (MPower Ventures).

4.0 CONCLUSION

Within the framework of forms of electronic banking, mobile banking is emerging and very well as well. Quiet a lot of banking operations are now mobile and many more will follow as people begins to have confidence in the system, and much more begin to acquire the technology to enable them do mobile banking. There had always been challenges in virtually all forms of electronic transactional systems, and mobile banking is not an exception. But the challenges are sunmountable, with developments in information technology.

5.0 SUMMARY

- Mobile banking (also known as M-Banking, mbanking, SMS Banking etc.) is a term used for performing balance checks, account transactions, payments etc. via a mobile device such as a mobile phone. Mobile banking today (2007) is most often performed via SMS or the Mobile Internet but can also use special programs called clients downloaded to the mobile device.
- The advent of the Internet has revolutionized the way the financial services industry conducts business, empowering organizations with new business models and new ways to offer 24 x 7 accessibility to their customers.
- A wide spectrum of Mobile/branchless banking models is evolving. These models differ primarily on the question that who will establish the relationship (account opening, deposit taking, lending etc.) to the end customer, the Bank or the Non-Bank/Telecommunication Company (Telco).
- Based on a survey conducted by Forrester, mobile banking will be attractive mainly to the younger, more "tech-savvy" customer segment
- Security of financial transactions, being executed from some remote location and transmission of financial information over the air, are the most complicated challenges that need to be addressed jointly by mobile application developers, wireless network service providers and the banks' IT departments
- There is a lack of common technology standards for mobile banking. Many protocols are being used for mobile banking – HTML, WAP, SOAP, XML to name a few.
- Countries like Sudan, Ghana and South Africa received very well this new commerce. In Latin America countries like Uruguay, Paraguay Argentina, Brazil, Venezuela, Colombia, Guatemala and recently Mexico started with a huge success

6.0 TUTOR-MARKED ASSIGNMENT

1. Briefly discuss the bank-led model of e-banking
2. Mention 5 core services offered by mobile banking

7.0 REFERENCES/FURTHER READING

Tiwari, Rajnish and Buse, Stephan. (2007). *The Mobile Commerce Prospects: A Strategic Analysis of Opportunities in the Banking Sector*, Hamburg University Press (E-Book)

Tiwari, Rajnish; Buse, Stephan and Herstatt, Cornelius (2007). *Mobile Services in Banking Sector: The Role of Innovative Business Solutions in Generating Competitive Advantage*, in: Proceedings of the International Research Conference on Quality, Innovation and Knowledge Management, New Delhi, pp. 886–894.

Tiwari, Rajnish; Buse, Stephan and Herstatt, Cornelius (2006). *Customer on the Move: Strategic Implications of Mobile Banking for Banks and Financial Enterprises*, in: CEC/EEE 2006, Proceedings of The 8th IEEE International Conference on E-Commerce Technology and The 3rd IEEE International Conference on Enterprise Computing, E-Commerce, and E-Services (CEC/EEE'06), San Francisco, pp. 522–529.

Tiwari, Rajnish; Buse, Stephan and Herstatt, Cornelius (2006). *Mobile Banking as Business Strategy: Impact of Mobile Technologies on Customer Behaviour and its Implications for Banks*, in Technology Management for the Global Future - Proceedings of PICMET '06.

Owens, John and Anna Bantug-Herrera (2006). *Catching the Technology Wave: Mobile Phone Banking and Text-A-Payment in the Philippines*

UNIT 4 ELECTRONIC PAYMENT SYSTEMS

CONTENTS

- 1.0 Introduction
- 2.0 Objectives
- 3.0 Main Content
 - 3.1 Overview of Electronic Payment Systems
 - 3.2 Electronic Bill Payment
 - 3.2.1 Limitations (United States)
 - 3.3 Electronic Funds Transfer
 - 3.3.1 What is Electronic Fund Transfer?
 - 3.3.2 EFTPOS
 - 3.3.3 Card-based SFT
 - 3.3.4 Transaction Types
 - 3.3.5 Authrisation
 - 3.3.6 Dual Message Authorisation/Clearing
 - 3.3.7 Single Message Authorisation/Clearing
 - 3.3.8 Authentication
 - 3.4 Electronic Money
 - 3.4.1 What is Electronic Money?
 - 3.4.2 Alternative Systems
 - 3.5 Off-Line Anonymous Electronic Money
 - 3.5.1 Future Evolution
 - 3.5.2 Issues
 - 3.6 Wire Transfer
 - 3.6.1 What is: Wire Transfer?
 - 3.6.2 History
 - 3.6.3 Process
 - 3.6.4 Regulation
 - 3.6.5 Security
 - 3.6.6 Methods
- 4.0 Conclusion
- 5.0 Summary
- 6.0 Tutor-Marked Assignment
- 7.0 References/Further Reading

1.0 INTRODUCTION

There are over a dozen proposals for electronic payment systems on the Internet. Advances in information technology have presented financial institutions with several options of electronic transaction methods to facilitate business processes. The coming of the Internet and the World Wide Web has made the operation of these electronic payment options to be worthwhile. Despite some lapses especially in the area of security, electronic payment systems have come to stay in modern-day business financial transactions.

2.0 OBJECTIVES

At the end of this unit, you are expected to:

- define and know the different types of electronic systems
- differentiate the forms of electronic systems
- understand their strengths and weaknesses
- understand the specific applications of each type.

3.0 MAIN CONTENT

3.1 Overview of Electronic Payment Systems

There are over a dozen proposals for electronic payment systems on the Internet. To briefly understand these systems, let's us examine a few issues by trying to pay a bill via the Internet with a credit card. In comparison to using cash in the real world, transmitting a credit card number over the Internet might lead to the following difficulties.

First, there is the entire question of security. Credit card numbers may be viewed by unauthorized individuals because the Internet is an open system. In the real world, there are a number of means to minimize fraud. A customer using a credit card will usually opt to carry out transactions at trustworthy or familiar facilities, stores, and markets.

Second, credit cards can be used only at authorized stores. Unauthorized small businesses or individuals generally cannot carry out transactions with credit cards. In other words, credit cards cannot be used for peer-to-peer payment. Cash encourages peer-to-peer payments.

Third, credit card payments usually charge a small fee. Although this cost is low, it can be a significant cost when the payment itself is very small. As a result, credit cards can not be used for micro-payments. Cash payments are used for even the smallest financial transactions.

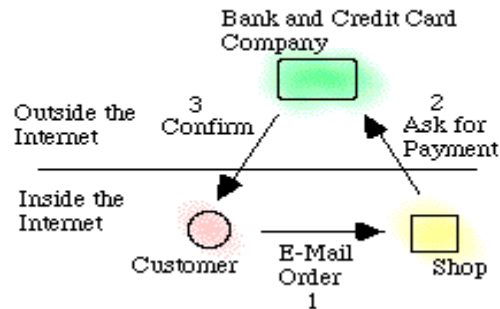
Finally, receipts from credit card payments leave residual records of expenditures. Those who issue credit cards know exactly what kinds of goods and services have been purchased, as well as where and when they were acquired. In other words, user's expenditures by credit card can be traced while cash payments are untraceable.

Electronic payment systems, more or less, try to cope with the above issues. According to the extent to which these systems cope with these problems, I classify digital cash programs into three categories.

1. Credit Card Base Type

To minimize security risks and the loss of credit card numbers in transit, First Virtual Holding began a payment system in which users transmit passwords instead of credit card numbers when purchasing an item (See Figure 1-i).

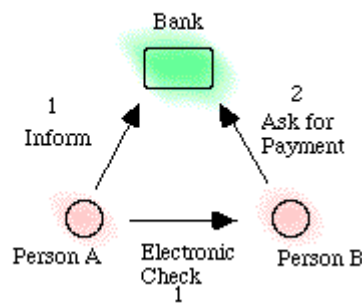
(i) Credit Card type



Customer sends his ID or encrypted creditcard number to the shop. Shop asks for payment to the Credit card company, which confirms customer by e-mail. After the confirmation, payment is done. Card number itself never goes through the Net.

Security X
Peer-to-peer -
Low fees -
Untraceability -

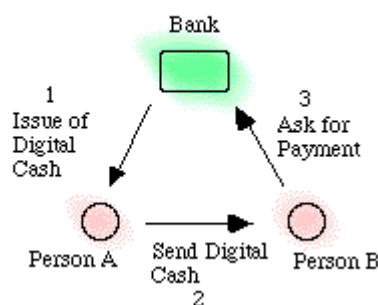
(ii) Check type



Person "A" issues his electronic check. He sends it to person "B" and informs the bank of his check. Person "B" asks for payment to the Bank. After the confirmation, the bank transfers money from person As account to person Bs.

Security X
Peer-to-peer X
Low fees X
Untraceability -

(ii) Cash type



Person "A" asks the bank to issue digital cash. The bank issues digital cash and reduces his account by that amount. He sends it to person "B". Person "B" asks the bank for payment. After confirming that the digital cash is not double-spent, the bank increases person Bs account by that amount. Note that the bank cannot know who sent that digital cash to person B. (Untraceability)

Security	X
Peer-to-peer	X
Low fees	X
Untraceability	X

In this system, a user registers in advance with First Virtual to secure a password corresponding to a credit card number. With the purchase of goods or services on the Internet, only a password is transmitted to complete the transactions. After the actual purchase, a confirmation electronic mail message confirms the validity of the transaction. This system is simple and is already in use to some extent. Visa and MasterCard are planning a similar payment program using encryption instead of passwords.

These credit-card based solutions solve only the security question. As Figure 1-(i) illustrates, the actual communication between the consumer and electronic storefront are addressed by this strategy. The transaction of real money remains to be done by conventional credit card transactions. These transactions require a fee. A peer-to-peer transaction is impossible. Certainly, the entire transaction is also traceable.

2. Check Type

Checks are closer transitionally to cash than to credit cards, because peer-to-peer transfers are possible. Micro-payments are possible as well though banks are reluctant to accept process micro-payments by checks thanks to the high operational cost of check clearance. As a result, several proposals (CyberCash, NetCheck, and others) have emerged to invent checks on the Internet, which would be transferable between individuals. As Figure 1-(ii) shows, a customer opens an account in a bank on the Internet, and issues an electronic check to pay a bill. The recipient of this digital check sends it to the Internet bank to confirm and cash it. Security is guaranteed by both encryption and the bank's confirmation process with the issuer of the check. This system permits peer-to-peer payments and reduces fees to some extent. But transactions are still traceable since a bank can track the actual use of the electronic check.

3. Cash Type

Cash transactions are untraceable and anonymous. To achieve untraceability on the Internet, encryption has to be fully employed to prevent untraceable money from being easily copied and spent twice, a phenomenon known as double-spending. David Chaum as well Tatsuaki Okamoto and Kazuo Ohta have proposed untraceable electronic payment systems using advanced encryption technology.

The mechanism in this system is similar to an electronic check, but it prevents banking institutions from linking purchasers to specific goods and services (see Figure 1-(iii)). How does this work? First, an Internet user opens an account with real money at an Internet-based bank. The customer asks the bank to issue a certain amount of digital cash for use on the Internet. The bank issues this digital cash using encryption and deducts the funds from the established account. An example of a bank that performs these sorts of transactions is Mark Twain Banks, operating since late in 1995.

This digital cash is a combination of two huge integers which have special mathematical relation. No other person or institution, but the bank, can imitate this relation. Any calculation that would attempt to duplicate this relation would take an almost infinite amount time in the absence of the bank's secret key.

When an individual uses digital cash, this unique data that defines the actual electronic currency is given to the merchant. The merchant in turn sends this data to the bank to confirm it. If the bank confirms it, the bank credits the merchant's bank account by that amount, or alternatively issues the merchant a sum of digital cash in the same amount. Only the bank can confirm that this data - or, digital cash - is legitimate and actually issued by the bank. Only the bank can verify that this that this data has not been used elsewhere, or double-spent. The bank cannot know who used the digital cash, as long as customers of the bank do not use it twice.

This payment system deserves the name of "cash on the Internet" because it is almost equal to a cash payment in terms of security, fee, peer-to-peer payment, and untraceability. I will now focus on this cash-type "digital cash."

3.2 Electronic Bill Payment

Electronic bill payment is a feature of online banking, similar in its effect to a giro, allowing a depositor to send money from his demand account to a creditor or vendor such as a public utility or a department store to be credited against a specific account. The payment is optimally executed electronically in real time, though some financial institutions or payment services will wait until the next business day to send out the payment. The bank can usually also generate and mail a paper cheque or banker's draft to a creditor who is not set up to receive electronic payments.

Electronic billing can also feature invoices sent by e-mail or viewed on a secure web site (with notices of new invoices being sent by e-mail).

Most large banks also offer various convenience features with their electronic bill payment systems, such as the ability to schedule payments in advance to be made on a specified date, the ability to manage payments from any computer with a web browser, and various options for searching one's recent payment history: when did I last pay Company X? To whom did I make my most recent payment? In many cases one can also integrate the electronic payment data with accounting or personal finance software.

Peer-to-peer payment systems are extremely popular. The best and most widely known example is PayPal. PayPal allows you to pay for just about anything online as long as the seller also has a PayPal account. Many online sellers use PayPal such as 75% of eBay sellers, overstock.com, ritzcamera.com, and Walgreens.com (Traver, 2004). PayPal is also sometimes used to pay for personal debts in situations where both parties have an account.

Electronic bill payment and presentment (EBPP) includes an electronic bill payment system (EBPS). Electronic bill payment and presentment is “the electronic bill presentment to the consumer and the electronic initiation of payment by the consumer” (Alexandria Andreeff). This was done completely by postal mail before the internet. Sending bills electronically via the internet is much faster and cheaper though. Although this technology was available before December in 1998, only 26.2% of U.S. households had internet access at that time according to the U.S. Department of Commerce in 2000 (Alexandria Andreeff). By August of 2000, electronic bill payment and presentment systems started to dramatically increase in popularity because 41.5% of U.S. households had internet access by then according to the U.S. Department of Commerce in 2000 (Alexandria Andreeff). In this model, the one who is charging the consumer, notifies the customer (usually) through e-mail (Alexandria Andreeff). The customer is then responsible to log on to the biller's website to pay the bill (Alexandria Andreeff).

3.2.1 Limitations (United States)

Typically, US financial institutions formally prohibit the use of their consumer electronic bill payment systems for payments to any tax authorities, collection agencies, or recipients of court-ordered payments like child support or alimony. Any organizations or individuals outside of the United States are also usually excluded. Payments to government agencies for utilities such as water are usually permitted.

3.3 Electronic Funds Transfer

3.3.1 What is Electronic Fund Transfer?

Electronic funds transfer or EFT refers to the computer-based systems used to perform financial transactions electronically.

The term is used for a number of different concepts:

- Cardholder-initiated transactions, where a cardholder makes use of a payment card
- Direct deposit payroll payments for a business to its employees, possibly via a payroll services company
- Direct debit payments from customer to business, where the transaction is initiated by the business with customer permission
- Electronic bill payment in online banking, which may be delivered by EFT or paper check
- Transactions involving stored value of electronic money, possibly in a private currency
- Wire transfer via an international banking network (generally carries a higher fee)
- Electronic Benefit Transfer

3.3.2 EFTPOS

EFTPOS (short for *Electronic Funds Transfer at Point of Sale*) is an Australian and New Zealand electronic processing system for credit cards, debit cards and charge cards.

EFTPOS also allows users of the system to withdraw cash at the time of purchasing a product or service through the merchant's EFTPOS terminal. This functionality is called debit card cashback in other countries.

The name and logo for EFTPOS in Australia were originally owned by the National Australia Bank and were trade marks from 1986 until 1991. There are over 60,000 participating EFTPOS outlets in Australia.

European banks and card companies also sometimes reference “EFTPOS” as the system used for processing card transactions through terminals on points of sale, though the system is not the trademarked Australian/New Zealand variant.

3.3.3 Card-Based EFT

Credit cards

EFT may be initiated by a cardholder when a payment card such as a credit card or debit card is used. This may take place at an automated teller machine (ATM) or point of sale (POS), or when the card is not present, which covers cards used for mail order, telephone order and internet purchases.

Card-based EFT transactions are often covered by the ISO 8583 standard.

3.3.4 Transaction Types

A number of transaction types may be performed, including the following:

- *Sale*: where the cardholder pays for goods or service
- *Refund*: where a merchant refunds an earlier payment made by a cardholder
- *Withdrawal*: the cardholder withdraws funds from their account, e.g. from an ATM. The term *Cash Advance* may also be used, typically when the funds are advanced by a merchant rather than at an ATM
- *Deposit*: where a cardholder deposits funds to their own account (typically at an ATM)
- *Cashback*: where a cardholder withdraws funds from their own account at the same time as making a purchase
- *Inter-account transfer*: transferring funds between linked accounts belonging to the same cardholder
- *Payment*: transferring funds to a third party account
- *Enquiry*: a transaction without financial impact, for instance balance enquiry, available funds enquiry, linked accounts enquiry, or request for a statement of recent transactions on the account
- *E top-up*: where a cardholder can use a device (typically POS or ATM) to add funds (top-up) their pre-pay mobile phone
- *Mini-statement*: where a cardholder uses a device (typically an ATM) to obtain details of recent transactions on their account
- *Administrative*: this covers a variety of non-financial transactions including PIN change

The transaction types offered depend on the terminal. An ATM would offer different transactions from a POS terminal, for instance.

3.3.5 Authorisation

EFT transactions require communication between a number of parties. When a card is used at a merchant or ATM, the transaction is first

routed to an acquirer, then through a number of networks to the issuer where the cardholder's account is held.

A transaction may be authorised *offline* by any of these entities through a stand-in agreement. Stand-in authorisation may be used when a communication link is not available, or simply to save communication cost or time. Stand-in is subject to the transaction amount being below agreed limits, known as floor limits. These limits are calculated based on the risk of authorising a transaction offline, and thus vary between merchants and card types. Offline transactions may be subject to other security checks such as checking the card number against a 'hotcard' (stolen card) list, velocity checks (limiting the number of offline transactions allowed by a cardholder) and random online authorisation.

Before online authorisation was standard practice and credit cards were processed using manual vouchers, each merchant would agree a limit ("floor limit) with his bank above which he must telephone for an authorisation code. If this was not carried out and the transaction subsequently was refused by the issuer ("bounced"), the merchant would not be entitled to a refund.

3.3.6 Dual Message Authorisation/Clearing

Depending on the business rules of the issuer, a "hold" may be placed on the funds authorised. This hold reserves that amount of money for a defined period. If a transaction is not cleared within the defined period then the "hold" will be removed and the funds made available again.

Example - Purchase for £10 on Day 2 never completes so hold removed on Day 4:

	Cleared Balance	Available Balance
Day 1	£100	£100
Day 2	£100	£90 (Hold for a purchase of £10)
Day 3	£100	£90
Day 4	£100	£100 (Hold for £10 purchase removed)

Example - Purchase for £10 on Day 2 completes on Day 4:

	Cleared Balance	Available Balance
Day 1	£100	£100

Day 2	£100	£90 (Hold for a purchase of £10)
Day 3	£100	£90
Day 4	£90	£90 (Transaction completes. Hold removed. Both balances updated with purchase amount)

An offline process, driven by the networks' clearing systems, generates clearing files which are sent to the card issuers on a daily basis. These files contain the completions messages to the on-line authorisations.

In addition, not all transactions in a dual-message environment require authorisation. Depending on the type of card used, and the floor-limit of the merchant, it may be that there are transactions in the clearing files which have not been authorised on-line. This is a financial exposure for banks as they have to honour the clearing records regardless of the balance on the cardholder's account.

Example - Purchase for £30 on Day 2 for a transaction not requiring authorisation:

	Cleared Balance	Available Balance
Day 1	£10	£10
Day 2	-£20	-£20 (Offline purchase of £30)

This transaction has to be applied even if the cardholder does not have sufficient funds or an overdraft.

3.3.7 Single Message Authorisation/Clearing

Some financial networks operate a single message solution, in which a transaction is authorised and cleared via the same message.

A transaction will be authorised via a *pre-authorisation* step, where the merchant requests the issuer to reserve an amount on the cardholder's account for a specific time, followed by *completion*, where the merchant requests an amount blocked earlier with a pre-authorisation. This transaction flow in two steps is often used in businesses such as hotels and car rental where the final amount is not known, and the pre-authorisation is made based on an estimated amount. Completion may form part of a *settlement* process, typically performed at the end of the day when the day's completed transactions are submitted. All these messages will be sent "on-line" from the merchant acquirer to the issuing bank.

3.3.8 Authentication

EFT transactions may be accompanied by methods to authenticate the card and the card holder. The merchant may manually verify the card holder's signature, or the card holder's Personal identification number (PIN) may be sent online in an encrypted form for validation by the card issuer. Other information may be included in the transaction, some of which is not visible to the card holder (for instance magnetic stripe data), and some of which may be requested from the card holder (for instance the card holder's address or the CVV2 value printed on the card).

EMV cards are smartcard-based payment cards, where the smartcard technology allows for a number of enhanced authentication measures.

3.4 Electronic Money

3.4.1 What is Electronic Money

Electronic money (also known as e-money, electronic cash, electronic currency, digital money, digital cash or digital currency) refers to money scrip which is exchanged only electronically. Typically, this involves use of computer networks, the internet and digital stored value systems. Electronic Funds Transfer (EFT) and direct deposit are examples of electronic money. Also, it is a collective term for financial cryptography and technologies enabling it.

While electronic money has been an interesting problem for cryptography (see for example the work of David Chaum and Markus Jakobsson), to date, use of digital cash has been relatively low-scale. One rare success has been Hong Kong, Octopus card system, which started as a transit payment system and has grown into a widely used electronic cash system. Singapore also has an electronic money implementation for its public transportation system (commuter trains, bus, etc), which is very similar to Hong Kong's Octopus card and based on the same type of card (FeliCa). A very successful implementation is in the Netherlands, known as Chipknip.

3.4.2 Alternative Systems

Technically electronic or digital money is a representation, or a system of debits and credits, used (but not limited to this) to exchange value, within another system, or itself as a stand alone system, online or offline. Also sometimes the term electronic money is used to refer to the provider itself. A private currency may use gold to provide extra security, such as digital gold currency. An e-currency system may be fully backed by gold (like e-gold and c-gold), non-gold backed, or both

gold and non-gold backed (like e-Bullion and Liberty Reserve). Also, some private organizations, such as the US military use private currencies such as Eagle Cash.

Many systems will sell their electronic currency directly to the end user, such as Paypal and WebMoney, but other systems, such as e-gold, sell only through third party digital currency exchangers.

In the case of Octopus Card in Hong Kong, deposits work similarly to banks'. After Octopus Card Limited receives money for deposit from users, the money is deposited into banks, which is similar to debit-card-issuing banks redepositing money at central banks.

Some community currencies, like some LETS systems, work with electronic transactions. Cyclos Software allows creation of electronic community currencies.

Ripple monetary system is a project to develop a distributed system of electronic money independent of local currency.

3.5 Off-Line Anonymous Electronic Money

In off-line electronic money the merchant does not need to interact with the bank before accepting a coin from the user. Instead he can collect multiple coins *Spent* by users and *Deposit* them later with the bank. In principle this could be done off-line, i.e. the merchant could go to the bank with his storage media to exchange e-cash for cash. Nevertheless the merchant is guaranteed that the user's e-coin will either be accepted by the bank, or the bank will be able to identify and punish the cheating user. In this way a user is prevented from spending the same coin twice (double-spending). Off-line e-cash schemes also need to protect against cheating merchants, i.e. merchants that want to deposit a coin twice (and then blame the user).

Using cryptography, anonymous ecash was introduced by David Chaum. He used blind signatures to achieve unlinkability between withdrawals and spend transactions. In cryptography, e-cash usually refers to anonymous e-cash. Depending on the properties of the payment transactions, one distinguishes between on-line and off-line e-cash. The first off-line e-cash system was proposed by Chaum and Naor. Like the first on-line scheme, it is based on RSA blind signatures.

3.5.1 Future Evolution

The main focuses of digital cash development are 1) being able to use it through a wider range of hardware such as secured credit cards; and 2)

linked bank accounts that would generally be used over an internet means, for exchange with a secure micropayment system such as in large corporations (PayPal).

Theoretical developments in the area of decentralized money are underway that may rival traditional, centralized money. Systems of accounting such as Altruistic Economics are emerging that are entirely electronic, and can be more efficient and more realistic because they do not assume a zero-sum transaction model.

3.5.2 Issues

Although digital cash can provide many benefits such as convenience and privacy, increased efficiency of transactions, lower transaction fees, new business opportunities with the expansion of economic activities on the Internet, there are many potential issues with the use of digital cash. The transfer of digital currencies raises local issues such as how to levy taxes or the possible ease of money laundering. There are also potential macroeconomic effects such as exchange rate instabilities and shortage of money supplies (total amount of digital cash versus total amount of real cash available, basically the possibility that digital cash could exceed the real cash available). These issues may only be addressable by some type of cyberspace regulations or laws that regulate the transactions and watch for signs of trouble.

3.6 Wire Transfer

3.6.1 What is: Wire Transfer

Wire transfer is a method of transferring money from one entity to another. A wire transfer can be made from one entity's bank account to the other entity's bank account, and by a transfer of cash at a cash office.

3.6.2 History

Although the genesis of the idea dates as far back as the giro, the modern wire transfer was a product of the telegraph companies, which made it possible to wire a money order from one office to another. Later, it became possible to wire money between banks, which is essentially the same process as the giro. Therefore, the term giro is still used for it in many other European countries.

3.6.3 Process

Bank wire transfers are often the most expedient method for transferring funds between bank accounts. A bank wire transfer is effected as follows:

- The person wishing to do a transfer (or someone who he has appointed and empowered financially to act on his behalf) goes to the bank and gives the bank the order to transfer a certain amount of money. IBAN and BIC code are given as well so the bank knows where the money needs to be sent to.
- The sending bank transmits a message, via a secure system (such as SWIFT or Fedwire), to the receiving bank, requesting that it effect payment according to the instructions given.
- The message also includes settlement instructions. The actual transfer is not instantaneous: funds may take several hours or even days to move from the sender's account to the receiver's account.
- Either the banks involved must hold a reciprocal account with each other, or the payment must be sent to a bank with such an account, a correspondent bank, for further benefit to the ultimate recipient.

3.6.4 Regulation

Bank transfer is the most common payment method in Europe, with several million transactions processed each day. Debit cards are used extensively to pay in stores, while monthly bills are usually paid with a direct transfer (by cellular phone or Internet, or at the bank or an ATM). In 2002, the European Commission relegated the regulation of the fees that a bank may charge for payments in euros between European Union member countries down to the domestic level, resulting in very low or no fees for transfers within the Eurozone; wire transfers between this zone and external areas can be expensive.

In the United States, domestic wire transfers are governed by Federal Regulation J and by Article 4A of the Uniform Commercial Code.

3.6.5 Security

Bank-to-bank wire transfer is considered the safest international payment method. Each account holder must have a proven identity. Chargeback is unlikely, although wires can be recalled. Information contained in wires is transmitted securely through encrypted communications methods. The price of bank wire transfers varies greatly, depending on the bank and its location; in some countries, the fee associated with the service can be costly.

Wire transfers done through cash offices are essentially anonymous and are designed for transfer between persons who trust each other. It is

unsafe to send money by wire to an unknown person to collect at a cash office: the receiver of the money may, after collecting it, simply disappear. This scam has been used often, especially in so-called Nigerian letters, also called *advance fee fraud* or *419 scams*.

International transfers involving the United States are subject to monitoring by the Office of Foreign Assets Control (OFAC), which monitors information provided in the text of the wire to ascertain whether money is being transferred to terrorist organizations or countries or entities under sanction by the United States government. If a financial institution suspects that funds are being sent from or to one of these entities, it must block the transfer and freeze the funds.

3.6.6 Methods

Western Union

One of the largest companies that offer wire transfer is Western Union, which allows individuals to transfer or receive money without an account with Western Union or any financial institution. Concern and controversy about Western Union transfers have increased in recent years, because of the increased monitoring of money-laundering transactions, as well as concern about terrorist groups using the service, particularly in the wake of the September 11, 2001 attacks. Although Western Union keeps information about senders and receivers, some transactions can be done essentially anonymously, for the receiver is not always required to show identification

International

Most international transfers are executed through SWIFT, a co-operative society, founded in 1974 by seven international banks, which operates a global network to facilitate the transfer of financial messages. Using these messages, banks can exchange data for funds transfer between financial institutions. SWIFT's headquarters are in La Hulpe, on the outskirts of Brussels, Belgium. The society also acts as a United Nations-sanctioned international-standards body, for the creation and maintenance of financial-messaging standards. See SWIFT Standards.

Each financial institution is provided an ISO 9362 code, also called a *Bank Identifier Code (BIC)* or *SWIFT Code*. These codes generally are eight characters long. For example: Deutsche Bank is an international bank, with its head office in Frankfurt, Germany, the SWIFT Code for which is *DEUTDEFF*:

- *DEUT* identifies Deutsche Bank.
- *DE* is the country code for Germany.
- *FF* is the code for Frankfurt.

Using an extended code of 11 digits (if the receiving bank has assigned extended codes to branches or to processing areas) allows the payment to be directed to a specific office. For example: DEUTDEFF500 would direct the payment to an office of Deutsche Bank in Bad Homburg.

United States

Banks in the United States use SWIFT to make payments to banks in other countries.

Domestic bank-to-bank transfers are conducted through the Fedwire system, which uses the Federal Reserve System and its assignment of routing transit number, which uniquely identify each bank.

4.0 CONCLUSION

Advances in information technology have presented financial institutions with several options of electronic transaction methods to facilitate business processes. The coming of the Internet and the World Wide Web has made the operation of these electronic payment options to be worthwhile. Despite some lapses especially in the area of security, electronic payment systems have come to stay in modern-day business financial transactions.

5.0 SUMMARY

- **Electronic bill payment** is a feature of online banking, similar in its effect to a giro, allowing a depositor to send money from his demand account to a creditor or vendor such as a public utility or a department store to be credited against a specific account.
- **EFTPOS** (short for *Electronic Funds Transfer at Point of Sale*) is an Australian and New Zealand electronic processing system for credit cards, debit cards and charge cards.
- EFT may be initiated by a cardholder when a payment card such as a credit card or debit card is used. This may take place at an automated teller machine (ATM) or point of sale (POS), or when the card is not present, which covers cards used for mail order, telephone order and internet purchases
- **Electronic money** (also known as **e-money**, **electronic cash**, **electronic currency**, **digital money**, **digital cash** or **digital currency**) refers to money which is exchanged only electronically.
- In off-line electronic money the merchant does not need to interact with the bank before accepting a coin from the user. Instead he can collect multiple coins *Spent* by users and *Deposit* them later with the

bank

- **Wire transfer** is a method of transferring money from one entity to another. A wire transfer can be made from one entity's bank account to the other entity's bank account, and by a transfer of cash at a cash office.
- Although the genesis of the idea dates as far back as the giro, the modern wire transfer was a product of the telegraph companies, which made it possible to wire a money order from one office to another
- Bank wire transfers are often the most expedient method for transferring funds between bank accounts
- Bank transfer is the most common payment method in Europe, with several million transactions processed each day
- Bank-to-bank wire transfer is considered the safest international payment method. Each account holder must have a proven identity.
- One of the largest companies that offer wire transfer is Western Union, which allows individuals to transfer or receive money without an account with Western Union or any financial institution.

6.0 TUTOR-MARKED ASSIGNMENT

1. Mention 10 transaction types that can be performed in an e-payment system

7.0 REFERENCES/FURTHER READING

EFTPOS. Merchant Banking Services. EFTPOS. Bank of Queensland Australia

Nab - Eftpos

ATMOSS - Australian Trade Mark Online Search System

Nab - Eftpos

David Chaum, Blind Signatures for Untraceable Payments, *Advances in Cryptology - Crypto '82*, Springer-Verlag (1983), 199-203. (PDF)

Chaum, D., Fiat, A., and Naor, M. (1990). "Untraceable electronic cash". In *Proceedings on Advances in Cryptology* (Santa Barbara, California, United States). S. Goldwasser, Ed. Springer-Verlag New York, 319-327. (PDF) registered

Regulation (EC) No 2560/2001. European Parliament and the Council of
the European Union

Regulation J - Check Collection and Funds Transfer.
BankersOnline.com

Section 4A of Universal Commercial Code. Legal Information Institute.

OFAC facts

Western Union Money Transfer Options

Can Western Union Keep On Delivering? *Business Week*

About BIC. Swift - BIC Portal

UNIT 5 AUTOMATED TELLER MACHINE

CONTENTS

- 1.0 Introduction
- 2.0 Objectives
- 3.0 Main Content
 - 3.1 History
 - 3.2 Location
 - 3.3 Financial Networks
 - 3.4 Global Use
 - 3.5 Security
 - 3.6 Alternative Uses
 - 3.7 Reliability
 - 3.8 Fraud
- 4.0 Conclusion
- 5.0 Summary
- 6.0 Tutor-Marked Assignment
- 7.0 References/Further Reading

1.0 INTRODUCTION

An automated teller machine (ATM) is a computerized telecommunications device that provides the customers of a financial institution with access to financial transactions in a public space without the need for a human clerk or bank teller. On most modern ATMs, the customer is identified by inserting a plastic ATM card with a magnetic stripe or a plastic smartcard with a chip, that contains a unique card number and some security information, such as an expiration date or CVC (CVV). Security is provided by the customer entering a personal identification number (PIN). They are sometimes referred to as "ATM machines", an example of RAS Syndrome.

Using an ATM, customers can access their bank accounts in order to make cash withdrawals (or credit card cash advances) and check their account balances as well as purchasing mobile cell phone prepaid credit. ATMs are known by various casual terms including *automated banking machine*, *money machine*, *bank machine*, *cash machine*, *hole-in-the-wall*, *cashpoint*, *Bancomat* (in various countries in Europe and Russia), *Multibanco* (after a registered trade mark, in Portugal), and *Any Time Money* (in India).

2.0 OBJECTIVES

At the end of this unit, you should be able to:

- define automated teller machine
- trace the history and development of ATM
- answer the question of what constitutes an ATM network
- identify the various uses of ATM
- explain now the security threats and solutions to the threats on ATM
- discuss the reliability of ATM's.

3.0 MAIN CONTENT

3.1 History

The first mechanical cash dispenser was developed and built by Luther George Simjian and installed in 1939 in New York City by the City Bank of New York, but removed after 6 months due to the lack of customer acceptance.

Thereafter, the history of ATMs paused for over 25 years, until De La Rue developed the first electronic ATM, which was installed first in Enfield Town in North London, United Kingdom on 27 June 1967 by Barclays Bank. This instance of the invention is credited to John Shepherd-Barron, although various other engineers were awarded patents for related technologies at the time. Shepherd-Barron was awarded an OBE in the 2005 New Year's Honours List. The first person to use the machine was the British variety artist and actor Reg Varney. The first ATMs accepted only a single-use token or voucher, which was retained by the machine. These worked on various principles including radiation and low-coercivity magnetism that was wiped by the card reader to make fraud more difficult. The machine dispensed pre-packaged envelopes containing ten pounds sterling. The idea of a PIN stored on the card was developed by the British engineer James Goodfellow in 1965.

In 1968, the networked ATM was pioneered in Dallas, Texas, by Donald Wetzel who was a department head at an automated baggage-handling company called Docutel. In 1995 the Smithsonian's National Museum of American History recognised Docutel and Wetzel as the inventors of the networked ATM.

ATMs first came into wide use in the UK in 1973; the IBM 2984 was designed at the request of Lloyds Bank. The 2984 CIT (Cash Issuing Terminal) was the first true Cashpoint, similar in function to today's machines; Cashpoint is still a registered trademark of Lloyds TSB in the

U.K. All were online and issued a variable amount which was immediately deducted from the account. A small number of 2984s were supplied to a USA bank. Notable historical models of ATMs include the IBM 3624 and 473x series, Diebold 10xx and TABS 9000 series, and NCR 5xxx series.

3.2 Location

ATMs are placed not only near or inside the premises of banks, but also in locations such as shopping centers/malls, airports, grocery stores, petrol/gas stations, restaurants, or any place large numbers of people may gather. These represent two types of ATM installations: on and off premise. On premise ATMs are typically more advanced, multi-function machines that complement an actual bank branch's capabilities and thus more expensive. Off premise machines are deployed by financial institutions and also ISOs (or Independent Sales Organizations) where there is usually just a straight need for cash, so they typically are the cheaper mono-function devices. In Canada, when an ATM is not operated by a financial institution it is known as a "White Label ATM".

In North America, banks often have drive-thru lanes providing access to ATMs.

Many ATMs have a sign above them indicating the name of the bank or organization owning the ATM, and possibly including the list of ATM networks to which that machine is connected. This type of sign is called a *topper*.

3.3 Financial Networks

Most ATMs are connected to interbank networks, enabling people to withdraw and deposit money from machines not belonging to the bank where they have their account or in the country where their accounts are held (enabling cash withdrawals in local currency). Some examples of interbank networks include PULSE, PLUS, Cirrus, Interac and LINK.

ATMs rely on authorization of a financial transaction by the card issuer or other authorizing institution via the communications network. This is often performed through an ISO 8583 messaging system.

Many banks charge ATM usage fees. In some cases, these fees are charged solely to users who are not customers of the bank where the ATM is installed; in other cases, they apply to all users. Many people oppose these fees because ATMs are actually less costly for banks than withdrawals from human tellers.

In order to allow a more diverse range of devices to attach to their networks, some interbank networks have passed rules expanding the definition of an ATM to be a terminal that either has the vault within its footprint or utilizes the vault or cash drawer within the merchant establishment, which allows for the use of a scrip cash dispenser.

ATMs typically connect directly to their ATM Controller via either a dial-up modem over a telephone line or directly via a leased line. Leased lines are preferable to POTS lines because they require less time to establish a connection. Leased lines may be comparatively expensive to operate versus a POTS line, meaning less-trafficked machines will usually rely on a dial-up modem. That dilemma may be solved as high-speed Internet VPN connections become more ubiquitous. Common lower-level layer communication protocols used by ATMs to communicate back to the bank include SNA over SDLC, TC500 over Async, X.25, and TCP/IP over Ethernet.

In addition to methods employed for transaction security and secrecy, all communications traffic between the ATM and the Transaction Processor may also be encrypted via methods such as SSL.

3.4 Global Use

There are no hard international or government-compiled numbers totaling the complete number of ATMs in use worldwide. Estimates developed by ATMIA place the number of ATMs in use at over 1.5 million as of August 2006.

For the purpose of analyzing ATM usage around the world, financial institutions generally divide the world into seven regions, due to the penetration rates, usage statistics, and features deployed. Four regions (USA, Canada, Europe, and Japan) have high numbers of ATMs per million people and generally slowing growth rates. Despite the large number of ATMs, there is additional demand for machines in the Asia/Pacific area as well as in Latin America. ATMs have yet to reach high numbers in the Near East/Africa.

The world's most northerly installed ATM is located at Longyearbyen, Svalbard, Norway.

The world's most southerly installed ATM is located at McMurdo Station, Antarctica.

While ATMs are ubiquitous on modern cruise ships, ATMs can also be found on some US Navy ships.

In the United Kingdom, an ATM may be colloquially referred to as a “Cashpoint”, named after the Lloyds Bank ATM brand, or “hole-in-the-wall”, after the equivalent Barclays brand. In Scotland the term Cashline has become a generic term for an ATM, based on the branding from the Royal Bank of Scotland.

3.5 Security

Security, as it relates to ATMs, has several dimensions. ATMs also provide a practical demonstration of a number of security systems and concepts operating together and how various security concerns are dealt with.

Physical

Early ATM security focused on making the ATMs invulnerable to physical attack; they were effectively safes with dispenser mechanisms. A number of attacks on ATMs resulted, with thieves attempting to steal entire ATMs by ram-raiding. Since late 1990s, criminal groups operating in Japan improved ram-raiding by stealing and using a truck loaded with a heavy construction machinery to effectively demolish or uproot an entire ATM and any housing to steal its cash.

Another attack method is to seal all openings of the ATM with silicone and fill the vault with a combustible gas or to place an explosive inside, attached, or near the ATM. This gas or explosive is ignited and the vault is opened or distorted by the force of the resulting explosion and the criminals can break in.

Modern ATM physical security, per other modern money-handling security, concentrates on denying the use of the money inside the machine to a thief, by means of techniques such as dye markers and smoke canisters.

Transactional Secrecy and Integrity

The security of ATM transactions relies mostly on the integrity of the secure cryptoprocessor: the ATM often uses commodity components that are not considered to be “trusted systems”.

Encryption of personal information, required by law in many jurisdictions, is used to prevent fraud. Sensitive data in ATM transactions are usually encrypted with DES, but transaction processors now usually require the use of Triple DES. Remote Key Loading techniques may be used to ensure the secrecy of the initialization of the encryption keys in the ATM. Message Authentication Code (MAC) or Partial MAC may also be used to ensure messages have not been

tampered with while in transit between the ATM and the financial network.

Customer Identity Integrity

There have also been a number of incidents of fraud where criminals have attached fake keypads or card readers to existing machines. These are then used to record customers' PINs and bank card information in order to gain unauthorized access to their accounts. Various ATM manufacturers have put in place countermeasures to protect the equipment they manufacture from these threats.

Alternate methods to verify cardholder identities have been tested and deployed in some countries, such as finger and palm vein patterns, iris, and facial recognition technologies. Cost of integrating and implementing these technologies along with concerns about consumer acceptance has limited their deployment so far.

Device Operation Integrity

Openings on the customer-side of ATMs are often covered by mechanical shutters to prevent tampering with the mechanisms when they are not in use. Alarm sensors are placed inside the ATM and in ATM servicing areas to alert their operators when doors have been opened by unauthorized personnel.

Rules are usually set by the government or ATM operating body that dictate what happens when integrity systems fail. Depending on the jurisdiction, a bank may or may not be liable when an attempt is made to dispense a customer's money from an ATM and the money either gets outside of the ATM's vault, or was exposed in a non-secure fashion, or they are unable to determine the state of the money after a failed transaction. Bank customers often complain that banks have made it difficult to recover money lost in this way, but this is often complicated by the bank's own internal policies regarding suspicious activities typical of the criminal element.

Customer security

Dunbar Armored ATM Techs watches over ATMs that have been installed in a van.

In some countries, multiple security cameras and security guards are a common feature. In the United States, The NY State Comptroller's Office has criticized the New York State Department of Banking for not following through on safety inspections of ATMs in high crime areas.

Critics of ATM operators assert that the issue of customer security appears to have been abandoned by the banking industry; it has been

suggested that efforts are now more concentrated on deterrent legislation than on solving the problem of forced withdrawals.

At least as far back as July 30, 1986, critics of the industry have called for the adoption of an emergency PIN system for ATMs, where the user is able to send a silent alarm in response to a threat. Legislative efforts to require an emergency PIN system have appeared in Illinois, Kansas and Georgia, but none have succeeded as of yet.

3.6 Alternative Uses

Although ATMs were originally developed as just cash dispensers, they have evolved to include many other bank-related functions. In some countries, especially those which benefit from a fully integrated cross-bank ATM network (e.g.: Multibanco in Portugal), ATMs include many functions which are not directly related to the management of one's own bank account, such as:

- Deposit currency recognition, acceptance, and recycling
- Paying routine bills, fees, and taxes (utilities, phone bills, social security, legal fees, taxes, etc.)
- Printing bank statements
- Updating passbooks
- Loading monetary value into stored value cards
- Purchasing
 - Postage stamps.
 - Lottery tickets
 - Train tickets
 - Concert tickets
 - Shopping mall gift certificates.
- Games and promotional features
- Donating to charities
- Cheque Processing Module
- Adding pre-paid cell phone credit.

Increasingly banks are seeking to use the ATM as a sales device to deliver pre approved loans and targeted advertising using products such as ITM (the Intelligent Teller Machine) from CR2 or Apra Relate from NCR. ATMs can also act as an advertising channel for companies to advertise their own products or third-party products and services.

In Canada, ATMs are called *guichets automatiques* in French and sometimes “Bank Machines” in English. The Interac shared cash network does not allow for the selling of goods from ATMs due to specific security requirements for PIN entry when buying goods. CIBC

machines in Canada are able to top-up the minutes on certain pay as you go phone's.

Manufacturers have demonstrated and have deployed several different technologies on ATMs that have not yet reached worldwide acceptance, such as:

1. Biometrics, where authorization of transactions is based on the scanning of a customer's fingerprint, iris, face, etc. Biometrics on ATMs can be found in Asia.
2. Cheque/Cash Acceptance, where the ATM accepts and recognises cheques and/or currency without using envelopes is expected to grow in importance in the US through Check 21 legislation.
3. Bar code scanning
4. On-demand printing of "items of value" (such as movie tickets, traveler's cheques, etc.)
5. Dispensing additional media (such as phone cards)
6. Co-ordination of ATMs with mobile phones
7. Customer-specific advertising
8. Integration with non-banking equipment

3.7 Reliability

Before an ATM is placed in a public place, it typically has undergone extensive testing with both test money and the backend computer systems that allow it to perform transactions. Banking customers also have come to expect high reliability in their ATMs, which provides incentives to ATM providers to minimize machine and network failures. Financial consequences of incorrect machine operation also provide high degrees of incentive to minimize malfunctions.

ATMs and the supporting electronic financial networks are generally very reliable, with industry benchmarks typically producing 98.25% customer availability for ATMs and up to 99.999% availability for host systems. If ATMs do go out of service, customers could be left without the ability to make transactions until the beginning of their bank's next time of opening hours.

Of course, not all errors are to the detriment of customers; there have been cases of machines giving out money without debiting the account, or giving out higher value notes as a result of incorrect denomination of banknote being loaded in the money cassettes. Errors that can occur may be mechanical (such as card transport mechanisms; keypads; hard disk failures); software (such as operating system; device driver; application); communications; or purely down to operator error.

To aid in reliability, some ATMs print each transaction to a roll paper journal that is stored inside the ATM, which allows both the users of the ATMs and the related financial institutions to settle things based on the records in the journal in case there is a dispute. In some cases, transactions are posted to an electronic journal to remove the cost of supplying journal paper to the ATM and for more convenient searching of data.

Improper money checking can cause the possibility of a customer receiving counterfeit banknotes from an ATM. While bank personnel are generally trained better at spotting and removing counterfeit cash, the resulting ATM money supplies used by banks provide no absolute guarantee for proper banknotes, as the Federal Criminal Police Office of Germany has confirmed that there are regularly incidents of false banknotes having been provided through bank ATMs. Some ATMs may be stocked and wholly owned by outside companies, which can further complicate this problem when it happens. Bill validation technology can be used by ATM providers to help ensure the authenticity of the cash before it is stocked in an ATM; ATMs that have cash recycling capabilities include this capability.

3.8 Fraud

As with any device containing objects of value, ATMs and the systems they depend on to function are the targets of fraud. Fraud against ATMs and people's attempts to use them takes several forms.

The first known instance of a fake ATM was installed at a shopping mall in Manchester, Connecticut in 1993. By modifying the inner workings of a Fujitsu model 7020 ATM, a criminal gang known as The Bucklands Boys were able to steal information from cards inserted into the machine by customers.

In some cases, bank fraud could occur at ATMs whereby the bank accidentally stocks the ATM with bills in the wrong denomination, therefore giving the customer more money than should be dispensed. The result of receiving too much money may be influenced on the card holder agreement in place between the customer and the bank.

In a variation of this, WAVY-TV reported an incident in Virginia Beach of September 2006 where a hacker who had probably obtained a factory-default admin password for a gas station's white label ATM caused the unit to assume it was loaded with \$5 USD bills instead of \$20s, enabling himself--and many subsequent customers--to walk away with four times the money they said they wanted to withdraw.

ATM behavior can change during what is called "stand-in" time, where the bank's cash dispensing network is unable to access databases that contain account information (possibly for database maintenance). In order to give customers access to cash, customers may be allowed to withdraw cash up to a certain amount that may be less than their usual daily withdrawal limit, but may still exceed the amount of available money in their account, which could result in fraud

Card Fraud

In an attempt to prevent criminals from shoulder surfing the customer's PINs, some banks draw privacy areas on the floor.

For a low-tech form of fraud, the easiest is to simply steal a customer's card. A later variant of this approach is to trap the card inside of the ATM's card reader with a device often referred to as a Lebanese loop. When the customer gets frustrated by not getting the card back and walks away from the machine, the criminal is able to remove the card and withdraw cash from the customer's account.

Another simple form of fraud involves attempting to get the customer's bank to issue a new card and stealing it from their mail.

Some ATMs may put up warning messages to customers to not use them when it detects possible tampering

The concept and various methods of copying the contents of an ATM card's magnetic stripe on to a duplicate card to access other people's financial information was well known in the hacking communities by late 1990.

In 1996, Andrew Stone, a computer security consultant from Hampshire in the UK, was convicted of stealing more than £1 million (at the time equivalent to US\$1.6 million) by pointing high definition video cameras at ATMs from a considerable distance, and by recording the card numbers, expiry dates, etc. from the embossed detail on the ATM cards along with video footage of the PINs being entered. After getting all the information from the videotapes, he was able to produce clone cards which not only allowed him to withdraw the full daily limit for each account, but also allowed him to sidestep withdrawal limits by using multiple copied cards. In court, it was shown that he could withdraw as much as £10,000 per hour by using this method. Stone was sentenced to five years and six months in prison.

By contrast, a newer high-tech *modus operandi* involves the installation of a magnetic card reader over the real ATM's card slot and the use of a wireless surveillance camera or a modified digital camera to observe the

user's PIN. Card data is then cloned onto a second card and the criminal attempts a standard cash withdrawal. The availability of low-cost commodity wireless cameras and card readers has made it a relatively simple form of fraud, with comparatively low risk to the fraudsters.

In an attempt to stop these practices, countermeasures against card cloning have been developed by the banking industry, in particular by the use of [smart cards](#) which cannot easily be copied or spoofed by unauthenticated devices, and by attempting to make the outside of their ATMs [tamper evident](#). Older chip-card security systems include the French [Carte Bleue](#), [Visa Cash](#), [Mondex](#), [Blue from American Express](#) and [EMV '96 or EMV 3.11](#). The most actively developed form of smart card security in the industry today is known as [EMV 2000 or EMV 4.x](#).

[EMV](#) is widely used in the UK ([Chip and PIN](#)) and other parts of Europe, but when it is not available in a specific area, ATMs must fallback to using the easy to copy magnetic stripe to perform transactions. This fallback behaviour can be exploited. However the fallback option has been removed by several UK banks, meaning if the chip is not read, the transaction will be declined.

4.0 CONCLUSION

Automated Teller Machines (ATMs) has been around for quiet some time now and has undergone lots of changes and improvements to match the challenges of today compared to when they were first introduced. Since their first installment, the number has grown so much especially in developing countries. The future trend for ATM remains how to improve the security of the ATM itself and the legitimate end users. The safer the ATM the better for all.

5.0 SUMMARY

- An automated teller machine (ATM) is a computerized telecommunications device that provides the customers of a financial institution with access to financial transactions in a public space without the need for a human clerk or bank teller.
- The first mechanical cash dispenser was developed and built by Luther George Simjian and installed in 1939 in New York City by the City Bank of New York, but removed after 6 months due to the lack of customer acceptance.
- ATMs are placed not only near or inside the premises of banks, but also in locations such as shopping centers/malls, airports, grocery stores, petrol/gas stations, restaurants, or any place large numbers of people may gather.

- Most ATMs are connected to interbank networks, enabling people to withdraw and deposit money from machines not belonging to the bank where they have their account or in the country where their accounts are held
- There are no hard international or government-compiled numbers totaling the complete number of ATMs in use worldwide. Estimates developed by ATMIA place the number of ATMs in use at over 1.5 million as of August 2006.
- Security, as it relates to ATMs, has several dimensions. ATMs also provide a practical demonstration of a number of security systems and concepts operating together and how various security concerns are dealt with.
- Although ATMs were originally developed as just cash dispensers, they have evolved to include many other bank-related functions
- Before an ATM is placed in a public place, it typically has undergone extensive testing with both test money and the backend computer systems that allow it to perform transactions.
- As with any device containing objects of value, ATMs and the systems they depend on to function are the targets of fraud. Fraud against ATMs and people's attempts to use them takes several forms.

6.0 TUTOR-MARKED ASSIGNMENT

1. Briefly discuss physical measures to secure an ATM
2. Mention 10 alternative uses of ATM apart from use in banking

7.0 REFERENCES/FURTHER READING

“The Man Who Invented the Cash Machine”. BBC News.

“Pins and Needles”. Guardian Unlimited (20 January 2005).

“ATM Inventor Honoured”. BBC News.

Eicon Networks Develops SSL-VPN. For Secure Remote Working IT
Observer

Number of ATMs Worldwide Expected to Hit 1.5 Million in December
www.atmmarketplace.com article

Statistics on Payment and Settlement Systems in Selected Countries -
Figures for 2004 Bank for International Settlements

Central Bank Payment System Information Bank for International
Settlements

Financial Access and Financial stabilityPDF (69.5 KiB) Bank for International Settlements, Penelope Hawkins

“Cards: Biometrics Stalled Amid the Hype” International Biometric Industry Association

“Consumer Complaint Board: Banks also Responsible for the Success of ATM Withdrawals Abroad” Kuluttajavirasto (Finnish Consumer Agency & Ombudsman)

“*New Reasons to Guard Your ATM Card*” Christian Science Monitor via MSN

“*Text of the ATM Safety Act*” State of New York Banking Department

DiNapoli Calls for Better Oversight of Bank ATMs

“*Consultants Call for Increased ATM Security Measures*”
www.atmmarketplace.com, Jane Blake, December 4, 2000.

“ATM Report” Illinois Department of Financial and Professional Regulation

“Rising Interest Rates, Gas Prices Hit Vault-Cash Providers”
www.selfserviceworld.com

NCR and Fujitsu Develop Cash Deposit and Bill Recycling Module for ATMs Fujitsu

“Indonesians make ATM sacrifices”, Bank puts the ‘fun’ into ‘funds’, BBC article about purchasing livestock for the poor in Indonesia

“Consumers’ FAQ, IDP Point 4” *Interac*

Japan Post to go with fingerprints for ATMs. *The Japan Times*

“*Place Your Hand on the Scanner*” Web Japan

Sensar Has its Eye on the Prize With \$42 Million Japanese Deal.
American City Business Journals

Higher Sales, Lower Costs, Better Experience—Self-Service Promises It All, BAI

Japanese Bank to Allow Cellphone ATM Access Engadget

Automated Gas Pumping Station and ATM MCF547x ColdFire
Freescale

“Mad Rush to Faulty ATM in France”, BBC Report about a Cash
Machine not being Stocked Correctly

“ATM Turns \$5s into \$20s” CNN/WAVY Report, 9/14/06, about a
Hacked ATM at a Gas Station

Fun with Automatic Tellers Phrack Magazine Volume One, Issue Eight

“Automatic Teller Machine Cards” Phrack Magazine, Phrack Classic
Volume Three, Issue 32.

Seeking After the Truth in Computer Evidence: any Proof of ATM
Fraud? Oxford Journals *ITNOW*

‘What the Hell Do Smart Cards Do?’ *Fast Company*.

Postal Service Mailing Kiosks Now in Every State United States Postal
Service News Release

Automated Postal Centers PostalReporter.com news report

MODULE 3

Unit 1	Internet/Electronic Crimes and Fraud 1
Unit 2	Internet/Electronic Crimes and Fraud 2
Unit 3	Risk of E-Finance: Money Laundering
Unit 4	WWW Security Management

UNIT 1 INTERNET/ELECTRONIC CRIMES AND FRAUD 1

CONTENTS

1.0	Introduction
2.0	Objectives
3.0	Main Content
3.1	Purchase Scams
3.2	Money Transfers Fraud
3.3	Click Fraud
3.4	International Modern Dialing
3.5	Internet Marketing and Retail Fraud
3.6	Internet Marketing SEO Fraud
3.7	Auction and Retail Schemes Online
3.8	Click Fraud
3.9	Avoiding Internet Investment Scams
4.0	Conclusion
5.0	Summary
6.0	Tutor-Marked Assignment
7.0	References/Further Reading
1.0	INTRODUCTION

Internet fraud

The term “Internet fraud” generally refers to any type of fraud scheme that uses one or more online services - such as chat rooms, e-mail, message boards, or Web sites - to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

- define the various forms of electronic finance and banking related frauds
- discuss what constitutes each type of electronic fraud
- explain how to identify and avoid electronic frauds
- explain some of the legal cases and the outcomes.

3.0 MAIN CONTENT

3.1 Purchase Scams

Direct solicitations

The most straightforward type of purchase scam is a buyer in another country approaching many merchants through spamming them and directly asking them if they can ship to them using credit cards to pay.

Most likely, a few weeks or months after the merchant ships and charges the credit card, he/she will be hit with a chargeback from the credit card processor and lose all the money.

Counterfeit Postal Money Orders

According to the FBI and postal inspectors, there has been a significant surge in the use of Counterfeit Postal Money Orders since October 2004. More than 3,700 counterfeit postal money orders (CPMOs) were intercepted by authorities from October to December 2004, and according to the USPS, the “quality” of the counterfeits is so good that ordinary consumers can easily be fooled.

On March 9, 2005, the FDIC issued an alert stating that it had learned that counterfeit U.S. Postal Money Orders had been presented for payment at financial institutions.

On April 26, 2005, Tom Zeller Jr. wrote an article in The New York Times regarding a surge in the quantity and quality of the forging of U.S. Postal Money Orders, and its use to commit online fraud. The article shows a picture of a man that had been corresponding with a woman in a country through a dating site, and received several fake postal money orders after the woman asked him to buy a computer and mail it to her.

Who has received Counterfeit Postal Money Orders (CPMOs):

- Small Internet retailers.
- Classified advertisers.
- Individuals that have been contacted through email or chat rooms by fraudsters posing as prospective social interests or business partners, and convinced to help the fraudsters unknowingly.

The penalty for making or using counterfeit postal money orders is up to ten years in jail and a US\$25,000 fine.

Online automotive fraud

There are two basic schemes in online automotive fraud:

1. A fraudster posts a vehicle for sale on an online site, generally for luxury or sports cars advertised for thousands less than market value. The details of the vehicle, including photos and description, are typically lifted from sites such as eBay Motors and re-posted elsewhere. An interested buyer, hopeful for a bargain, emails the seller, who responds saying the car is still available but is located overseas. He then instructs the buyer to send a deposit via wire transfer to initiate the "shipping" process. The unwitting buyer wires the funds, and doesn't discover until days or weeks later that they were scammed.
2. A fraudster feigns interest in an actual vehicle for sale on the Internet. The "buyer" explains that a client of his is interested in the car, but due to an earlier sale that fell through has a certified check for thousands more than the asking price and requests the seller to send the balance via wire transfer. If the seller agrees to the transaction, the buyer sends the certified check via express courier. The seller takes the check to their bank, which makes the funds available immediately. Thinking the bank has cleared the check, the seller follows through on the transaction by wiring the balance to the buyer. Days later, the check bounces and the seller realizes they have been scammed. But the money has long since been picked up and is not recoverable.

In another type of fraud, a fraudster contacts the seller of an automobile, asking for the vehicle identification number, putatively to check the accident record of the vehicle. However, the supposed buyer actually uses the VIN to make fake papers for a stolen car that is then sold.

Cash the check system

In some cases, fraudsters approach merchants and ask for large orders: \$50,000 to \$200,000, and agree to pay via wire transfer in advance. After brief negotiation, the buyer gives an excuse about the impossibility of sending a bank wire transfer. The buyer then offers to send a check, stating that the merchant can wait for the check to clear before shipping any goods. The check received, however, is a counterfeit of a check from a medium to large U.S. Company. If asked, the buyer will claim that the check is money owed from the large company. The merchant deposits the check and it clears, so the goods are sent. Only later, when the larger company notices the check, will the merchant's account be debited.

In some cases, the fraudsters agree to the wire but ask the merchant for their bank's address. The fraudsters send the counterfeited check directly to the merchant's bank with a note asking to deposit it to the merchant's account. Unsuspecting bank officers deposit the check, and then the

fraudster contacts the merchant stating that they made a [direct deposit](#) into the merchant's account.

Re-shippers

Re-shipping scams trick individuals or small businesses into shipping goods to countries with weak legal systems. The goods are generally paid for with stolen or fake credit cards.

Call tag scam

The [Merchant Risk Council](#) reported that the “[call tag](#)” scam re-emerged over the 2005 holidays and several large merchants suffered losses. Under the scheme, criminals use stolen credit card information to purchase goods online for shipment to the legitimate cardholder. When the item is shipped and the criminal receives tracking information via email, he/she calls the cardholder and falsely identifies himself as the merchant that shipped the goods, saying that the product was mistakenly shipped and asking permission to pick it up upon receipt. The criminal then arranges the pickup issuing a “call tag” with a shipping company different from the one the original merchant used. The cardholder normally doesn't notice that there is a second shipping company picking up the product, which in turn has no knowledge it is participating in a fraud scheme. The cardholder then notices a charge in his card and generates a chargeback to the unsuspecting merchant.

Business Opportunity/“Work-at-Home” Schemes

Fraudulent schemes often use the Internet to advertise purported business opportunities that will allow individuals to earn thousands of dollars a month in “work-at-home” ventures. These schemes typically require the individuals to pay anywhere from \$35 to several hundred dollars or more, but fail to deliver the materials or information that would be needed to make the work-at-home opportunity a potentially viable business.

Often, after paying a registration fee, the applicant will be sent advice on how to place ads similar to the one that recruited him in order to recruit others, which is effectively a pyramid scheme.

Other types of work at home scams include [home assembly kits](#). The applicant pays a fee for the kit, but after assembling and returning the item, it's rejected as [substandard](#), meaning the applicant is out of pocket for the materials. Similar scams include home-working [directories](#), [medical billing](#), [data entry](#) ([data entry scam](#)) at home or reading books for money.

3.2 Money Transfer Fraud

This type of fraud consists of an employment offer to help transfer money to a foreign company, supposedly because it costs too much to do it through other methods (which is usually not the case). The prospective victim receives fake email. The fraudsters will then send fake checks or postal money orders, in the hopes of getting the victims to cash those fake money instruments and then getting real money from the victims.

These scams are also used as [phishing](#) tools, because many times the fraudsters are able to get the victims' full name, address, social security, bank account number, etc, which ends up being identity fraud.

3.3 Click Fraud

The latest scam to hit the headlines is the multi-million dollar [click fraud](#) which occurs when advertising network affiliates force paid views or clicks to ads on their own websites via [spyware](#), the affiliate is then paid a commission on the [cost-per-click](#) that was artificially generated. Affiliate programs such as Google's [AdSense](#) capability pay high commissions that drive the generation of bogus clicks. With paid clicks costing as much as US\$100 and an online advertising industry worth more than US\$10 [billion](#), this form of Internet fraud is on the increase.

3.4 International Modern Dialing

Customers of dial-up Internet Service Providers, such as AOL, use a modem to dial a local connection number. Some web sites, normally containing adult content, use international dialing to trick consumers into paying to view content on their web site. Often these sites purport to be free and advertise that no credit card is needed. They then prompt the user to download a "viewer" or "dialer" to allow them to view the content. Once the program is downloaded it disconnects the computer from the Internet and proceeds to dial an international long distance or premium rate number, charging anything up to [US\\$7-8](#) per minute. An international block is recommended to prevent this, but in the U.S. and Canada, calls to the Caribbean (except Haiti) can be dialed with a "1" and a three-digit area code, so such numbers, as well as "10-10 dial-round" phone company prefixes, can circumvent an international block.

3.5 Internet Marketing and Retail Fraud

This is a fast-growing area of internet fraud perpetrated by dishonest internet marketing and retail sites. A variety of products and services are involved. The customer is tricked by a legitimate-looking site and effective marketing into giving their credit card information and CVV number, or sending cash by other means, in exchange for what they believe to be the goods or services. The goods are never arrive, turn out to be fake, or are products worth less than those advertised.

Where a credit card is involved, the perpetrators may also aim to use the customer's credit card information to obtain cash or to make purchases of their own. A common example of this type of fraud are pornographic websites that advertise free access. Upon further inspection, however, a credit card is required "for age verification purposes only." The scammers then use your credit card information to make large charges to the credit card.

In cases involving fake or worthless goods, many are health products, related to [health fraud](#). These products might advertise anything from a quick way to loose weight to a cure for a serious disease, and may:

- promise a lot, claiming they can "do it all"
- claim to be a "scientific breakthrough", featuring fake doctors or scientists making claims for the product, with technical jargon that only experts in the field know is used falsely
- feature a long list of "personal testimonials", with no way to check if they are true or fake.

Once your credit card information is given to these type of scam companies, they usually will charge you no matter what type of cancellation you attempt to go through. This can often be overcome by contacting the [credit card](#) company. Credit and consumer protection laws in many countries hold the credit card company liable to refund their customers' money for goods or services purchased with the card but not delivered. The loss is then suffered by the card company, but ultimately passed on to customers in higher interest and fees.

Internet ticket fraud

A variation of internet marketing fraud is offering tickets to sought-after events such as concerts, shows and sports events. The tickets turn out to be fake or are simply never delivered. The proliferation of online ticket agencies and the existence of experienced and dishonest [ticket touts](#) has fuelled this kind of fraud in recent years. Many such scams are run by [British](#) ticket touts, though they may base their operations in other countries.

A prime example was the global [Beijing Olympic Games](#) ticket fraud run by US-registered Xclusive Leisure and Hospitality, sold through a professionally-designed website, www.beijingticketing.com with the name “Beijing 2008 Ticketing”. On 4 August it was reported that more than \$50 million worth of fake tickets had been sold through the website. On 6 August it was reported that the person behind the scam, which was wholly based outside China, was a British ticket tout, Terance Shepherd.

3.6 Internet Marketing SEO Fraud

This type of fraud involves a supposed internet marketing specialist presenting a prospective client with detailed graphs and charts that indicate that his web site receives (x) thousands of hits per month, emphasizing that if you pay for his services you will succeed in getting a number clicks converted to customers or clients.

When you receive no request for more information and no clients, the fraudster responds that it must be something your web site is not doing right.

3.7 Auction and Retail scheme Online

Fraudsters launch auctions on eBay or TradeMe with very low prices and no reservations especially for high priced items like watches, computers or high value collectibles. They received payment but never deliver, or deliver an item that is less valuable than the one offered, such as counterfeit, refurbished or used. Some fraudsters also create complete webstores that appear to be legitimate, but they never deliver the goods. An example of such a fraudulent site is marselle.com, jeremimora.com, thiesbikestore.com. They take payment but never shipped the order. In some cases, some stores or auctioneers are legitimate but eventually they stopped shipping after cashing the customers' payments.

Sometimes fraudsters will combine phishing to hijacking legitimate member accounts on eBay, typically with very high numbers of positive feedback, and then set up a phony online store. They received payment usually via check, money-order, cash or wire transfer but never deliver the goods; then they leave the poor, unknowing eBay member to sort out the mess. In this case the fraudster collects the money while ruining the reputation of the conned eBay member and leaving a large number of people without the goods they thought they purchased.

3.8 Click Fraud

Introduction

Click fraud is a type of [internet crime](#) that occurs in [pay per click online advertising](#) when a person, automated script, or computer program imitates a legitimate user of a [web browser](#) clicking on an ad, for the purpose of generating a [charge per click](#) without having actual interest in the target of the ad's link. Click fraud is the subject of some controversy and increasing litigation due to the advertising networks being a key beneficiary of the fraud.

Use of a computer to commit this type of [Internet fraud](#) is a [felony](#) in many jurisdictions, for example as covered by [Penal code 502](#) in [California](#), USA, and the [Computer Misuse Act 1990](#) in the [United Kingdom](#). There have been arrests relating to click fraud with regard to malicious clicking in order to deplete a competitor's advertising budget.

Pay per click advertising

[Pay per click](#) advertising or PPC advertising is an arrangement in which [webmasters](#) (operators of web sites), acting as publishers, display clickable links from advertisers, in exchange for a [charge per click](#). As this industry evolved, a number of advertising networks developed which acted as middlemen between these two groups (publishers and advertisers). Each time a (believed to be) valid web user clicks on an ad, the advertiser pays the advertising network, who in turn pays the publisher a share of this money. This revenue sharing system is seen as an incentive for click fraud.

The largest of the advertising networks, [Google's AdWords/AdSense](#) and [Yahoo! Search Marketing](#), act in a dual role, since they are also publishers themselves (on their search engines). According to critics, this complex relationship may create a conflict of interest. For instance, Google loses money to undetected click fraud when it pays out to the publisher, but it makes more money when it collects fees from the advertiser. Because of the spread between what Google collects and what Google pays out, click fraud directly and invisibly profits Google.

Non-Contracting Parties

A secondary source of click fraud is non-contracting parties, who are not part of any pay-per-click agreement. This type of fraud is even harder to police because perpetrators generally cannot be sued for breach of contract or charged criminally with fraud.

Examples of non-contracting parties are:

- **Competitors of advertisers:** These parties may wish to harm a competitor who advertises in the same market by clicking on their ads. The perpetrators don't profit directly, but force the advertiser to pay for irrelevant clicks thus weakening or eliminating a source of competition.
- **Competitors of publishers:** These persons may wish to frame a publisher. It is made to look like the publisher is clicking on its own ads. The advertising network may then terminate the relationship. Many publishers rely exclusively on revenue from advertising and can be put out of business by such an attack.
- **Other malicious intent:** As with [vandalism](#), there's an array of motives for wishing to cause harm to either an advertiser or a publisher, even by people who have nothing to gain financially. Motives include political and personal vendettas. These cases are often the hardest to deal with, since it is difficult to track down the culprit, and if found, there is little legal action that can be taken against them.
- **Friends of the publisher:** Sometimes upon learning a publisher profits from ads being clicked, a supporter of the publisher (like a fan, family member, or personal friend), will click on the ads to help. However, this can backfire when the publisher (not the friend) is accused of click fraud.

Advertising networks try to stop fraud by all parties, but often do not know which clicks are legitimate. Unlike fraud committed by the publisher, it is difficult to know who should pay when past click fraud is found. Publishers resent having to pay refunds for something that is not their fault. However, advertisers are adamant that they should not have to pay for phony clicks.

Organization

Click fraud can be as simple as one person starting a small web site, becoming a publisher of ads, and clicking on those ads to generate revenue. Often the number of clicks and their value is so small that the fraud goes undetected. Frequently publishers will claim small amounts of such clicking is an accident, which is often the case.

Much larger scale fraud also occurs. Those engaged in large scale fraud will often run [scripts](#) which simulate a human clicking on ads in web pages. However, huge numbers of clicks appearing to come from just one, or a small number of computers, or a single geographic area, look highly suspicious to the advertising network and advertisers. Clicks coming from a computer known to be that of a publisher also look

suspicious to those watching for click fraud. A person attempting large scale fraud, alone in their home, stands a good chance of being caught.

One type of fraud that circumvents detection based on IP patterns is one that uses existing user traffic, turning this into clicks or impressions. Such an attack can be camouflaged from users by using 0-size iframes to display advertisements that are programmatically retrieved using JavaScript. It could also be camouflaged from advertisers and portals by ensuring that so-called reverse [spiders](#) are presented with a legitimate page, while human visitors are presented with a page that commits click-fraud. The use of 0-size iframes and other techniques involving human visitors may also be combined with the use of incentivized traffic, where members of “Paid to Read” sites are paid small amounts of money (often a fraction of a cent) to visit a website and/or click on keywords and search results, sometimes hundreds or thousands of times every day. Some owners of PTR sites are members of PPC engines, and may send many email ads to users who do search, while sending little ads to those who don't. They do this mainly because the charge per click on search results is often the only source of revenue to the site. This is known as “forced searching,” a practice that is frowned upon in the Get Paid To industry.

Organized crime can handle this by having many computers with their own Internet connections in different geographic locations. Often scripts fail to mimic true human behavior, so organized crime networks use [Trojan](#) code to turn the average person's machines into [zombie computers](#) and using sporadic [redirects](#) or [DNS cache poisoning](#) to turn the oblivious user's actions into actions generating revenue for the scammer. It can be difficult for advertisers, advertising networks, and authorities to pursue cases against networks of people spread around multiple countries.

[Impression fraud](#) is when falsely generated ad impressions affect an advertiser's account. In the case of [click-through rate](#) based auction models, the advertiser may be penalized for having an unacceptably low click-through for a given [keyword](#). This involves making numerous searches for a keyword but without clicking of the ad. Such ads are disabled automatically, enabling a competitor's lower-bid ad for the same keyword to continue while several high bidders (on the first page of the search results) have been eliminated.

Legal cases

Class action lawsuits

- Disputes over the issue have resulted in a number of lawsuits. In one case, Google (acting as both an advertiser and advertising network) won a lawsuit against a Texas company called Auction Experts

(acting as a publisher), which Google accused of paying people to click on ads that appeared on Auction Experts' site, costing advertisers \$50,000[3]. Despite networks' efforts to stop it, publishers are suspicious of the motives of the advertising networks because the advertising network receives money for each click, even if it is fraudulent.

- In July 2005, Yahoo settled a class action lawsuit against it by plaintiffs alleging it did not do enough to prevent click fraud. Yahoo paid \$4.5 million in legal bills for the plaintiffs, and agreed to settle advertiser claims dating back to 2004 [4]. In July 2006, Google settled a similar suit for \$90 million [5][6].
- On March 8, 2006, Google agreed to a \$90 million settlement fund in the class action lawsuit filed by Lane's Gifts & Collectibles. [7]. The class action lawsuit was filed in Miller County, Arkansas by Dallas attorneys, Steve Malouf, Joel Fineberg, and Dean Gresham.]

Michael Anthony Bradley

In 2004, California resident [Michael Anthony Bradley](#) created "[Google Clique](#)", a software program that he claimed could let spammers defraud [Google](#) out of millions of dollars in fraudulent clicks. Authorities said he was arrested while trying to [blackmail](#) Google for \$150,000 to hand over the program, believed to be the first arrest for click fraud.

Charges were dropped without explanation on [November 22, 2006](#); both the US Attorney's office and Google declined to comment. [Business Week](#) suggests that Google was unwilling to cooperate with the prosecution, as it would be forced to publicly disclose its click fraud detection techniques, and as it also makes money from fraudulent clicks.

Solutions

Proving click fraud can be very difficult, since it is hard to know who is behind a computer and what their intentions are. Often the best an advertising network can do is to identify which clicks are most likely fraudulent and not charge the account of the advertiser. Even more sophisticated means of detection are used, but none is foolproof.

[The Tuzhilin report](#), produced as part of a click fraud lawsuit settlement, has a detailed and comprehensive discussion of these issues. In particular, it defines "the Fundamental Problem of invalid (fraudulent) clicks":

- "There is no conceptual definition of invalid clicks that can be operationalized [except for certain obviously clear cases]."
- "An operational definition cannot be fully disclosed to the general public because of the concerns that unethical users will take

advantage of it, which may lead to a massive click fraud. However, if it is not disclosed, advertisers cannot verify or even dispute why they have been charged for certain clicks.”

The pay-per-click industry is lobbying for tighter laws on the issue. Many hope to have laws that will cover those not bound by contracts. A number of companies are developing viable solutions for click fraud identification and are developing intermediary relationships with advertising networks. Such solutions fall into two categories:

1. Forensic analysis of advertisers’ web server log files.

This analysis of the advertiser's web server data requires an in-depth look at the source and behavior of the traffic. As industry standard log files are used for the analysis, the data is verifiable by advertising networks. The problem with this approach is that it relies on the honesty of the middlemen in identifying fraud.

2. Third-party corroboration

Third parties offer web-based solutions that might involve placement of single-pixel images or Javascript on the advertiser's web pages and suitable tagging of the ads. The visitor may be presented with a cookie. Visitor information is then collected in a third-party data store and made available for download. The better offerings make it easy to highlight suspicious clicks and they show the reasons for such a conclusion. Since an advertiser's log files can be tampered with, their accompaniment with corroborating data from a third party forms a more convincing body of evidence to present to the advertising network. However, the problem with third-party solutions is that such solutions see only part of the traffic of the entire network. Hence, they can be less likely identify patterns that span several advertisers. In addition, due to the limited amount of traffic they receive, when compared to middlemen, they can be overly or less aggressive when judging traffic to be fraud.

Click Fraud in Academia

The fact that the middlemen (search engines) have the upper hand in the operational definition of invalid clicks is the reason for the conflict of interest between advertisers and the middlemen, as described above. This is manifested in [the Tuzhilin report](#) as described above. The Tuzhilin report did not publicly define invalid clicks and did not describe the operational definitions in detail. Rather, it gave a high-level picture of the fraud detection system and argued that the operational definition of the search engine under investigations is "reasonable." One aim of the report was to preserve the privacy of the fraud detection system in order to maintain its effectiveness. This prompted some

researchers to conduct public research on how the middlemen can fight click fraud. Since such research is presumably not tainted by market forces, there is hope that this research can be adopted to assess how rigorous a middleman is in detecting click fraud in future law cases. The fear that this research can expose the internal fraud detection system of middlemen still applies. An example of such research is that done by [Metwally, Agrawal](#) and [El Abbadi](#) at [UCSB](#). Recent work by [Majumdar, Kulkarni](#), and [Ravishankar](#) at [UC Riverside](#) proposes protocols for the identification of fraudulent behavior by brokers and other intermediaries in content-delivery networks.

3.9 Avoiding Internet Investment Scams

The US Security Exchange Commission have enumerated guideline on how to avoid internet investment scams. The summary are as follows:

- The Internet allows individuals or companies to communicate with a large audience without spending a lot of time, effort, or money. Anyone can reach tens of thousands of people by building an Internet web site, posting a message on an online bulletin board, entering a discussion in a live “chat” room, or sending mass e-mails.
- If you want to invest wisely and steer clear of frauds, you must get the facts.
- The types of investment fraud seen online mirror the frauds perpetrated over the phone or through the mail. Consider all offers with skepticism.

4.0 CONCLUSION

Electronic systems are very vulnerable to fraud and abuse. This has informed the growth in types of e-frauds as well as individual case of e-frauds. The ease of access to information technology paraphernalia has not helped the matter either. In fact vulnerability to fraud remains the major hindrance to the full utilization of the internet in financial transactions. Several efforts, legislative, legal, moral, institutional and individual efforts are made to tackle e-frauds, some of which are fruitful.

5.0 SUMMARY

- The term “Internet fraud” generally refers to any type of fraud scheme that uses one or more online services - such as chat rooms, e-mail, message boards, or Web sites - to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme.

- The most straightforward type of purchase scam is a buyer in another country approaching many merchants through spamming them and directly asking them if they can ship to them using credit cards to pay.
- Money transfer fraud consists of an employment offer to help transfer money to a foreign company, supposedly because it costs too much to do it through other methods (which is usually not the case)
- The latest scam to hit the headlines is the multi-million dollar [click fraud](#) which occurs when advertising network affiliates force paid views or clicks to ads on their own websites via [spyware](#), the affiliate is then paid a commission on the [cost-per-click](#) that was artificially generated
- Customers of dial-up Internet Service Providers, such as AOL, use a modem to dial a local connection number. Some web sites, normally containing adult content, use international dialing to trick consumers into paying to view content on their web site.
- A variation of internet marketing fraud is offering tickets to sought-after events such as concerts, shows and sports events. The tickets turn out to be fake or are simply never delivered.
- Fraudsters launch auctions on eBay or TradeMe with very low prices and no reservations especially for high priced items like watches, computers or high value collectibles
- Click fraud is a type of [internet crime](#) that occurs in [pay per click online advertising](#) when a person, automated script, or computer program imitates a legitimate user of a [web browser](#) clicking on an ad, for the purpose of generating a [charge per click](#) without having actual interest in the target of the ad's link
- The US Security Exchange Commission have enumerated guideline on how to avoid internet investment scams

6.0 TUTOR-MARKED ASSIGNMENT

1. Briefly discuss money transfer fraud
2. Briefly discuss pay per click advertising fraud

7.0 REFERENCES/FURTHER READING

‘Counterfeit U.S. Postal Money Orders Counterfeit Postal Money Orders are reportedly in Circulation’,(FDIC) March 9, 2005.

A Common Currency for Online Fraud Forgers of U.S. Postal Money Orders Grow by Tom Zeller Jr (NYT) April 26, 2005

Jamie Doward: “How Boom in Rogue Ticket Websites Fleeces Britons”. The Observer, Sunday March 9, 2008.

“USOC and IOC File Lawsuit against Fraudulent Ticket Seller”.
“Sports City” website. Retrieved August 1, 2008.

“Ticket Swindle Leaves Trail of Losers”. By Jacquelin Magnay, Sydney Morning Herald”, August 4, 2008.

Kelly Burke. “British fraud ran Beijing ticket scam”. *The Sydney Morning Herald*, August 6, 2008.

“*The Lane’s Gifts v. Google Report, by Alexander Tuzhilin.*” [Alexander Tuzhilin](#). Retrieved [December 7, 2006](#).

Metwally, Ahmed; Agrawal, Divyakant; El Abbadi, Amr (2007).
“[DETECTIVES: Detecting Coalition hit Inflation attacks in Advertising networks Streams](#)”. *Proceedings of the International WWW conference*: 241-250, IW3C2.

Metwally, Ahmed; Agrawal, Divyakant; El Abbadi, Amr (2005).
“[Duplicate Detection in Click Streams](#)”. *Proceedings of the International WWW conference*: 12-21, IW3C2.

Majumdar, Saugat; Kulkarni, Dhananjay; Ravishankar, China (2007).
“[Addressing Click Fraud in Content Delivery Systems](#)”. *Infocom*, IEEE.

UNIT 2 INTERNET/ELECTRONIC CRIMES AND FRAUD 2

CONTENTS

- 1.0 Introduction
- 2.0 Objectives
- 3.0 Main Content
 - 3.1 Origins
 - 3.2 Stolen Cards
 - 3.3 Compromised Accounts
 - 3.4 Profits, Losses and Punishment
 - 3.5 Forex Scam
- 4.0 Conclusion
- 5.0 Summary
- 6.0 Tutor-Marked Assignment
- 7.0 References/Further Reading

1.0 INTRODUCTION

Credit card fraud is a wide-ranging term for theft and fraud committed using a credit card or any similar payment mechanism as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account. Credit card fraud is also an adjunct to identity theft.

The cost of credit card fraud reaches into billions of dollars annually. In 2006, fraud in the United Kingdom alone was estimated at £428 million, or US\$750-830 million at prevailing 2006 exchange rates.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

- explain what is, and the costs of credit card fraud
- trace the history and development of credit card fraud
- discuss the various forms of credit card frauds
- understand the technicalities of forex scam
- understand the kind of punishment meted on offenders.

3.0 MAIN CONTENT

3.1 Origins

The fraud begins with either the theft of the physical card or the compromise of data associated with the account, including the card

account number or other information that would routinely and necessarily be available to a merchant during a legitimate transaction. The compromise can occur by many common routes and can usually be conducted without tipping off the card holder, the merchant or the bank, at least until the account is ultimately used for fraud. A simple example is that of a store clerk copying sales receipts for later use. The rapid growth of credit card use on the Internet has made database security lapses particularly costly; in some cases, millions of accounts have been compromised.

Stolen cards can be reported quickly by card holders, but a compromised account can be hoarded by a thief for weeks or months before any fraudulent use, making it difficult to identify the source of the compromise. The card holder may not discover fraudulent use until receiving a billing statement, which may be delivered infrequently.

3.2 Stolen Cards

When a credit card is lost or stolen, it remains usable until the holder notifies the bank that the card is lost. Most banks have toll-free telephone numbers with 24-hour support to encourage prompt reporting. Still, it is possible for a thief to make unauthorized purchases on that card up until the card is cancelled. In the absence of other security measures, a thief could potentially purchase thousands of dollars in merchandise or services before the card holder or the bank realize that the card is in the wrong hands.

In the United States, federal law limits the liability of card holders to \$50 in the event of theft, regardless of the amount charged on the card. In practice, however, many banks will waive even this small payment and simply remove the fraudulent charges from the customer's account if the customer signs an affidavit confirming that the charges are indeed fraudulent. Other countries generally have similar laws aimed at protecting consumers from physical theft of the card.

The only common security measure on all cards is a signature panel, but signatures are relatively easy to forge. Many merchants will demand to see a picture ID, such as a driver's license, to verify the identity of the purchaser, and some credit cards include the holder's picture on the card itself. However, the card holder has a right to refuse to show additional verification, and asking for such verification may be a violation of the merchant's agreement with the credit card companies. Self-serve payment systems (gas stations, kiosks, etc.) are common targets for stolen cards, as there is no way to verify the card holder's identity. A common countermeasure is to require the user to key in some identifying information, such as the user's ZIP or postal code. This

method may deter casual theft of a card found alone, but if the card holder's wallet is stolen, it may be trivial for the thief to deduce the information by looking at other items in the wallet. For instance, a U.S. driver license commonly has the holder's home address and ZIP code printed on it.

Banks have a number of countermeasures at the network level, including sophisticated real-time analysis that can estimate the probability of fraud based on a number of factors. For example, a large transaction occurring a great distance from the card holder's home might be flagged as suspicious. The merchant may be instructed to call the bank for verification, to decline the transaction, or even to hold the card and refuse to return it to the customer.

3.3 Compromised Accounts

Card account information is stored in a number of formats. Account numbers are often embossed or imprinted on the card, and a magnetic stripe on the back contains the data in machine readable format. Fields can vary, but the most common include:

- Name of card holder
- Account number
- Expiration date
- Verification/[CVV code](#) - not ever embossed or stored on the magnetic strip.

There have been high profile examples of companies being compromised resulting in large scale identity theft, the largest to date being [TJX](#).

Mail/Internet order fraud

The mail and the Internet are major routes for fraud against merchants who sell and ship products, as well Internet merchants who provide online services. The industry term for catalog order and similar transactions is "Card Not Present" (CNP), meaning that the card is not physically available for the merchant to inspect. The merchant must rely on the holder (or someone purporting to be the holder) to present the information on the card by indirect means, whether by mail, telephone or over the Internet when the cardholder is not present at the point of sale.

It is difficult for a merchant to verify that the actual card holder is indeed authorizing the purchase. Shipping companies can guarantee delivery to a location, but they are not required to check identification and they are usually are not involved in processing payments for the

merchandise. A common preventive measure for merchants is to allow shipment only to an address approved by the cardholder, and merchant banking systems offer simple methods of verifying this information.

Additionally, smaller transactions generally undergo less scrutiny, and are less likely to be investigated by either the bank or the merchant. CNP merchants must take extra precaution against fraud exposure and associated losses, and they pay higher rates to merchant banks for the privilege of accepting cards. Anonymous scam artists bet on the fact that many fraud prevention features do not apply in this environment.

Merchant associations have developed some prevention measures, such as single use card numbers, but these have not met with much success. Customers expect to be able to use their credit card without any hassles, and have little incentive to pursue additional security due to laws limiting customer liability in the event of fraud. Merchants can implement these prevention measures but risk losing business if the customer chooses not to use the measures.

Account takeover

There are two types of fraud within the identity theft category, application fraud and account takeover.

Application fraud occurs when criminals use stolen or fake documents to open an account in someone else's name. Criminals may try to steal documents such as utility bills and bank statements to build up useful personal information. Alternatively, they may create counterfeit documents.

Account takeover involves a criminal trying to take over another person's account, first by gathering information about the intended victim, then contacting their bank or credit issuer — masquerading as the genuine cardholder — asking for mail to be redirected to a new address. The criminal then reports the card lost and asks for a replacement to be sent. The replacement card is then used fraudulently.

Some merchants added a new practice to protect consumers and self reputation, where they ask the buyer to send a copy of the physical card and statement to ensure the legitimate usage of a card.

Skimming

Skimming is the theft of credit card information used in an otherwise legitimate transaction. It is typically an "inside job" by a dishonest employee of a legitimate merchant. The thief can procure a victim's credit card number using basic methods such as photocopying receipts or more advanced methods such as using a small electronic device

(skimmer) to swipe and store hundreds of victim's credit card numbers. Common scenarios for skimming are restaurants or bars where the skimmer has possession of the victim's credit card out of their immediate view. The thief may also use a small keypad to unobtrusively transcribe the 3 or 4 digit Card Security Code which is not present on the magnetic strip.

Instances of skimming have been reported where the perpetrator has put a device over the card slot of a ATM (automated teller machine), which reads the magnetic strip as the user unknowingly passes their card through it. These devices are often used in conjunction with a pinhole camera to read the user's [PIN](#) at the same time.

Skimming is difficult for the typical card holder to detect, but given a large enough sample, it is fairly easy for the bank to detect. The bank collects a list of all the card holders who have complained about fraudulent transactions, and then uses [data mining](#) to discover relationships among the card holders and the merchants they use. For example, if many of the customers used one particular merchant, that merchant's terminals (devices used to authorize transactions) can be directly investigated. Sophisticated algorithms can also search for known patterns of fraud. Merchants must ensure the physical security of their terminals, and penalties for merchants can be severe in cases of compromise, ranging from large fines to complete exclusion from the merchant banking system, which can be a death blow to businesses such as restaurants which rely on credit card processing.

Carding

Carding is a term used for a process to verify the validity of stolen card data. The thief presents the card information on a website that has real-time transaction processing. If the card is processed successfully, the thief knows that the card is still good. The specific item purchased is immaterial, and the thief does not need to purchase an actual product; a Web site subscription or charitable donation would be sufficient. The purchase is usually for a small monetary amount, both to avoid using the card's credit limit, and also to avoid attracting the bank's attention. A website known to be susceptible to carding is known as a cardable website.

In the past, carders used computer programs called "generators" to produce a sequence of credit card numbers, and then test them to see which valid accounts were. Another variation would be to take false card numbers to a location that does not immediately process card numbers, such as a trade show or special event. However, this process is no longer viable due to widespread requirement by internet credit card processing systems for additional data such as the billing address, the 3

to 4 digit [Card Security Code](#) and/or the card's expiry date, as well as the more prevalent use of wireless card scanners that can process transactions right away. Nowadays, carding is more typically used to verify credit card data obtained directly from the victims by [skimming](#) or [phishing](#).

A set of credit card details that has been verified in this way is known in fraud circles as a [phish](#). A carder will typically sell data files of phish to other individuals who will carry out the actual fraud. Market price for a phish ranges from US\$1.00 to US\$50.00 depending on the type of card, freshness of the data and credit status of the victim.

3.4 Profits, Losses and Punishment

U.S. federal law can hold the cardholder victim responsible for up to \$50. Merchants in high-risk industries, such as unattended automated fuel pumps or Internet sales, anticipate a certain amount of credit card fraud, and set prices accordingly. These higher costs are then passed onto the customer. The FBI's Financial Report to the Public for 2007 report losses of \$52.6 billion, affecting 9.91 million Americans.

Credit card companies

In the case of fraud, the merchant and not the credit card company pays the full cost of the fraud plus a chargeback fee or the merchant.

3.5 Forex Scam

Introduction

A forex scam is any trading scheme used to defraud individual traders by convincing them that they can expect to gain a high profit by trading in the [foreign exchange market](#). Currency trading “has become the fraud du jour,” according to Michael Dunn of the U.S. [Commodity Futures Trading Commission](#). But “the market has long been plagued by swindlers preying on the gullible,” according to the [New York Times](#). “The average individual foreign-exchange-trading victim loses about \$15,000, according to CFTC records” as reported by [The Wall Street Journal](#). The [North American Securities Administrators Association](#) says that “off-exchange forex trading by retail investors is at best extremely risky, and at worst, outright fraud.”

“In a typical case, investors may be promised tens of thousands of dollars in profits in just a few weeks or months, with an initial investment of only \$5,000. Often, the investor’s money is never actually placed in the market through a legitimate dealer, but simply diverted – stolen – for the personal benefit of the con artists.”

The forex market is a [zero-sum game](#), meaning that whatever one trader gains, another loses, except that brokerage commissions and other [transaction costs](#) are subtracted from the results of all traders, technically making forex a “negative-sum” game.

These scams might include churning of customer accounts for the purpose of generating commissions, selling software that is supposed to guide the customer to large profits, improperly managed "managed accounts", false advertising, [Ponzi schemes](#) and outright fraud. It also refers to any [retail forex](#) broker who indicates that trading foreign exchange is a low risk, high profit investment.

The U.S. Commodity Futures Trading Commission (CFTC), which loosely regulates the foreign exchange market in the United States, has noted an increase in the amount of unscrupulous activity in the non-bank foreign exchange industry.

An official of the National Futures Association was quoted as saying, “Retail forex trading has increased dramatically over the past few years. Unfortunately, the amount of forex fraud has also increased dramatically...” between 2001 and 2006 the U.S.

Commodity Futures Trading Commission has prosecuted more than 80 cases involving the defrauding of more than 23,000 customers who lost \$350 million. From 2001 to 2007, about 26,000 people lost \$460 million in forex frauds. CNN quoted Godfried De Vidts, President of the Financial Markets Association, a European body, as saying, “Banks have a duty to protect their customers and they should make sure customers understand what they are doing. Now if people go online, on non-bank portals, how is this control being done?”

Not beating the market

The foreign exchange market is a zero sum game in which there are many experienced well-capitalized professional traders (e.g. working for banks) who can devote their attention full time to trading. An inexperienced retail trader will have a significant information disadvantage compared to these traders.

Although it is possible for a few experts to successfully arbitrage the market for an unusually large return, this does not mean that a larger number could earn the same returns even given the same tools, techniques and data sources. This is because the arbitrages are essentially drawn from a pool of finite size; although information about how to capture arbitrages is a nonrival good, the arbitrages themselves are a rival good. (To draw an analogy, the total amount of buried

treasure on an island is the same, regardless of how many treasure hunters have bought copies of a treasure map.)

Retail traders are - almost by definition - undercapitalized. Thus they are subject to the problem of gambler's ruin. In a fair game (one with no information advantages) between two players that continues until one trader goes bankrupt, the player with the lower amount of capital has a higher probability of going bankrupt first. Since the retail speculator is effectively playing against the market as a whole - which has nearly infinite capital - he will almost certainly go bankrupt.

The retail trader always pays the bid/ask spread which makes his odds of winning less than those of a fair game. Additional costs may include margin interest, or if a spot position is kept open for more than one day the trade may be "resettled" each day, each time costing the full bid/ask spread.

According to the Wall Street Journal (Currency Markets Draw Speculation, Fraud July 26, 2005) "Even people running the trading shops warn clients against trying to time the market. 'If 15% of day traders are profitable,' says Drew Niv, chief executive of FXCM, 'I'd be surprised.'"

Paul Belogour, the Managing Director of a Boston based retail forex trader, was quoted by the Financial Times as saying, "Trading foreign exchange is an excellent way for investors to find out how tough the markets really are. But I say to customers: if this is money you have worked hard for - that you cannot afford to lose - never, never invest in foreign exchange."

The use of high leverage

By offering high leverage, the market maker encourages traders to trade extremely large positions. This increases the trading volume cleared by the market maker and increases his profits, but increases the risk that the trader will receive a margin call. While professional currency dealers (banks, hedge funds) never use more than 10:1 leverage, retail clients are generally offered leverage between 50:1 and 200:1.

A self-regulating body for the foreign exchange market, the National Futures Association, warns traders in a forex training presentation of the risk in trading currency. "As stated at the beginning of this program, off-exchange foreign currency trading carries a high level of risk and may not be suitable for all customers. The only funds that should ever be used to speculate in foreign currency trading, or any type of highly speculative investment, are funds that represent risk capital; in other

words, funds you can afford to lose without affecting your financial situation.“

4.0 CONCLUSION

Electronic systems are very vulnerable to fraud and abuse. This has informed the growth in types of e-frauds as well as individual case of e-frauds. The ease of access to information technology paraphernalias has not helped the matter either. In fact vulnerability to fraud remains the major hindrance to the full utilization of the internet in financial transactions. Several efforts, legislative, legal, moral, institutional and individual efforts are made to tackle e-frauds, some of which are fruitful.

5.0 SUMMARY

- Credit card fraud is a wide-ranging term for theft and fraud committed using a credit card or any similar payment mechanism as a fraudulent source of funds in a transaction.
- The fraud begins with either the theft of the physical card or the compromise of data associated with the account, including the card account number or other information that would routinely and necessarily be available to a merchant during a legitimate transaction
- When a credit card is lost or stolen, it remains usable until the holder notifies the bank that the card is lost. Most banks have toll-free telephone numbers with 24-hour support to encourage prompt reporting.
- There have been high profile examples of companies being compromised resulting in large scale identity theft, the largest to date being [TJX](#).
- Skimming is the theft of credit card information used in an otherwise legitimate transaction. It is typically an "inside job" by a dishonest employee of a legitimate merchant
- U.S. federal law can hold the cardholder victim responsible for up to \$50. Merchants in high-risk industries, such as unattended automated fuel pumps or Internet sales, anticipate a certain amount of credit card fraud, and set prices accordingly
- A **forex scam** is any trading scheme used to defraud individual traders by convincing them that they can expect to gain a high profit by trading in the [foreign exchange market](#).

6.0 TUTOR-MARKED ASSIGNMENT

1. Briefly discuss skimming as electronic fraud scheme

7.0 REFERENCES/FURTHER READING

Karmin, Craig “[How a Money Trader went Bad; Bets on Currency Prices Become 'Fraud du Jour' Amid Regulatory Holes](#)”, *The Wall Street Journal*, Dow Jones and Company, January 12, 2008, PB1.

Egan, Jack “[Check the Currency Risk. Then Multiply by 100](#)”, *The New York Times*. June 19, 2005.

McKay, Peter A. “[Scammers Operating on Periphery Of CFTC's Domain Lure Little Guy With Fantastic Promises of Profits](#)”, *The Wall Street Journal*, Dow Jones and Company. July 26, 2005.

[Forex Fraud Investor Alert](#) North American Securities Administrators Association, Accessed January 12, 2008

[Regulators Join Forces to Warn Public of Foreign Currency Trading Frauds](#)”. U.S. Commodity Futures Trading Commission (2007-05-07).

“[CFTC Establishes Task Force on Currency Fraud](#)” (2007-08-11).

Douch, Nick (1989). *The Economics of Foreign Exchange*. Greenwood Press, pp. 87-90. ISBN13 9780899304991.

[SOFTWARE VENDOR CHARGED](#) CFTC News Release 4789-03, May 21, 2003

[CFTC complaint](#) Forex Advisory Firm and Trade Risk Management Firm Charged With Fraud

[Fraud Charges Against Multiple Forex Firms](#) Commodity Futures Trading Commission (CFTC) Release: 4946-0

[Foreign Currency Fraud Action](#) Commodity Futures Trading Commission (CFTC) vs. Donald O’Neill

[FOREX Advisory](#) Commodity Futures Trading Commission's FOREIGN CURRENCY TRADING FRAUDS

[Forex Information](#) Commodity Futures Trading Commission (CFTC) Forex Information for investors

[National Futures Association \(NFA\)](#) NFA launches learning program

Karmin, Craig “[Currency Markets Draw Speculation, Fraud](#)”, *The Wall Street Journal*, Dow Jones and Company. July 26, 2005.

Garnham, Peter "FX gamblers geared to win (or lose)". *The Financial Times Ltd.* May 17, 2006.

UNIT 3 RISK OF E-FINANCE: MONEY LAUNDERING

CONTENTS

- 1.0 Introduction
- 2.0 Objectives
- 3.0 Main Content
 - 3.1 Stored Value Cards (SVC)
 - 3.2 Money Laundering Concerns
 - 3.3 Events that may raise Suspicious
 - 3.4 Other Events that may raise Suspicious
- 4.0 Conclusion
- 5.0 Summary
- 6.0 Tutor-Marked Assignment
- 7.0 References/Further Reading

1.0 INTRODUCTION

In the past decade, there has been an increasing reliance on electronic means of transferring funds for personal and business purposes. One recent development has been the emergence of plastic cards with the capacity to store value electronically, which can be used for a range of retail transactions. With the advent of comprehensive anti-money laundering laws throughout the developed world, criminals are turning to alternative ways of moving funds across borders to circumvent reporting and detection systems. One identified risk is the misuse of prepaid stored value cards to keep the proceeds of crime and move them across borders without alerting law enforcement and financial intelligence units. This unit describes the nature of these risks and considers whether existing regulatory measures are adequate to address them.

The use of electronic transactions has increased considerably in recent years. For example, in Australia, the volume and value of cheque transactions in paper-based clearing systems fell from an average of 2.7 million per day in 2001 to 2.1 million in 2005, and from an average of \$8.3b per day in 2001 to \$6.3b in 2005 (APCA 2005). A correspondingly large increase in electronic banking has also been observed. This is hardly surprising, as the financial incentive to do business electronically in today's highly competitive market is significant, with the cost of an online transaction often being a fraction of a non-electronic transaction (De Young 2001). Similarly, online retail spending has increased considerably with total sales in the United States in 2007 exceeding US\$100b (Ames 2007). One of the more popular electronic payment systems is prepaid stored value cards (SVCs), such as gift cards issued by retail stores.

The overall market for gift cards is projected to grow to nearly \$88 billion in 2008, with the fastest growth occurring in corporate purchases of gift cards for employees and customers, and in “open” gift cards - like the American Express Gift Card that can be redeemed at multiple merchants.... Corporate purchases will rise 72% from 2005 to 2008, growing from [US]\$9 billion to [US]\$15.5 billion. Open gift card sales are expected to almost quadruple from 2005 to 2008, growing from [US] \$1.3 billion to [US]\$5 billion, according to Mercator (American Express 2006).

This extensive use of SVCs, coupled with the convergence of financial services and electronic payment technologies, has created new opportunities for money laundering. This paper examines the nature of the risks and how they can best be addressed.

2.0 OBJECTIVES

At the end of this unit, you should be able to:

- discuss the growths pattern in the use of electronic payment systems
- discuss the players in the plastic stored value card
- discuss and differentiate the types of stored value cards
- discuss the concerns of money laundering in e-financial transactions
- explain how to identify the events that may raise suspicions of money laundering.

3.0 MAIN CONTENT

3.1 Stored Value Cards (SVC)

Stored value cards are cards with data encoded in either a magnetic strip or a computer chip that are preloaded with a fixed amount of electronic currency or value. This can be redeemed or transferred to individuals and/or merchants in a manner that is similar to spending physical currency.

The players in a typical SVC program include:

- program managers - owners of prepaid SVC programs who establish relationships with payment processing facilities (e.g. banks and payment networks) and distributors, and establish pooled account(s) at banks
- payment processing facilities - are responsible for payment transactions for prepaid SVC programs, and they track and distribute funds in pooled accounts. Program managers may also choose to function as their own payment processors

- banks - may also function as program managers and/or distributors, and are responsible for maintaining pooled accounts, settling payments and issuing branded prepaid SVCs (open-system cards)
- the payments network - the 'link' between payment processing facilities, and the retailer and automated teller machine (ATM), for authorisation of payment transactions
- a distributor (e.g. banks and non-financial institutions) - responsible for selling prepaid SVCs.

The market for SVCs has increased considerably over the years, particularly in terms of its availability and size. A recent study by Mercator Advisory Group estimated that '[US]\$171.18 Billion was loaded on Closed Loop Prepaid Solutions in 2006, an increase of 13.9% over the 2005 spend of [US]\$160.29 [billion]' (Sloane 2007). Another study on prepaid general-purpose spending cards (open system cards) predicted that more than 300 million individuals in Latin America (Argentina, Brazil, Chile, Colombia, Ecuador, Mexico, Peru, Venezuela, Central America and Dominican Republic) could have prepaid cards that do not require bank accounts by 2015. The spending power is estimated to be more than US\$214b (NovoPayment 2008).

This is, perhaps, not surprising, considering the many benefits associated with SVCs:

- easy to get and use (cardholder/ buyer anonymity) - credit checks are not required when purchasing SVCs and for some cards, evidence of identification is also not needed
- convenient - SVCs can be purchased, reloaded (for open and semi-open card systems), and redeemed and refunded at conveniently located participating merchant locations (e.g. supermarkets and convenience stores). The UK-based pay-as-you-go MasterCard? card, for example, allows cardholders to obtain their balance, top up their card or lock/unlock their card for added security, from anywhere, 24 hours a day, by sending text messages from a registered mobile phone (Payments News 2008)
- affordable - funds are immediately available, often at a lower cost than when using traditional banking services
- reduced overdraft risk - reduces the risk of overdrafts while providing nearly immediate liquidity for consumers.

The Payments Dynamics SM 2007 study also found that ease of use, universal acceptance, the ability to use one's own money, safety and security, and the ability to have control over one's finances are the key drivers for the growth of prepaid cards in the unbanked population (Abal 2007).

SVCs can be categorised broadly into open systems (or open-loop systems), semi-open systems, closed systems (or closed-loop systems) and semi-closed systems (Table 1).

Table 1: Categories of stored value cards

Description	Anonymous?	Reloadable?	Examples
a: http://www.cashpassportcard.com/			
b: http://www.nets.com.sg/consumers/netscashcard/index.php			
c: http://www.davidjones.com.au/gift_card.jsp			
d: https://www.flybuys.com.au			
Typically branded (e.g. by American Express) and connected to global debit and ATM networks, which allow the cards to be used for multiple purposes and at multiple points of sale with different participating merchants	Typically no (similar in appearance to traditional debit cards, which are embossed with the cardholder's name and the expiry date)	Typically yes (e.g. via regular deposit arrangement, internet and at participating merchant outlets)	Visa cash passport card ^a , a Visa-branded SVC, which allows cardholders to withdraw cash from Visa ATMs worldwide and use the cards at places where Visa debit cards are accepted
Generally have the same features as open system cards, but cannot be used to access cash at ATMs (also known as purchasing-only cards)	Typically no (similar in appearance to traditional debit cards, which are embossed with the cardholder's name and the expiry date)	Typically yes	NETS CashCard ^b
Limited to only buying goods or services from the merchant	Typically yes	Typically no, and sold at preset denominations, but some retail	David Jones Gift Card ^c

Table 1: Categories of stored value cards

Description	Anonymous?	Reloadable?	Examples
issuing the card		gift cards are reloadable	
Can be used at a selected group of merchants or service providers	Typically yes	Typically no, and sold at preset denominations	FlyBuys gift cards ^d , which can only be used at participating merchants

Open system cards typically allow high values to be loaded and kept on cards. Open system cards that are designed to facilitate cross-border remittance payments are also offered by offshore banks. Such systems often allow multiple cards to be issued per account, so that friends and family in receiving countries can use the cards to access cash and make purchases, without additional information being provided or existing information confirmed.

The Travelex Cash Passport card in Australia, for example, has a maximum card balance value (at any one time) of A\$10,000; a maximum amount that can be loaded onto the card during any 12-month period of A\$45,000; a 24-hour ATM withdrawal limit of A\$6,000; and up to two cards able to be issued per Cash Passport fund.

Closed and semi-closed systems, conversely, are typically used for micropayments in view of their limited storage capacity. Such cards can be purchased without the need for any evidence of identification or prior account history.

In the same way that legitimate businesses will look at market forces and new opportunities for SVCs, criminals will also explore new areas that can be exploited to maximise their profits, and to evade the scrutiny of law enforcement agencies and regulators.

The widespread availability of SVCs (particularly at non-financial outlets), the high loading and card balance value limits of open system cards, and the anonymity offered by closed and semi-closed system cards could be abused by organised criminals for illicit financial transactions, money laundering and bulk cash smuggling, particularly as value limits increase. Stored value cards have been identified in several reports as a potential tool for organised crime groups to launder their illicit crime proceeds (APG 2005; US NDIC 2006). A study on cross-border electronic funds transfer systems raises similar concerns:

In virtually every investigation of these groups, the movement of the proceeds of the criminal acts from the U.S. back to Canada, whether by movement of bulk cash, funds transfers, or stored value cards, has been significant (FinCEN 2007a: 100).

3.2 Money Laundering Concerns

Although the actual amount of money being laundered will never be known with accuracy, money laundering transactions in Australia are estimated to involve between \$2b (Institute of Chartered Accountants 2006) and \$4.5b per year (Walker et al. 2007). The International Monetary Fund has further suggested that money laundering transactions are approximately two to five percent of the global gross domestic product. Money laundering could, potentially, lead to a shift of economic power to organised crime groups, thus eroding political and social systems.

To disguise the origins of illicit proceeds, criminals can perform a series of business transactions such as transferring electronic currency through a series of offshore companies and purchasing goods for resale, prior to integrating the 'cleaned' proceeds into the legitimate financial system. The money laundering process is typically segmented into three stages:

- placement - in which illegal funds or assets are introduced into the financial system, or converted into monetary instruments (e.g. SVCs)
- layering - in which the illegal origins of placed funds are disguised
- integration - in which disguised funds are made available for investment in legitimate or illegitimate businesses.

Placement

In general, it is relatively easy to purchase SVCs, because customers do not generally require a bank account to acquire them. Applications for stored value cards can usually be accepted online, via fax or through non-financial outlets (e.g. local cheque-cashing outlets and convenience stores), which may not require any face-to-face verification of cardholder identity. Small to medium-sized non-financial distributors are also unlikely to have an adequate, or any, risk-based program based on the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act) in place, and may not carry out customer due diligence and have trained staff in the areas of money laundering detection.

In cases where face-to-face verification of cardholder identity is required, evidence of identity may be difficult to verify, particularly at non-financial distribution outlets (e.g. verification of a foreign passport at a convenience store). A criminal can, therefore, easily purchase large

quantities of stored value cards (perhaps with different issuers) using cash generated from criminal proceeds, and it may then be possible to take these overseas without detection. Even if cards are located at entry ports, customs officials may be unable to ascertain how much value is loaded on each card.

Events that may raise suspicions

- An excessively obstructive or secretive client.
- Customer asks questions or makes comments that raise suspicions (e.g. questions such as 'Will these purchases be reported to the authorities?').
- Large payments made in actual cash (especially if the cash is wrapped in currency straps).
- Customer purchases a large quantity of stored value cards, particularly reloadable open system or semi-open system cards, in an apparent effort to avoid triggering identification or reporting requirements - an activity also known as structuring.
- Customer purchases a large quantity of stored value cards of large denomination that is not commensurate with normal business activities.
- For open system card purchases at banks, customer makes a large number of stored value card transactions using the banks' services or third-party online payment systems, which appear inconsistent with the stated business activities.

Individuals can also be recruited by organised crime groups to purchase SVCs using stolen credit cards. These individuals ('card mules') may be recruited through email messages, websites or newspaper advertisements that purport to be legitimate businesses seeking new staff. One US case involved the arrest of a six-member syndicate in March 2007. Arrests were made by the Gainesville Police Department for allegedly using stolen credit cards to purchase large quantities of Wal-Mart and Sam's Club gift cards (US FDLE 2007).

Layering

Depending on the types of cards purchased during the placement stage, value can either be redeemed for merchandise or sent overseas.

Closed or semi-closed cards - These can be redeemed for merchandise. For example, in the arrests made by the Gainesville Police Department, the purchased cards were redeemed for merchandise such as computers, gaming devices and large-screen televisions (US FDLE 2007). The redeemed merchandise can either be sent overseas or resold and the proceeds remitted to third-party accounts (minus a commission).

Another recent US example involved the arrest of four Russians who, it was noted:

- then transferred] the fraudulently-obtained money and goods back to Russia. ... Using stolen identity and credit information, defendant CHUGAEV made on-line purchases of PayPal cards, gift cards, computers, and other merchandise, and requested that the items be shipped to United States addresses under the control of his associates. Those associates quickly withdrew cash from the credit cards, then deposited the cash into bank accounts, and allowed CHUGAEV to withdraw the stolen money in Russia using ATM cards associated with the bank accounts. The computers and other merchandise were repackaged ... in the United States and mailed on to Russia, where the stolen goods were resold (US DoJ 2007).

SVCs can also be 'purchased for currency and transferred from one person to another and resold [because beneficiaries' names are not required]. Often, a firm independent of a bank processes all card transactions through a "pooled" bank account held in the name of the firm managing the card program' (US FFIEC 2007: 206). The use of pooled accounts also increases the difficulty in monitoring any specific cardholder's activity.

Open or semi-open cards - Due to the worldwide acceptance of these cards (as most of the open system cards have access to the Plus and Cirrus/Maestro networks), card mules can be instructed to mail the purchased stored value cards to countries with lax anti-money laundering legislation where funds can then be withdrawn from local ATMs (including 'white label' ATMs - machines that offer only cash dispensing services). FINTRAC (2007: 24) pointed out that white label ATMs 'can be "self-loaded" with illicit funds, increasing the potential for money laundering. The involvement of organized crime was a key characteristic of disclosure cases involving white label ATMs this year'. SVCs can also be easily taken through border controls because of their size - they are often in wallets, which may not be subject to scrutiny.

In another US case, the alleged mastermind of an international theft ring deposited money into several SVCs and sent six of the cards to Russia where his co-conspirators retrieved the money from ATMs (FinCEN 2007b: 25).

3.3 Events That May Raise Suspicious

- Customer makes payments using multiple payment methods or a large number of stored value cards.
- Customer purchasing pattern does not make economic sense (e.g. an individual customer pays for numerous laptops using several cards).
- The merchandise, particularly high-value and low-volume goods such as consumer electronics being shipped, appears inconsistent with the exporter's stated business activities or the merchandise is shipped to a jurisdiction designated as 'high risk' for money laundering activities.
- Stored value cards, particularly open or semi-open system cards (particularly with a large denomination), being sent through the post or found on travellers that appear inconsistent with the stated business activities (similar to bulk cash smuggling).

Integration

SVCs, particularly those used in open systems, can also be used as a means of payment by criminals. For example, precursor chemicals used in the production of illegal drugs, real estate investment, or life insurance policies could be paid for with SVCs.

SVCs can also be used as a means of payment for services rendered. In one case, a former employee of the Ohio Bureau of Motor Vehicles was prosecuted in connection with selling fraudulent Ohio drivers' licences in 2005. It was reported that she was paid using US\$10 phone cards (US ICE 2005).

Legislative framework

For example, the AML/CTF Act was enacted to enhance Australia's capacity to detect, prevent and combat money laundering, and to bring Australia in line with international best practice in detecting and deterring money laundering.

Designated services

The AML/CTF Act presently covers industry sectors with obligations under existing legislation, including the banking and finance sector, and other persons or businesses providing designated services. Industry sectors are considered 'reporting entities' under the AML/CTF Act when they provide 'designated services' defined in Section 6 of the AML/CTF Act. Although SVCs were not regulated under the *Financial*

Transaction Reports Act 1988 (Cth), issuing and reloading SVCs are now listed as designated services under the AML/CTF Act.

Entities providing designated services are subject to the full range of AML/CTF regulatory controls such as statutory reporting of suspicious activity, recordkeeping, and developing and implementing a risk-based AML/CTF program. As the main regulatory obligations under the AML/CTF Act are civil penalty provisions, non-compliance may attract a civil penalty (a fine up to A\$2.2 million and A\$11 million for individuals and corporations).

3.4 Other Events That May Raise Suspicions

- Living standards of employees (or public officials) exceed their known lawful income or if they control or possess pecuniary resources or property, that are disproportionate to their present or past known sources of income, and when they are unable or unwilling to account for the discrepancy.
- Transactions incompatible with the customer's normal activity or are beyond the customer's apparent financial means are causes for concern (e.g. a lump sum payment for real estate or life insurance in cash).

Section 81 of the AML/CTF Act requires all reporting entities to have an anti-money laundering and counter-terrorism financing (AML/CTF) program in place by 12 December 2007. The AML/CTF program includes general provisions concerning risk management and specific requirements concerning customer identification.

Banks and major financial institutions recognise the importance of sound ongoing customer due diligence policies and procedures (e.g. Know Your Customer) to reduce their *reputational risk* (e.g. maintain their brand and reputation in a competitive world market sensitive to the threats of international organised crime), *legal risk* and *financial risk*; and have monitoring systems in place to prevent exploitation of SVCs (e.g. monitoring of reloading above a threshold value).

In terms of customer identification at point of purchase or where value is reloaded onto SVCs, major banks and financial institutions employ technologies to detect forged identification documents and carry out enhanced customer due diligence for cardholders who reload SVCs frequently, have cash access and/or use their cards outside Australia.

In relation to monitoring SVC usage and detecting suspicious patterns or high-risk situations, real-time transaction monitoring using monitoring

technologies is used. These technologies can be broadly categorised into:

- rules-based systems - assess individual transactions against a set of predefined rules based on value thresholds and other criteria
- pattern recognition systems - use sophisticated techniques such as neural networks, link analysis, peer group analysis, time sequence matching and name recognition technologies to monitor for a library of known patterns and scenarios
- hybrid systems - allow a combination of rules writing by monitoring against a library of known patterns.

4.0 CONCLUSION

To reduce the money laundering risk, SVC providers need to be aware of and comply with local regulatory requirements such as AML/CTF regulation, and prudential and financial regulations. Compliance with these measures can, however, be challenging and expensive for SVC providers, although the potential legal liability and reputational risk for non-compliance can be significantly costly.

Tsingou (2005: 15) pointed out that '[t]he burden of compliance is more significant for smaller, local institutions, where “know your customer” and reporting requirements are less automated'. Prohibitive AML compliance costs, unlikely to be affordable by small to medium-sized non-financial distributors, might have the unintended consequence of driving the small players underground or driving providers (and users) of SVCs to less restrictive and less costly jurisdictions (regulatory arbitrage).

The process of disintermediation currently experienced in SVC programs (whereby physical contact between organisations and their clients is replaced by virtual contact) also compounds the challenge of customer identity verification at distribution outlets, particularly small to medium-sized non-financial distributors. Individuals in the unbanked sector may be unable to meet AML regulatory demands in terms of providing identification documentation such as passports or driving licences.

5.0 SUMMARY

- In the past decade, there has been an increasing reliance on electronic means of transferring funds for personal and business purposes. One recent development has been the emergence of plastic cards with the capacity to store value electronically, which can be used for a range of retail transactions.

- Stored value cards are cards with data encoded in either a magnetic strip or a computer chip that are preloaded with a fixed amount of electronic currency or value. This can be redeemed or transferred to individuals and/or merchants in a manner that is similar to spending physical currency.
- To disguise the origins of illicit proceeds, criminals can perform a series of business transactions such as transferring electronic currency through a series of offshore companies and purchasing goods for resale, prior to integrating the 'cleaned' proceeds into the legitimate financial system
- The market for SVCs has increased considerably over the years, particularly in terms of its availability and size.
- Open system cards typically allow high values to be loaded and kept on cards.
- Although the actual amount of money being laundered will never be known with accuracy, money laundering transactions in Australia are estimated to involve between \$2b (Institute of Chartered Accountants 2006) and \$4.5b per year (Walker et al. 2007).
- Customer purchasing pattern does not make economic sense (e.g. an individual customer pays for numerous laptops using several cards). This raises suspicion of money laundering
- Transactions incompatible with the customer's normal activity or are beyond the customer's apparent financial means are causes for concern (e.g. a lump sum payment for real estate or life insurance in cash).

6.0 TUTOR-MARKED ASSIGNMENT

1. Discuss briefly the major players of SVC program
2. Mention 5 events that may raise suspicion of money laundering during the placement of money in an account

7.0 REFERENCES/FURTHER READING

All URLs were correct at 20 June 2008

Abal, R. (2007). "Rich Opportunity in the Unbanked Segment". *Insight* 25: 1-6

American Express (2006). "American Express Enhances Corporate Gifting Services to Tap Fastest-Growing Segment of Burgeoning Gift Card Market". *Media release* 24 October

Ames B (2007). *Online Spending Tops US\$100 Billion*. Computerworld.com.au 5 January

- Asia-Pacific Group on Money Laundering (2005). *APG Yearly Typologies Report 2004-05*. n.p.: APG.
- Australian Payments Clearing Association (APCA). *Annual Report 2005*.
- De Young, R (2001). "The Internet's Place in the Banking Industry". *Chicago Fed letter* no. 163.
- Financial Crimes Enforcement Network (FinCEN) (2007)a. *Feasibility of a Cross-Border Electronic Funds Transfer Reporting System Under the Bank Secrecy Act*.
- Financial Crimes Enforcement Network (FinCEN) (2007). *The SAR Activity Review: Trends, Tips & Issues*. 12 (October)
- Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) 2007. *FINTRAC Annual Report*. Ottawa: FINTRAC.
- Institute of Chartered Accountants. Money Laundering Worth up to 5% of Global GDP. *Media Release* 26 May, 2006.
- Linn CJ (2008). Regulating the Cross-Border Movement of Prepaid cards. *Journal of Money Laundering Control* 11(2): 146-171
- Kim-Kwang Raymond Choo , "Trends and Issues in Crime and Criminal Justice". No. 363, ISBN 978 1 921185 92 2; ISSN 0817-8542, Canberra: Australian Institute of Criminology, September 2008
- NovoPayment. "NovoPayment Forecasts General Purpose Spending Cards for Latin America's unbanked". *Media Release* 10 June.
- Payments News, "FSTC Launches Mobile Technology Initiative". *Media Release* 3 June, (2008).
- Sloane, T. (2007). *4th Annual Prepaid Closed Loop Market Assessment*. Boston, MA: Mercator Advisory Group
- Tsingou, E. (2005). *Global Governance and Transnational Financial Crime: Opportunities and Tensions in the Global Anti-Money Laundering Regime*. Coventry, UK: Centre for the Study of Globalisation and Regionalisation.
- United States Department of Justice (US DoJ) "Four Russians Indicted in Identity Theft and Fraud Ring". *Media release* 1 March, 2007.

United States Federal Financial Institutions Examination Council (US FFIEC) (2007). *Bank Secrecy Act/Anti-Money Laundering Examination Manual*. n.p.: US FFIEC.

United States Florida Department of Law Enforcement (US FDLE) Arrests Made in Gift Card Fraud Case Totalling More Than \$8 Million in Losses. *News release* 19 March, 2007.

United States Immigration and Customs Enforcement (US ICE) (2005). Prepaid Cards an Emerging Threat. *The Cornerstone Report* 3(2): 4

United States National Drug Intelligence Center (US NDIC). *Prepaid Stored Value Cards: a Potential Alternative to Traditional Money Laundering Methods*. 31 October, 2006

Walker J et al. (2007). *The Extent of Money Laundering in and through Australia in 2004*. Canberra: Criminology Research Council.

UNIT 4 WWW SECURITY MANAGEMENT

CONTENTS

- 1.0 Introduction
- 2.0 Objectives
- 3.0 Main Content
 - 3.1 Internet/WWW Security Objectives
 - 3.2 Internet and WWW Security Policies and Procedures
 - 3.3 Appropriate Use Policy
 - 3.4 Internet/External Applications
 - 3.5 Web Browser Security Strategies
 - 3.6 Audit Tools and Capabilities
 - 3.7 WWW Security Flaws
- 4.0 Conclusion
- 5.0 Summary
- 6.0 Tutor-Marked Assignment
- 7.0 References/Further Reading

1.0 INTRODUCTION

Companies continue to flock to the Internet in ever-increasing numbers, despite the fact that the overall and underlying environment is not secure. To further complicate the matter, vendors, standards bodies, security organizations, and practitioners cannot agree on a standard, compliant, and technically available approach. As a group of investors concerned with the success of the Internet for business purposes, it is critical that we pull our collective resources and work together to quickly establish and support interoperable security standards; open security interfaces to existing security products and security control mechanisms within other program products; and hardware and software solutions within heterogeneous operating systems which will facilitate smooth transitions.

Having the tools and solutions available within the marketplace is a beginning, but we also need strategies and migration paths to accommodate and integrate Internet, intranet, and World Wide Web (WWW) technologies into our existing IT infrastructure. While there are always emerging challenges, introduction of newer technologies, and customers with challenging and perplexing problems to solve, this approach should enable us to maximize the effectiveness of our existing security investments, while bridging the gap to the long awaited and always sought after perfect solution!

This unit establishes and supports the need for an underlying baseline security framework that will enable companies to successfully evolve to

doing financial and banking business over the Internet and using internal intranet- and World Wide Web-based technologies most effectively within their own corporate computing and networking infrastructures. It presents a solution set that exploits existing skills, resources, and security implementations.

Security requirements, goals, and objectives remain the same, while the application of security, control mechanisms, and solution sets are different and require the involvement and cooperation of multidisciplined technical and functional area teams. As in any distributed environment, there are more players, and it is more difficult to find or interpret the overall requirements or even talk to anyone who sees or understands the big picture. More people are involved than ever before, emphasizing the need to communicate both strategic and tactical security plans broadly and effectively throughout the entire enterprise. The security challenges and the resultant problems become larger and more complex in this environment. Management must be kept up-to-date and thoroughly understand overall risk to the corporation's information assets with the implementation or decisions to implement new technologies. They must also understand, fund, and support the influx of resources required to manage the security environment.

As with any new and emerging technology, security should be addressed early in terms of understanding the requirements, participating in the evaluation of products and related technologies, and finally in the engineering, design, and implementation of new applications and systems. Security should also be considered during all phases of the systems development life cycle. This is nothing new, and many of us have learned this lesson painfully over the years as we have tried to retrofit security solutions as an adjunct to the implementation of some large and complex system. Another important point to consider throughout the integration of new technologies is "technology does not drive or dictate security policies, but the existing and established security policies drive the application of new technologies." This point must be made to management, customers, and supporting IT personnel.

For most of us, the WWW will be one of the most universal and influential trends impacting our internal enterprise and its computing and networking support structure. It will widely influence our decisions to extend our internal business processes out to the Internet and beyond. It will enable us to use the same user interface, the same critical systems and applications, work towards one single original source of data, and continue to address the age-old problem: how can I reach the largest number of users at the lowest cost possible?"

2.0 OBJECTIVES

At the end of this unit, you should be able to:

- understand what is network security and management
- explain what constitutes the objectives of a network security
- discuss the policies put in place for a network security project
- identify the basic threat to encounter in a network project
- identify Web browser security strategies
- identify the considerations in a www audit
- identify and understand the common disadvantages of a www network.

3.0 MAIN CONTENT

3.1 Internet/WWW Security Objectives

As mentioned earlier, security requirements do not change with the introduction and use of these technologies, but the emphasis on where security is placed and how it is implemented does change. The company's Internet, intranet, and WWW security strategies should address the following objectives, in combination or in prioritized sequence, depending on security and access requirements, company philosophy, the relative sensitivity of the company's information resources, and the business imperative for using these technologies.

- Ensure that Internet- and WWW-based application and the resultant access to information resources are protected, and that there is a cost-effective and user-friendly way to maintain and manage the underlying security components over time as new technology evolves and security solutions mature in response.
- Information assets should be protected against unauthorized usage and destruction. Communication paths should be encrypted as well as transmitted information that is broadcast over public networks.
- Receipt of information from external sources should be decrypted and authenticated. Internet- and WWW-based applications, WWW pages, directories, discussion groups, and data bases should all be secured using access control mechanisms.
- Security administration and overall support should accommodate a combination of centralized and decentralized management.
- User privileges should be linked to resources, with privileges to those resources managed and distributed through directory services.
- Mail and real-time communications should also be consistently protected. Encryption key management systems should be easy to administer, compliant with existing security architectures,

compatible with existing security strategies and tactical plans, and secure to manage and administer.

- New security policies, security architectures, and control mechanisms should evolve to accommodate this new technology; not change in principle or design.

Continue to use risk management methodologies as a baseline for deciding how many of the new Internet, intranet, and WWW technologies to use and how to integrate them into the existing Information Security Distributed Architecture. As always, ensure that the optimum balance between access to information and protection of information is achieved during all phases of the development, integration, implementation, and operational support life cycle.

3.2 Internet and WWW Security Policies and Procedures

Having said all of this, it is clear that we need new and different policies, or minimally, an enhancement or refreshing of current policies supporting more traditional means of sharing, accessing, storing, and transmitting information. In general, high-level security philosophies, policies, and procedures should not change. In other words, who is responsible for what (the fundamental purpose of most high-level security policies) does not change. These policies are fundamentally directed at corporate management, process, application and system owners, functional area management, and those tasked with the implementation and support of the overall IT environment. There should be minimal changes to these policies, perhaps only adding the Internet and WWW terminology.

Other high-level corporate policies must also be modified, such as the use of corporate assets, responsibility for sharing and protecting corporate information, etc. The second-level corporate policies, usually more procedure oriented typically addressing more of the “how,” should be more closely scrutinized and may change the most when addressing the use of the Internet, intranet, and Web technologies for corporate business purposes. New classifications and categories of information may need to be established and new labeling mechanisms denoting a category of information that cannot be displayed on the Internet or new meanings to “all allow” or “public” data. The term “public,” for instance, when used internally, usually means anyone authorized to use internal systems. In most companies, access to internal networks, computing systems and information is severely restricted and “public” would not mean unauthorized users, and certainly not any user on the Internet.

Candidate lower-level policies and procedures for update to accommodate the Internet and WWW include external connectivity, network security, transmission of data, use of electronic commerce, sourcing and procurement, E-mail, nonemployee use of corporate information and electronic systems, access to information, appropriate use of electronic systems, use of corporate assets, etc.

New policies and procedures (most likely enhancements to existing policies) highlight the new environment and present an opportunity to dust off and update old policies. Involve a broad group of customers and functional support areas in the update to these policies. The benefits are many. It exposes everyone to the issues surrounding the new technologies, the new security issues and challenges, and gains buy-in through the development and approval process from those who will have to comply when the policies are approved. It is also an excellent way to raise the awareness level and get attention to security up front.

The most successful corporate security policies and procedures address security at three levels, at the management level through high-level policies, at the functional level through security procedures and technical guidelines, and at the end-user level through user awareness and training guidelines. Consider the opportunity to create or update all three when implementing Internet, intranet, and WWW technologies.

Since these new technologies increase the level of risk and vulnerability to your corporate computing and network environment, security policies should probably be beefed up in the areas of audit and monitoring. This is particularly important because security and technical control mechanisms are not mature for the Internet and WWW and therefore more manual processes need to be put in place and mandated to ensure the protection of information.

The distributed nature of Internet, intranet, and WWW and their inherent security risks can be addressed at a more detailed level through an integrated set of policies, procedures, and technical guidelines. Because these policies and processes will be implemented by various functional support areas, there is a great need to obtain buy-in from these groups and ensure coordination and integration through all phases of the systems' life cycle. Individual and collective roles and responsibilities should be clearly delineated to include monitoring and enforcement.

Other areas to consider in the policy update include legal liabilities, risk to competition-sensitive information, employees' use of company time while "surfing" the Internet, use of company logos and trade names by employees using the Internet, defamation of character involving

company employees, loss of trade secrets, loss of the competitive edge, ethical use of the Internet, etc.

3.4 Appropriate Use Policy

It is important to communicate management's expectation for employee's use of these new technologies. An effective way to do that is to supplement the corporate policies and procedures with a more user-friendly bulletined list of requirements. The list should be specific, highlight employee expectations and outline what employees can and cannot do on the Internet, intranet, and WWW. The goal is to communicate with each and every employee, leaving little room for doubt or confusion. An Appropriate Use Policy (Exhibit 2) could achieve these goals and reinforce the higher level. Areas to address include the proper use of employee time, corporate computing and networking resources, and acceptable material to be viewed or downloaded to company resources.

Most companies are concerned with the Telecommunications Act and their liabilities in terms of allowing employees to use the Internet on company time and with company resources. Most find that the trade-off is highly skewed to the benefit of the corporation in support of the utility of the Internet. Guidelines must be carefully spelled out and coordinated with the legal department to ensure that company liabilities are addressed through clear specification of roles and responsibilities. Most companies do not monitor their employee's use of the Internet or the intranet, but find that audit trail information is critical to prosecution and defense for computer crime.

Overall computer security policies and procedures are the baseline for any security architecture and the first thing to do when implementing any new technology. However, you are never really finished as the development and support of security policies is an iterative process and should be revisited on an ongoing basis to ensure that they are up-to-date, accommodate new technologies, address current risk levels, and reflect the company's use of information and network and computing resources.

There are four basic threats to consider when you begin to use Internet, intranet, and Web technologies:

- Unauthorized alteration of data
- Unauthorized access to the underlying operating system
- Eavesdropping on messages passed between a server and a browser
- Impersonation

Your security strategies should address all of the above. These threats are common to any technology in terms of protecting information. In the remainder of this chapter, we will build upon the general “good security practices and traditional security management” discussed in the first section and apply these lessons to the technical implementation of security and control mechanisms in the Internet, intranet, and Web environments.

The profile of a computer hacker is changing with the exploitation of Internet and Web technologies. Computerized bulletin board services and network chat groups link computer hackers (formerly characterized as loners and misfits) together. Hacker techniques, programs and utilities, and easy-to-follow instructions are readily available on the net. This enables hackers to more quickly assemble the tools to steal information and break into computers and networks, and it also provides the “would-be” hacker a readily available arsenal of tools.

3.4 Internal/External Application

Most companies segment their networks and use firewalls to separate the internal and external networks. Most have also chosen to push their marketing, publications, and services to the public side of the firewall using file servers and Web servers. There are benefits and challenges to each of these approaches. It is difficult to keep data synchronized when duplicating applications outside the network. It is also difficult to ensure the security of those applications and the integrity of the information. Outside the firewall is simply *outside*, and therefore also outside the protections of the internal security environment. It is possible to protect that information and the underlying system through the use of new security technologies for authentication and authorization. These techniques are not without trade-offs in terms of cost and ongoing administration, management, and support.

Security goals for external applications that bridge the gap between internal and external and for internal applications using the Internet, intranet, and WWW technologies should all address these traditional security controls:

- Authentication
- Authorization
- Access control
- Audit
- Security administration

Some of what you already used can be ported to the new environment, and some of the techniques and supporting infrastructure already in

place supporting mainframe-based applications can be applied to securing the new technologies.

Using the Internet and other public networks is an attractive option, not only for conducting business-related transactions and electronic commerce, but also for providing remote access for employees, sharing information with business partners and customers, and supplying products and services. However, public networks create added security challenges for IS management and security practitioners, who must devise security systems and solutions to protect company computing, networking, and information resources. Security is a CRITICAL component.

Two watchdog groups are trying to protect online businesses and consumers from hackers and fraud. The council of Better Business Bureaus has launched BBBOnline, a service that provides a way to evaluate the legitimacy of online businesses. In addition, the national computer security association, NCSA, launched a certification program for secure WWW sites. Among the qualities that NCSA looks for in its certification process are extensive logging, the use of encryption including those addressed in this chapter and authentication services.

There are a variety of protection measures that can be implemented to reduce the threats in the Web/server environment, making it more acceptable for business use. Direct server protection measures include secure Web server products which use differing designs to enhance the security over user access and data transmittal. In addition to enhanced secure Web server products, the Web server network architecture can also be addressed to protect the server and the corporate enterprise which could be placed in a vulnerable position due to server enabled connectivity. Both secure server and secure Web server designs will be addressed, including the application and benefits to using each.

3.5 Web Browser Security Strategies

Ideally, Web browser security strategies should use a network-based security architecture that integrates your company's external Internet and the internal intranet security policies. Ensure that users on any platform, with any browser, can access any system from any location if they are authorized and have a "need-to-know." Be careful not to adopt the latest evolving security product from a new vendor or an old vendor capitalizing on a hot marketplace.

Recognizing that the security environment is changing rapidly, and knowing that we don't want to change our security strategy, architecture, and control mechanisms every time a new product or

solution emerges, we need to take time and use precautions when devising browser security solutions. It is sometimes a better strategy to stick with the vendors that you have already invested in and negotiate with them to enhance their existing products, or even contract with them to make product changes specific or tailored to accommodate your individual company requirements. Be careful in these negotiations as it is extremely likely that other companies have the very same requirements. User groups can also form a common position and interface to vendors for added clout and pressure.

You can basically secure your Web server as much as or as little as you wish with the current available security products and technologies. The trade offs are obvious: cost, management, administrative requirements, and time. Solutions can be hardware, software and personnel intensive.

Enhancing the security of the Web server itself has been a paramount concern since the first Web server initially emerged, but progress has been slow in deployment and implementation. As the market has mushroomed for server use, and the diversity of data types that are being placed on the server has grown, the demand has increased for enhanced Web server security. Various approaches have emerged, with no single *de facto* standard yet emerging (though there are some early leaders — among them Secure Sockets Layer [SSL] and Secure Hypertext Transfer Protocol [S-HTTP]). These are two significantly different approaches, but both widely seen in the marketplace.

Secure Socket Layer (SSL) Trust Model

One of the early entrants into the secure Web server and client arena is Netscape's Commerce Server, which utilizes the Secure Sockets Layer (SSL) trust model. This model is built around the RSA Public Key/Private Key architecture. Under this model, the SSL-enabled server is authenticated to SSL-aware clients, proving its identity at each SSL connection. This proof of identity is conducted through the use of a public/private key pair issued to the server validated with x.509 digital certificates. Under the SSL architecture, Web server validation can be the only validation performed, which may be all that is needed in some circumstances. This would be applicable for those applications where it is important to the user to be assured of the identity of the target server, such as when placing company orders, or other information submittal where the client is expecting some important action to take place.

Secure Hypertext Transfer Protocol (S-HTTP)

Secure Hypertext Transfer Protocol, (S-HTTP) is emerging as another security tool and incorporates a flexible trust model for providing secure Web server and client HTTP communications. It is specifically designed for direct integration into HTTP transactions, with its focus on flexibility for establishing secure communications in a HTTP

environment while providing transaction confidentiality, authenticity/integrity, and nonrepudiation. S-HTTP incorporates a great deal of flexibility in its trust model by leaving defined variable fields in the header definition which identifies the trust model or security algorithm to be used to enable a secure transaction. S-HTTP can support symmetric or asymmetric keys, and even a Kerberos-based trust model. The intention of the authors was to build a flexible protocol that supports multiple trusted modes, key management mechanisms, and cryptographic algorithms through clearly defined negotiation between parties for specific transactions.

3.6 Audit Tools and Capabilities

This topic will be discussed extensively in another unit, especially from a practical perspective as it relates to Internet Banking

WWW/Internet Audit Considerations

After your distributed Internet, intranet, and WWW security policies are firmly established, distributed security architectures are updated to accommodate this new environment. When planning for audit, and security control mechanisms are designed and implemented, you should plan how you will implement the audit environment — not only which audit facilities to use to collect and centralize the audit function, but how much and what type of information to capture, how to filter and review the audit data and logs, and what actions to take on the violations or anomalies identified. Additional consideration should be given to secure storage and access to the audit data. Other considerations include:

- Timely resolution of violations
- Disk space storage availability
- Increased staffing and administration
- In-house developed programming
- Ability to alarm and monitor in real time

3.7 WWW Security Flaws

As with all new and emerging technology, many initial releases come with some deficiency. But this has been of critical importance when that deficiency can impact the access or corruption of a whole corporation or enterprise's display to the world. This can be the case with Web implementations utilizing the most current releases which have been found to contain some impacting code deficiencies, though up to this point most of these deficiencies have been identified before any major damage has been done. This underlines the need to maintain a strong link or connection with industry organizations that announce code shortcomings that impact a sites Web implementation. A couple of the

leading organizations are CERT, the Computer Emergency Response Team, and CIAC, Computer Incident Advisory Capability.

Just a few of these types of code or design issues that could impact a sites Web security include initial issues with the Sun JAVA language and Netscape's JavaScript (which is an extension library of their HyperText Markup Language, HTML).

The Sun Java language was actually designed with some aspects of security in mind, though upon its initial release there were several functions that were found to be a security risk. One of the most impacting bugs in an early release was the ability to execute arbitrary machine instructions by loading a malicious Java applet. By utilizing Netscape's caching mechanism a malicious machine instruction can be downloaded into a user's machine and Java can be tricked into executing it. This doesn't present a risk to the enterprise server, but the user community within one's enterprise is of course at risk.

Other Sun Java language bugs include the ability to make network connections with arbitrary hosts (though this has since been patched with the following release) and Java's ability to launch denial of service attacks though the use of corrupt applets.

These types of security holes are more prevalent than the security profession would like to believe, as the JavaScript environment also was found to contain capabilities that allowed malicious functions to take place. The following three are among the most current and prevalent risks:

- JavaScripts ability to trick the user into uploading a file on his local hard disk to an arbitrary machine on the Internet
- The ability to hand out the user's directory listing from the internal hard disk
- The ability to monitor all pages the user visits during a session

The following are among the possible protection mechanisms:

- Maintain monitoring through CERT or CIAC, or other industry organizations that highlight such security risks.
- Utilize a strong software distribution and control capability, so that early releases aren't immediately distributed, and that new patched code known to fix a previous bug is released when deemed safe.

In sensitive environments it may become necessary to disable the browser's capability to even utilize or execute JAVA or JavaScript — a selectable function now available in many browsers.

4.0 CONCLUSION

Security solutions are slowly emerging, but interoperability, universally accepted security standards, application programming interfaces (APIs) for security, vendor support and cooperation, and multiplatform security products are still problematic. Where there are products and solutions, they tend to have niche applicability, be vendor-centric or only address one of a larger set of security problems and requirements. For the most part, no single vendor or even software/vendor consortium has addressed the overall security problem within “open” systems and public networks. This indicates that the problem is very large, and that we are years away from solving today’s problem, not to mention tomorrow’s.

5.0 SUMMARY

- Companies continue to flock to the Internet in ever-increasing numbers, despite the fact that the overall and underlying environment is not secure. To further complicate the matter, vendors, standards bodies, security organizations, and practitioners cannot agree on a standard, compliant, and technically available approach.
- Security requirements do not change with the introduction and use of these technologies, but the emphasis on where security is placed and how it is implemented does change
- It is clear that we need new and different policies, or minimally, an enhancement or refreshing of current policies supporting more traditional means of sharing, accessing, storing, and transmitting information
- It is important to communicate management’s expectation for employee’s use of these new technologies. An effective way to do that is to supplement the corporate policies and procedures with a more user-friendly bulletined list of requirements
- Most companies segment their networks and use firewalls to separate the internal and external networks. Most have also chosen to push their marketing, publications, and services to the public side of the firewall using file servers and Web servers.
- Ideally, Web browser security strategies should use a network-based security architecture that integrates your company’s external Internet and the internal intranet security policies.
- After your distributed Internet, intranet, and WWW security policies are firmly established, distributed security architectures are updated to accommodate this new environment
- As with all new and emerging technology, many initial releases come with some deficiency. But this has been of critical importance

when that deficiency can impact the access or corruption of a whole corporation or enterprise's display to the world.

6.0 TUTOR-MARKED ASSIGNMENT

1. Discuss briefly the objectives of Internet and WWW security
2. Mention 5 considerations to secure storage and access to audit data

7.0 REFERENCES/FURTHER READING

Krause, M. and Tipton, H.F. *Handbook of Information Security Management*