

# **The Evolution of Electronic Payments**

*by*  
***Benjamin Graham***

**School of Information Technology and  
Electrical Engineering,  
The University of Queensland.**

**Submitted for the Degree of  
Bachelor of Engineering  
in the Division of Electrical and Electronics Engineering  
October 2003**

101/24 Macquarie Street  
Teneriffe QLD 4005  
Telephone (07) 3254 4734

October 29, 2003

The Head  
School of Information Technology and Electrical Engineering  
The University of Queensland  
St Lucia QLD 4072

Dear Professor Kaplan,

In accordance with the requirements of the degree of Bachelor of Engineering in the Electrical and Electronics stream, I present the following thesis entitled "The Evolution of Electronic Payments". This work was performed under the supervision of Jon Whitty.

I declare that the work submitted in this thesis is my own, except as acknowledged in the text and endnotes, and has not been previously submitted for a degree at the University of Queensland or any other institution.

Yours sincerely,

Benjamin Graham

## **Abstract**

As authorities struggle to keep terrorism at bay, we are subjected to more digital attacks and credit card fraud than at any other time in history. We live in a world where criminals no longer need to carry guns. A computer now enables them access to all the money in the world. Meanwhile banks are encouraging the increased use of electronic payments and levels of fraud are experiencing dangerous growth. In considering these facts, I have chosen to investigate the sustainability and longevity of our current electronic payment systems.

I have concentrated on credit card and internet fraud and the susceptibility our current systems have to these crimes, realizing that significant advances in credit card and internet security cannot be achieved overnight. I have researched alternatives such as smart cards, biometric identification and radio frequency identification which I believe, based on my research, will form the backbone of our payments security in the short to medium term. More importantly I have also researched long term revolutionary changes, such as dual-currencies and alternative currencies, in the way we transact for goods and services.

## Acknowledgements

- **Mr Jon Whitty** – I would like to thank my thesis supervisor for his guidance and encouragement throughout the process of completing my thesis. Jon's positive attitude and support have been greatly appreciated.
- **My wife Cara** – I would like to thank her dearly, as without her help and support throughout this year, I do not think study and full-time work would have been possible.

## Table of Contents

ABSTRACT .....	3
ACKNOWLEDGEMENTS .....	4
TABLE OF CONTENTS.....	5
LIST OF FIGURES .....	6
CHAPTER 1 - WHERE ARE WE NOW? .....	7
CHAPTER 2 - HISTORY OF ELECTRONIC PAYMENTS .....	9
CHAPTER 3 - STRENGTHS AND WEAKNESSES OF OUR CURRENT SYSTEM .....	12
CHAPTER 4 - FRAUD .....	14
4.1    ONLINE FRAUD .....	14
4.2    IDENTITY & ACCOUNT THEFT .....	20
4.3    SPAM SCAMS .....	22
4.4    SKIMMING.....	25
CHAPTER 5 - POSSIBLE ALTERNATIVE SOLUTIONS .....	28
5.1    BIOMETRICS .....	28
5.1.1 <i>Facial Recognition</i> .....	31
5.1.1.1    Facial Scan Process .....	32
5.1.1.2    Verification versus Identification .....	32
5.1.1.3    Primary Facial Recognition Technologies .....	33
5.1.1.4    Facial Recognition and Payment Security .....	36
5.1.2 <i>Iris Recognition</i> .....	37
5.1.2.1    Iris Scan Process.....	38
5.1.2.2    Iris Recognition and Payment Security.....	40
5.1.3 <i>Fingerprint Recognition</i> .....	41
5.1.3.1    Fingerprint Process.....	42
5.1.3.2    Fingerprinting and Payment Security .....	43
5.2    SMART CARDS .....	45
5.2.1 <i>What is a Smartcard?</i> .....	45
5.2.2 <i>Risks of the Smart card</i> .....	49
5.3    PROXIMITY PAYMENTS .....	50
CHAPTER 6 - REVOLUTIONARY IDEAS IN PAYMENTS.....	52
6.1    DUAL-CURRENCY SYSTEMS.....	52
6.1.1 <i>What are Complementary Currencies?</i> .....	52
6.1.2 <i>How are Complementary Currencies different from Conventional Money?</i> .....	53
6.1.3 <i>Example of How Dual Currency Systems Work</i> .....	53
6.2    ATTENTION ECONOMY.....	55
CHAPTER 7 – CONCLUSION AND FUTURE RECOMMENDED WORK.....	59
REFERENCES .....	61

## List of figures

Figure 1 - Details of fraudulent and false-positive orders .....	18
Figure 2 - Victim's liability - identity fraud .....	21
Figure 3 - Victim's liability - account theft .....	21
Figure 4 - Time spent resolving problem - account theft .....	22
Figure 5 - Typical Eigenfaces - Source: MIT Face Recognition Demo Page .....	34
Figure 6 - Iris scan .....	39
Figure 7 - Iris scan .....	40
Figure 8 - Fingerprint characteristics .....	41
Figure 9 – Contact Smartcard .....	46
Figure 10 – Points on a Contact Smartcard .....	47

## Chapter 1 - Where are we now?

The evolution of payments in recent history has gone from cash to cheques to payment cards such as credit and debit cards. Each payment method has served its purpose very well, but as the level of electronic fraud continues to rise, authorities are realizing a more sophisticated technology or revolutionary change is needed.

Before writing-off the paper money society, it is important to remember that currently in the United States of America (US), 61% of transactions are paper-based. However this type of payment is rapidly decreasing. Only 13 years ago in 1990, paper-based payments represented 81% of transactions.<sup>1</sup>

Technology and convenience are seen as the primary reasons why these forms of payment are decreasing so rapidly, just as the substitution of paper money for precious metals paved the way for the industrial revolution. We are now seeing paper itself as an inconvenience in the payment process.

In recent years, with the closure of many traditional bank branches and the advent of internet banking, Automatic Teller Machines (ATMs) and Electronic Funds Transfer (EFT), we now have access to our money 24 hours a day, 7 days a week, 365 days a year through an electronic interface as opposed to a human one. Research suggests that more of us are embracing this technology than ever before.

However the growth seen in these types of payments and other modern technology has been a catalyst for today's modern criminals. Although payment technology and protective measures advance, so too does the sophistication of today's crooks.

---

<sup>1</sup> Marshall, R. 2002, "Prepare for paperless payments", *Financial Times*, 20 December, p 10.

Ironically, criminals now have access to the same conveniences that modern society craves when it comes to electronic payments.

## Chapter 2 - History of Electronic Payments

In 1918, electric money was born when Federal Reserve Banks first moved currency via telegraph. However it wasn't until the automated clearinghouse (ACH) was setup by the US Federal Reserve in 1972 that electronic currency became widespread. This provided the US Treasury and commercial banks with an electronic alternative to processing cheques.

In 1939, a serial inventor by the name Luther George Simjian created the Bankmatic automatic teller machine. He filed 20 patents and asked the company now know as Citicorp to trial it. After six months the bank had reported that there was no demand for such a product. However in 1968, Don Wetzel, Tom Barnes (mechanical engineer) and George Chastin (electrical engineer) conceptualized what is now known as the modern ATM. In 1969 and five million dollars later, the first prototype of the modern ATM was made and patents were then issued in 1973. The first working ATM was installed into the Chemical Bank based in New York City.

The first ATM's were off line machines, meaning that the money was not automatically withdrawn from users' accounts. Therefore only exclusive customers with good credit history were able to use ATMs. Today, almost everyone has access to the use of these devices and at last count there were over 352,000 ATMs in the US alone. These ATMs now perform over 1.1 billion transactions per month or 26,000 transactions a minute.

Charge cards date back to as early as 1914 when Western Union provided metal cards, allowing deferred payment privileges to preferred customers. These cards were colloquially known as "metal money". By 1924, General Petroleum Corporation was allowing customers to use metal money to buy fuel.

In the late 1930s, American Telephone and Telegraph (AT&T) introduced the “Bell System Card” and before long, railroads and airlines had introduced similar cards.

In 1950, Diners Club issued the first “plastic money” charge card and in 1951 it issued the first credit card to 200 customers who could use it at 27 different restaurants in New York. Bank of America issued the BankAmericard (now Visa) - the first bank credit card - later in 1958. This was first promoted to traveling salesmen (more common in that era) for use on the road. By the early 1960s, more companies offered credit cards, advertising them as a time-saving device rather than a form of credit. But it wasn't until the establishment of standards for the magnetic strip in 1970 that the credit card became part of the information age.<sup>2</sup> This saw companies such as American Express and MasterCard become huge successes overnight, which prompted moves by Congress to begin regulation of the credit card industry by banning practices such as the mass mailing of active cards to those who had not requested them.

In 1983, RSA encryption algorithm was invented by Ronald Rivest, Adi Shamir and Len Adelman, (hence the name RSA) at MIT's Laboratory for Computer Science. The breakthrough was that it allowed for encryption in a multi-user environment, that is, no active participation was necessary between the sender and the receiver of data at the other end.

Unfortunately credit card security has not seen substantial growth during this time. Although some security improvements have been made, the actual process of reading numbers off a magnetic strip and possibly a signature to verify the user is realistically as far as the industry has progressed.

---

<sup>2</sup> Bellis, M. 2003, “The History of Money and Credit Cards”, <http://inventors.about.com/library/inventors/blmoney.htm>

Compared to the advances of almost any other industry over the last 30 years, it is no wonder credit card issuers are finding it hard to quell consumer concerns over security.

## Chapter 3 - Strengths and Weaknesses of our Current System

Despite the fact that the current credit card system lends itself to fraud, it does have a lot of advantages. Ironically many of the reasons why credit cards have become so popular are the same as those that lead to greater fraud risk. The convenience of being able to use a credit card at almost any location interstate or internationally at any retailer, without so much as a signature, is seen by many as a right. Is the cost convenience becoming too great?

If for example a restaurateur was to question the validity of a patron's signature after the patron had enjoyed 2 bottles of wine at dinner, the patron may be offended and never return to the restaurant. If so, was it really worth questioning the signature in the first place?

As the cost of credit card fraud is currently the merchant's responsibility, a retailer needs to employ a risk management strategy to include weighing up both inconvenience and potential financial harm.<sup>3</sup> Let's say the retailer was to assume 5% of its credit card sales are fraudulent. While the merchant could require photo identification for every credit card user, how great would the percentage of customers be that are going to view this as inconvenient and choose another merchant? From another perspective, some customers might believe that if their credit card was stolen, a thief would be less likely to be able to use the card with that merchant. Therefore the merchant could be perceived as going the extra mile to protect them.

Credit cards do not require personal identification numbers (PIN) to remember and, in many cases, not even a card is required, just the card's number and expiry date. On top of this, many credit card receipts thrown out everyday disclose all this

---

<sup>3</sup> Tedeschi, T. 2002, "Retail Executives are Uniting to Fight Credit-Card Fraud in the Online-Bazaar", *New York Times*, October 21, Late Edition (East Coast), p C6.

information. Although more modern EFT terminals have hidden some of this information, many still do not. However having no PIN allows merchants to perform off-line transactions. It also enables a customer who may not be in the same country as the merchant the ability to purchase products over the phone or internet in a matter of minutes. Although increasing the risk of fraud, credit card payments such as this, have enabled an increase in sales. But is this increase in sales starting to be overtaken by the amount of credit card fraud?

## Chapter 4 - Fraud

### 4.1 Online Fraud

Bank robbery is still big business around the world. But thanks to surveillance cameras, guards, alarms, security screens, dye packs and law enforcement efforts, the odds of walking into a bank and successfully stealing large sums of cash are stacked heavily against today's criminal.

However the risks commonly faced by the likes of Ned Kelly earlier in the century are nearly all but mitigated. Thanks to the internet banking and high tech credit card fraud, it is now possible to steal large amounts of money anonymously from financial institutions from the comfort of your own home and it is happening all over the world.

Italian police broke up a Mafia scheme to "clone" an online branch of the Banco di Sicilia and siphon hundreds of millions of dollars from an account belonging to the Sicilian regional government. The gang, with help from two bank employees and a couple of Telecom Italia technicians used stolen computer files, codes and passwords to penetrate the bank's systems.<sup>4</sup>

In analyzing the most vulnerable part of any financial service enterprise, the credit card division would be nearly always at the top of the list. The US secret service calls credit card fraud "the bank robbery of the future"<sup>5</sup> because it is seen as easy pickings to criminals. This is emphasized by the recent study by the Internet Fraud Prevention Advisory Council which found that on-line fraud as a percentage of business revenue was as much as 40 times higher than "real world" fraud. This

---

<sup>4</sup> Alexander, M. 2003, "Web fraud undetected? Not for long", *USBanker*, June 2003, p 80.

<sup>5</sup> *Ibid.*

on-line credit card fraud cost businesses an estimated \$US 9 billion in 2001 and, according to Meridien research, could reach as high as \$US 60 billion by 2005.<sup>6</sup>

Although these figures represent the high side of researched estimations, researchers all agree that on-line fraud is high. A 2002 survey of e-merchants by Stamford, found that fraudulent transactions comprise 1% of total online transactions, which is 15 times higher than fraud in the physical world. With the on-line retail market growing rapidly and with an already estimated turnover of over \$US 45 billion per annum, the card industry cannot afford to lose this market due to lack of innovation.<sup>7</sup>

This is not to say that nothing has been done to curb cyber fraud. The card industry and law enforcement agencies have devoted a lot of time and money to the cause with the first efforts starting over 10 years ago. However a viable solution still eludes them, in part due to the ever-changing face of online fraud. It can range from stolen card numbers used at a pornographic web site, to a hacker breaching an online merchant's database. The worst of these reported to date was earlier this year when a computer hacker gained access to millions of debit and credit card numbers from a processor's database. At least 3 debit card issuers cancelled and reissued cards in response to the attack, which affected up to 8 million debit and credit card account numbers, including 2.2 million MasterCard and about 3.4 million Visa accounts, the associations reported on February 14, 2003.

These large scale breaches of web site databases are probably the most concerning for international credit card companies. This is mainly due to the fact that there are literally tens of millions of businesses around the world that accept, store and recurrently bill credit cards. As they cannot realistically manage every

---

<sup>6</sup> Ibid.

<sup>7</sup> Punch, L. 2003, "A problem yet to be solved", *Credit Card Management*, April 2003, p 18.

single business that uses their card services, security of this information is up to business itself. With many organizations facing rising costs and with recent economic downturn, companies are under increasing pressure to bring value to shareholders. To many companies, security can be seen as an expensive, yet expendable item. However as CD Universe (a web-based CD store) found out in January 2000, security is paramount. A hacker broke through their security system and gained access to 300,000 credit card account numbers resulting in the web site being shut down.<sup>8</sup>

Compare this to the more publicly feared “in transit” type of hack which is where the credit card numbers are stolen whilst being transmitted from your computer to the merchant’s computer. The risks and reward are significantly less, not only because it is locked down with transaction encryption but also because you have to sniff literally millions of messages and packets to find any useful information. Further, a hacker can usually only uncover one set of credit card details at a time.<sup>9</sup>

Criminals use many ways to hack into merchants’ databases. One of the more common ways is to exploit weaknesses in the software. Usually software companies who produce such software issue patches to fix weak spots. However, in many cases, web-site administrators are reluctant to install all of these patches for fear it will disrupt the system, which from their point of view can be seen as a bigger disaster. Ironically even when a web site is hacked, that site is usually not the one where the fraudulent credit card transaction takes place - it is the subsequent web site the fraudsters visit that will pay the price.

Once a thief obtains credit card details, they have to be used to purchase goods or services to complete the crime. One of the best weapons of an on-line criminal is geographic anonymity. Whereas once upon a time when credit cards were stolen,

---

<sup>8</sup> Ibid.

<sup>9</sup> Ibid.

the merchant would be able to report the stolen card immediately and authorities could apprehend the thief on-site, the internet has opened a seemingly infinite source for obtaining card numbers and other consumer information whilst also providing literally millions of sites where these details can be used. However with the introduction of geolocation technology, the merchant is able to instantly locate the origin computer down to the metro area level by identifying the internet protocol (IP) domain of the origin computer. This allows the merchant to flag potentially fraudulent transactions. If a customer in Australia is buying goods or services from the United Kingdom to be delivered to Hong Kong, this would be raised as a high fraud risk. Studies by ClearCommerce identify a short list of 15 nations that produce 60% of fraudulent transactions. In the later half of 2002, more than 10% of the transactions originating from Yugoslavia, Nigeria and Romania turned out to be scams, and Pakistan, Indonesia and Bulgaria were all over 6%. However ClearCommerce recently discovered that transactions approved by the bank card associations' address verification system (geolocation technology) had a higher fraud rate than transactions that were declined. In the past, the fraud rate (on approved transactions) was about 0.20% or 0.25% and in the last six months the fraud rate has grown to 0.95%.<sup>10</sup>

This growth is suspected to be caused by the increase in account takeover. Account takeover is when a fraudster calls a credit card issuer and changes the cardholder's address and contact details to the fraudster's contact details. Then when an order is placed and the relevant checks are made, the item is shipped as a low fraud risk case. When the actual owner of the card discovers the unauthorized charge/s, which can take a considerable amount of time because of the change of address, the fraudster has usually moved on.

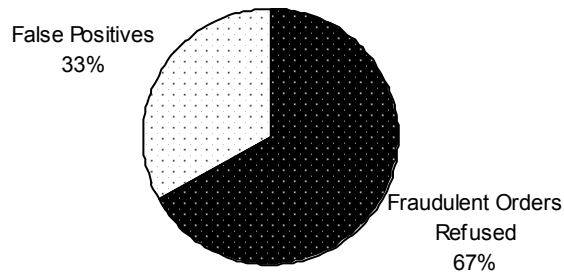
But as vigilance rises, so too does the incidence of "false-positives." This is when a merchant refuses an order based on the higher risk factor determined when the

---

<sup>10</sup> Ibid.

transaction was in fact legitimate. The process of judging a book by its cover can prove quite costly, as not only sales but loyalty is lost.

The top 25 online merchants last year predicted that they would reject \$US 315 million in sales during the 2002 holiday season because transactions looked fraudulent. This accounts for 6% of total online orders being rejected, with one-third of these rejected orders being false positives, making 2% of all online orders being mistakenly rejected. Roy Banks, general manager of Authorize.net, says that “false-positive is an unfortunate by-product of employing stringent fraud-fighting systems, you can be too risk averse”.<sup>11</sup>



**Figure 1 - Details of fraudulent and false-positive orders**

The problem with this is that there is no magic cure. Merchants need to tailor their fraud risk analysis specifically to their area of business and the types of clientele they attract.

---

<sup>11</sup> Simpson, B. 2003, 'Throwing out the good with the bad', *Credit Card Management*, July 2003, p 40.

Fair Isaac Corporation is a company that uses a neural network to build profiles of cardholder behavior by reviewing billions of transaction records. This in turn allows them to conduct risk analysis and predictive modeling. When an order is reviewed, it will receive a score between 0 – 1,000 signifying the level of risk, with 1,000 being the highest level of risk. A merchant will then select a cut-off number for accepting or declining a transaction. They also create a false-positive rate for all transactions. For example, if a merchant were to receive 16 orders with a risky score of around 800, with one order having particularly strong fraud indications, the false-positive ratio is 15 to 1. If the same merchant receives 40 orders in the 600 range, but only one looks fraudulent, that range will be given a 39 to 1 false-positive ratio.<sup>12</sup>

This is where a merchant needs to adopt a strategy relevant to their own business. If they are operating on high margins, they will probably not mind losing 1 out of every 40 transactions to fraud. However if you are dealing with a very low margin product having a high false-positive ratio can be the downfall of your business.

It is easy to understand why online merchants are concerned, with law-enforcement agencies concentrating their efforts on six-figure loss cases, small e-merchants have an uphill battle. The losses usually extend beyond the cost of the product or service charged to a fraudulent card. Because e-merchants operate in a “card not present environment” the retailer is subjected to the highest interchange rates. Under Mastercard’s interchange rates, a merchant pays 1.90% plus 10 cents for every internet transaction, compared with 1.40% and 10 cents for a card-present transaction. What’s more, online merchants face stiff fines and may lose their right to accept cards if their fraud and charge-back rises above certain levels.<sup>13</sup>

---

<sup>12</sup> Ibid.

<sup>13</sup> Punch, L. 2003, “Fraud-control tug of war”, *Credit Card Management*, June 2003, p 44.

## 4.2 Identity & Account Theft

Identity theft is one of the fastest growing epidemics in electronic fraud in the world. Identity theft occurs when fraudsters gain access to personal details of unsuspecting victims through various electronic and non-electronic means. This information is then used to open accounts (usually credit card), initialize loans and mobile phone accounts or anything else involving a line of credit.

Account theft, which is commonly mistaken for identity theft, occurs when existing credit or debit cards or financial records are used to steal from existing accounts. Although account theft is a more common occurrence than identity theft, identity theft financial losses are on average greater and usually require a longer period of time to resolve.

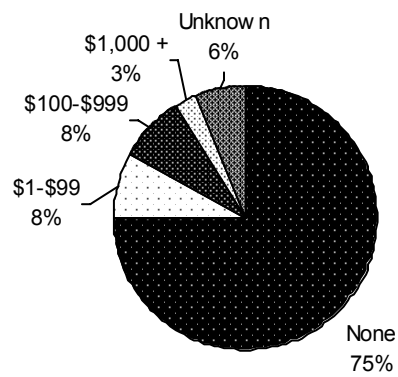
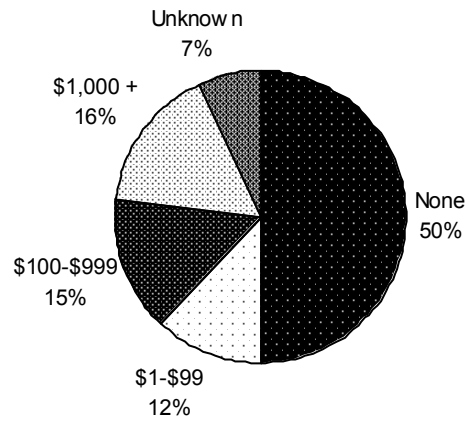
The Federal Trade Commission (US) has released some staggering figures on identity and account theft. In the last five years, 27.3 million Americans have fallen victim to these crimes. The Commission also reported that these cases have collectively cost businesses \$US 32.9 billion and consumers \$US 3.8 billion. This equates to an average loss for identity theft of \$US 10,200 for businesses and financial institutions and \$US 1,180 for consumers, plus an average 60 hours work spent repairing their credit history. Account theft in contrast costs businesses an average of \$US 2,100 a case and consumers \$US 60 plus an average of 15 hours rectifying the situation. As the time taken to discover identity theft is great than account theft, the level of damage is usually greater.<sup>14, 15</sup>

---

<sup>14</sup> Davenport, T. 2003, "FTC: ID theft costs \$50 billion", *American Banker*, September 2003, p 3.

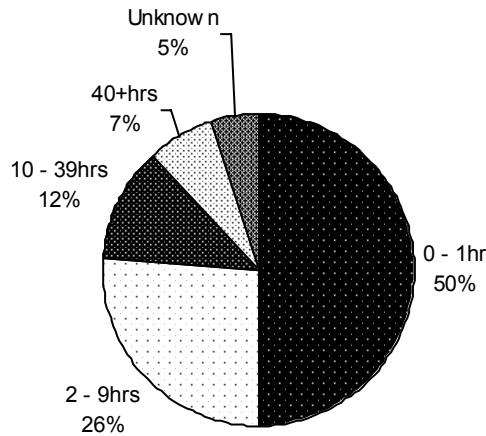
<sup>15</sup> Lee, J. 2003, "Identity Theft Victimized Millions, Costs Billions", *New York Times*, September 2003, p 20.

**Figure 2 - Victim's liability - identity fraud**



**Figure 3 - Victim's liability - account theft**

**Figure 4 - Time spent resolving problem - account theft**



### **4.3 Spam Scams**

Card issuers and customers rely on the internet and email to send and receive all sorts of messages from promotions to billing information. But junk unsolicited email known as “spam” is filling up customers’ inboxes and is fast becoming an epidemic around the world. Most of us would be very familiar with the affects of spam and increasingly, legitimate messages from companies with whom existing relationships have been established are being dismissed. Complaints from Internet Service Providers (ISP), lawmakers and legitimate businesses are demanding solutions for a problem which is estimated at costing up to \$US 10 billion a year.<sup>16</sup>

In recent months, the Australian Federal Police (AFP) have been investigating a spate of ghost sites posing as Internet banking sites of major Australian banks in

<sup>16</sup> Potomac, 2003, “Fighting the phantom menace: Junk e-mail linked to identity theft and fraud”, *Card News*, May 2003, p 1.

order to capture customer passwords and access codes. The fraudsters have been sending spam emails informing customers of some seemingly legitimate reason to log in to their accounts. A link is provided in the email to take the user to a log in screen of their bank site, however the link that is provided actually takes the user to a ghost site, where their log in details can be recorded by the fraudster. This information is then used to pay bills and or transfer balances for the fraudster's financial reward

A spokesperson for the Australian High Tech Crime Centre, an agency hosted by the AFP, said on August 27, 2003, that arrests have been made in connection with the Internet banking scams but would not reveal how many.<sup>17</sup>

However spams are not always this sophisticated. Internet-based payments are attracting a more mainstream, and less technically-oriented, market. Spammers are taking advantage of this fact and are sending mass emails asking to update all sorts of personal information which can be used for such crimes as identity fraud and credit card fraud. Because the spammer can send millions of these messages at a time, they only need a very small number of replies to make it worth while.

For example, a Californian citizen recently received an email seemingly from PayPal Inc. "Paysecurity" mailbox said her account with the payment service provider was under review because of inactivity and asked her to confirm her new email address. The email also asked her to verify her account password, credit card information and PIN of her ATM card.

These questions rang alarm bells, even though the message looked exactly like the one from PayPal and contained a link to what looked like the PayPal site, right

---

<sup>17</sup> Anonymous, 2003, "Australian police close 'ghost' bank sites, make some arrests in ongoing investigation", *BNA's Banking Report*, September 2003, p 340.

down to the boilerplate notices at the bottom. She contacted PayPal and confirmed her suspicions that it was in fact a fraudulent email.<sup>18</sup>

Currently there is no reliable weapon to combat the fraudsters faking these emails from reputable institutions. Although most net surfers are savvy enough these days to recognize the differences in an email from their bank and a spammer, many are still getting tricked into supplying their details. The problem lies in the fact that no company is currently prepared to guarantee that its products can prevent these crimes and products that have been used to safeguard email scams are ones which criminals are able imitate.

ePrivacy has developed what they call a “trusted sender” seal, which is not a simple digital file that can be easily faked. Each seal, which bears the brand of the sender, is generated on an individual basis and cryptographically protected. Recipients are also able to verify the message authenticity by clicking on the seal, which then sends them to a screen which verifies the address of the sender, recipient and date. Although this will deter the less experienced spammer, Stephen Cobb senior vice president admits that an experienced hacker could imitate it. Eric A. Wagner an attorney at the Federal Trade Commission’s bureau of consumer protection said a hacker could easily spoof such a seal commenting that “it might not be the same thing, but it would look real enough”.<sup>19</sup>

SunTrust Banks Inc. is an organization that has set up a formal method of tracking unauthorized use of its brand. This is done through its e-commerce risk management group, set up two years ago for Internet-related risks. The group’s main aims are to ensure that SunTrust’s partners and vendors meet all the latest in

---

<sup>18</sup> Wade, W. 2003, “Con artists stealing data via phony bank sites”, *American Banker*, June 2003, p 17.

<sup>19</sup> Costanzo, C. 2003, “No bulletproof shield against new e-scams”, *American Banker*, October 2003, p 1.

security and privacy standards. The group also monitors all use of SunTrust's brand online to try and detect any unauthorized use.<sup>20</sup>

The most concerning aspect of this type of crime is that it is threatening to undermine consumer confidence in technology whilst also devaluing the potential of the internet.

#### **4.4 Skimming**

Law enforcement authorities have been exposed as almost powerless to crack down on a new breed of criminals using hi-tech devices as well as very low-tech methods to steal credit card details. Card skimming refers to the use of portable swiping devices (usually not much larger than a pager) to obtain credit card and EFT card data. This data is rewritten to a dummy card, which is then usually taken on elaborate shopping sprees. As the fraudster can sign the back of the card themselves, the merchant will usually be none-the-wiser that they have fallen victim to the fraud.

The most common targets for card skimmers are places where the card is actually taken away from the owner, such as restaurants. Service stations are also a common target as customers are often in a rush and can be distracted easily. Overseas intelligence indicates criminal gangs have intercepted data cables from department stores and other commercial premises capable of copying credit card and Eftpos data. This skimmed card data is then transmitted overseas, usually to South - East Asia, where the information is recorded on bogus cards with Australian bank logos.<sup>21</sup>

---

<sup>20</sup> Ibid.

<sup>21</sup> Jones, C. 2003, "Millions swiped by credit crooks", *The Courier Mail*, June 13, p 9.

Another style of skimming which is becoming more widespread is ATM skimming. The two most common methods of ATM skimming involve either altering the ATM itself, or placing a plastic sleeve into the machine's card slot.

When a criminal alters the ATM, a device which is designed to look like part of the machine is placed over the card slot. This device reads the magnetic strip and stores the data. However as the PIN of 4 to 6 digits, which is not stored on the card itself, is still required to fleece the accounts, pinhole cameras are also placed strategically to record the number sequence. Once this information is retrieved, the fraudster has everything they need to reproduce the cards and empty the bank accounts.

The other style involves inserting a plastic sleeve in the card slot of the ATM that traps the card. When an unsuspecting cardholder inserts their card and enters their PIN and nothing happens, a seemingly helpful member of the public then comes along and tells the person to enter their PIN again. The cardholder complies but the card remains trapped in the sleeve. They eventually give up, leaving the criminal to take the sleeve and the card out of the machine. Armed with the PIN they have just noted, they can now empty the account straight away.<sup>22</sup>

Although preventing traditional skimming is very difficult, ATM manufacturers have been working on features designed to fight ATM skimming. Newer machines from Diebold Inc and NCR Corporation have sensors that detect foreign objects and send alert messages to the host data centre, which can then send a security officer to the site to investigate further. Diebold machines also have a metal pin that rises to prevent further transactions taking place after a foreign object has been detected. Both NCR and Diebold have also made "jitter technology" available, which moves the card in and out in irregular patterns to prevent skimmers from reading the data properly. This technique means skimming devices setup on

---

<sup>22</sup> Clayton, H. 2003, "Hole-in-the-wallet machines", *Financial Times (London)*, August 2, p 22.

ATMs will record data that is repeated, backwards and not legible, making the scan useless.<sup>23</sup>

But as the authorities improve security measures, criminals too are coming up with new and more innovative ways of stealing money. Some recent cases have emerged with criminals buying ATMs and reprogramming them to record card and PIN data. As it is virtually impossible to control the deployment of fraudulent ATMs on the open market, this is a difficult situation to solve.<sup>24</sup>

---

<sup>23</sup> Breitkopf, D. 2003, "ATM makers tout new fraud-fighting features", *American Banker*, June 10, p 8.

<sup>24</sup> Ibid.

## Chapter 5 - Possible Alternative Solutions

### 5.1 Biometrics

The key focus in minimizing credit card and electronic fraud is to enable the actual user of the account to be correctly identified. The notion of allowing a card to prove your identity is fast becoming antiquated and unreliable. With this in mind, using biometrics to develop a more accurate identification process could greatly reduce fraud and increase convenience by allowing consumers to move closer to a “no wallet” society.

The main forms of biometrics which are available today are:

- Fingerprinting
- Facial recognition
- Iris recognition
- Voice recognition
- Computer recognized hand writing analysis

Although all of these biometric techniques are accurate ways of identifying people, voice recognition and handwriting analysis do not lend themselves to electronic payments use as easily. Hand writing styles change over time and, depending on the state the customer (i.e. sober), could easily affect their ability to satisfy the computer of their identity. A similar problem is experienced with voice recognition. If the environment experiences high levels of background noise, the ability to identify the customer becomes more difficult.

The International Biometric Group (IBG) of New York recently tested 240 people from various demographic groups on eight different fingerprint systems and two face recognition systems currently available on the market. The finger scanning systems analyzed were from American Biometric Co., Digital Persona, Identicator,

Identix, Mytec, Sony, ST micro Electronics and Veridicom and the face recognition systems were from Miros and Visionics. They found that the major factors which affect the accuracy of these systems are age, race and profession.<sup>25</sup>

Experts in these fields of identification technologies have long suspected that the elderly, Asians and people who are subjected to large amounts of physical hand contact such as construction workers would be difficult to identify. IBG say its study has been the first of its kind to compare and contrast how a number of different biometric identification systems stack up against each other.

One of the key performance measures in the study was the “failure to enroll” rate which is when a system cannot distinguish a user the first time the person’s face or fingerprint is presented. Variances in failure to enroll rates on different systems were mainly demographic highlighting the system’s country of origin.

However with iris scanning, an exact match will almost always be achieved as the environment, race or profession has almost no bearing on the result. But these procedures are also considered to be the most invasive and as such many consumer groups are opposed to their use.<sup>26</sup>

In a study conducted by SYNERGISTICS Research Corporation, results showed the majority of ATM users believed a biometric identification system would be a welcome improvement over current PIN-based identification methods. The survey consisted of 1,000 people aged 18 years or older with household incomes greater than \$US 25,000 per annum. Finger or handprint analysis was the preference of more than 4 in 10 ATM users. A quarter of participants preferred iris scanning, one in eight would prefer signature verification and one in ten preferred voice recognition. The majority of all surveys also agreed that they felt a biometric

---

<sup>25</sup> Snel, R. 1999, “On-line banking: Factors found to affect accuracy of biometric identification systems”, *American Banker*, April 1, p 13.

<sup>26</sup> Ibid.

identification system would make them feel more secure in performing the transaction as well.<sup>27</sup>

A fingerprinting trial is currently being tested at three supermarkets in the US. Participants register with one of the stores by placing one finger on an electronic screen which records a digital template. Makers of the equipment say that rather than recording an actual image, the equipment recognizes important elements of the fingerprint, such as the intersection of lines. This encrypted information is linked to either their credit or debit card and usually to some sought of loyalty card as well. A picture ID also establishes the customer's identity.

The supermarkets which have installed the system say that limiting fraud was their main goal in introducing the finger imaging system. In 2000, credit card fraud costs grocery chains an average of US\$ 179,000 each, while debit card fraud cost them more than \$US 17,000, according to a survey conducted last year by the Food Marketing Institute, a supermarket trade association.<sup>28</sup>

When Purdue University asked its employee credit union to extend service to its Westville campus, the credit union studied how to provide 24-7 access without building a new branch. Opening a traditional ATM was not going to be enough as there would be no way to open an account.

Members using a Purdue EFCU kiosk to open an account have their fingerprints scanned as well as a copy of their driver's license and their face to provide a backup security measure. The next day, staff at the credit union review the scanned information to verify the details of the account. This then allows members next day ATM access to their accounts without waiting for a card.

---

<sup>27</sup> Anonymous, 2003, "ATM-users say they would welcome biometric efforts", *Credit Union Journal*, June 2, p 8.

<sup>28</sup> Blank, C. 2002, "At Grocery Checkout, No Wallet Needed", *New York Times*, 25 July, Late Edition (East Coast), p 3.

Before launching the biometric kiosks, Purdue EFCU tested them in their main lobby. Their success was instantaneous with members not wanting to see them removed from the lobby.

The biometric kiosks open around 3,000 to 4,000 accounts at the start of semester at the university and about 23% (14,430) of all Purdue EFCU members use the biometric kiosks.<sup>29</sup>

### **5.1.1 Facial Recognition**

Facial recognition involves the use of facial features, such as the upper outlines of the eye sockets, the areas surrounding the cheekbones, the sides of the mouth, and the location of the nose and eyes, to perform verification and identification. As with other forms of biometrics, using facial recognition for the purpose of identifying individuals is not an exact science. Rather, the various features of the individual's face are matched with a pre-existing image to determine whether sufficient likeness exists to conclude that the individual and the image are the same.

Facial recognition is limited by two factors:

- the ease with which individuals can manipulate their appearance through the use of disguises or, in more extreme cases, plastic surgery; and
- the quality of the image to which the individual is being matched.

Obviously, the higher the image quality, the more accurate the matching process. For example, images taken from live subjects are more likely to result in an accurate match than sketched images.

---

<sup>29</sup> Bankston, K. 2001, "Biometrics: toys or tools?", *Credit Union Journal*, January, p 51.

### **5.1.1.1 Facial Scan Process**

Four steps are utilized in undertaking a facial scan:

- sample capture
- feature extraction
- template comparison
- matching.

To enhance accuracy, several pictures are typically taken of the face using slightly different angles and facial expressions. The pictures enable distinctive features to be identified resulting in the creation of a reference template. To perform the matching, a comparison is made between the similarity of the individual with the reference template on file. The point at which two templates are similar enough to match, known as the threshold, will be dependent on the use to which the information will be put.

### **5.1.1.2 Verification versus Identification**

Given that facial recognition is effectively a 'best guess' technique rather than a definitive method of identification, facial scan identification systems can only attempt to answer the question "Who am I?" If there are a limited number of reference templates in the database, this requirement is not demanding. However, as the number of reference templates in the database grows, this task becomes much more difficult. It is likely that the system may only be able to narrow the database to a number of potential candidates, with human intervention required at the final verification stages.

The success of using facial recognition for the purpose of identification is also subject to the interaction between the target subjects and capture device. Facial scan technology needs to be able to cope with subjects that are uncooperative as a failure to do so will render the system useless.

### 5.1.1.3 Primary Facial Recognition Technologies

The four primary methods employed by facial recognition systems to identify and verify subjects are:

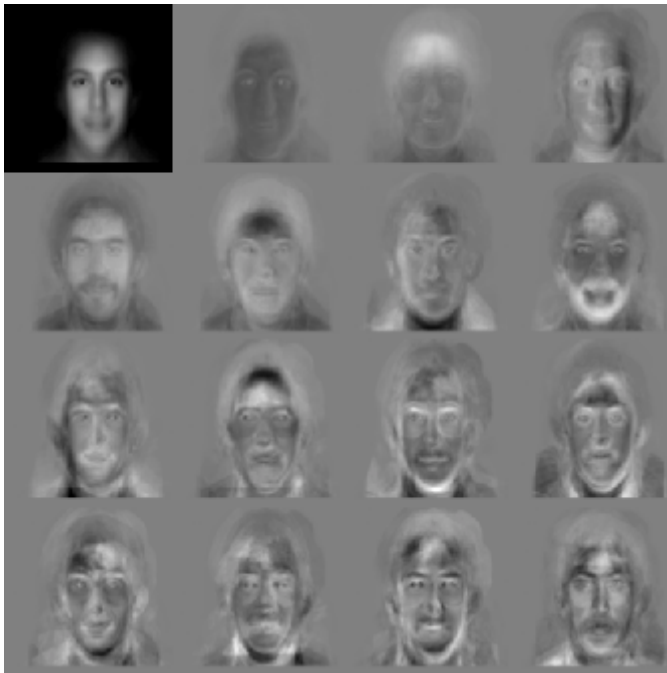
- Eigenfaces
- feature analysis
- neural network
- automatic face processing

Some types of facial scan technology are more suitable than others for applications such as forensics, network access, and surveillance.

"Eigenface," roughly translated as "one's own face," is a technology patented at MIT which utilizes two dimensional, global grayscale images representing distinctive characteristics of a facial image.<sup>30</sup> Variations of eigenface are frequently used as the basis of other face recognition methods.

---

<sup>30</sup> [http://www.biometricgroup.com/reports/public/reports\\_iris-scan.html](http://www.biometricgroup.com/reports/public/reports_iris-scan.html)



**Figure 5 - Typical Eigenfaces - Source: MIT Face Recognition Demo Page**

Distinctive characteristics of the entire face are highlighted for use in future authentication. The vast majority of faces can be reconstructed by combining features of approximately 100-125 Eigenfaces. The subject's Eigenface is mapped to a series of numbers (coefficients). For 1-to-1 authentication, in which the image is being used to verify a claimed identity, one's "live" template is compared against the template to determine coefficient variation. The degree of variance from the template will determine acceptance or rejection. For 1-to-many identification, the same principle applies, but with a much larger comparison set. Like all facial recognition technology, Eigenface technology is best utilized in well-lit, frontal image capture situations.

Feature analysis is perhaps the most widely utilized facial recognition technology. This technology is related to Eigenface, but is more capable of accommodating

changes in appearance or facial aspect (for example, smiling versus frowning). Visionics, a prominent facial recognition company, uses Local Feature Analysis (LFA), which can be summarized as an "irreducible set of building elements." LFA utilizes dozens of features from different regions of the face, and also incorporates the relative location of these features. The extracted (very small) features are building blocks, and both the type of blocks and their arrangement are used to identify/verify the subject. It anticipates that the slight movement of a feature located near one's mouth will be accompanied by relatively similar movement of adjacent features. Since feature analysis is not a global representation of the face, it can accommodate angles up to approximately 25° in the horizontal plane, and approximately 15° in the vertical plane. A straight-ahead video image from a distance of three feet will be the most accurate. Feature analysis is robust enough to perform 1-1 or 1-many searches.

In Neural Network Mapping technology, features from both faces – the template and live face - vote on whether there is a match. Neural networks employ an algorithm to determine the similarity of the unique global features of live versus reference faces, using as much of the facial image as possible. An incorrect vote, i.e. a false match, prompts the matching algorithm to modify the weight it gives to certain facial features. This method theoretically leads to an increased ability to identify faces in difficult conditions. As with all primary technologies, neural network facial recognition can do 1-1 or 1-many.

Automatic Face Processing (AFP) is a more rudimentary technology, using distances and distance ratios between easily acquired features such as eyes, end of nose, and corners of mouth. Though overall not as robust as Eigenfaces, feature analysis, or neural network, AFP may be more effective in dimly lit, frontal image capture situations.

#### **5.1.1.4 Facial Recognition and Payment Security**

The success of facial recognition is largely dependent on users' perceptions of its accuracy and intrusiveness. Other biometric technologies such as retinal scan and finger scan are sometimes perceived as being intrusive or invasive.

The use of facial scan biometrics in applications such as ATM access and network logon suggests that acceptance of the technology is high among users. However, IBG's Consumer Response to Biometrics performed a study which highlights that there are some reservations which may limit facial scan's broader usage. Using a scale of 1 – 5 (1 = very comfortable, 5 = very uncomfortable), subjects were asked to rate how they would feel using a finger scan system instead of a PIN when using an ATM as opposed to using a facial recognition system instead of a PIN when using an ATM.

Finger scan rated 2.19, and face geometry (facial scan) rated 2.43. The results clearly demonstrate the viability of biometrics in this area, but are markedly better for finger scanning than face scanning. The lower rating for facial scanning were explained as follows:

1. Many people simply don't like having their picture taken, much less having to look at their own low-resolution image on a computer screen or terminal. Both men and women expressed reservations, suggesting that the cameras being used were low quality (they were actually high-quality), insisting on wearing hats if being photographed, looking for mirrors etc. In contrast to finger scan testing, where all subjects used the devices in spite of whatever slight reservations they may have had, some subjects in the face geometry testing simply refused to use the technology.

2. Despite its use in everyday life as our primary means of recognition, the face (as opposed to a signature or fingerprint) is not traditionally interpreted as an

authentication mechanism. The face is almost too personal a part of the body to think of its being "scanned", broken into grids or axes, or having prominent features made note of.

3. On the topic of intrusiveness, most vendors suggest that facial scan is the least intrusive technology. In terms of ease-of-use, this is probably true - looking at a camera and holding still momentarily is not a demanding task. However, if intrusiveness is defined in a different way, facial scan may be among the most intrusive technologies. Aside from voice, which is largely incapable of executing 1-to-many searches (where the subject's identity is not known), face is the only commonly used biometric which does not require cooperative subjects. A hidden camera could take your picture, and perform 1-to-many identification, without your knowledge. Of course, such 1-to-many identification is not inherently problematic - there are situations where it is beneficial (surveillance of embassies or military sites).

### **5.1.2 Iris Recognition**

Iris recognition is the process of identifying individuals based on the unique features of the human iris. The iris's features can be identified by using either regular or infrared light.

The main visible characteristics of the iris are:

- the trabecular meshwork, which is the tissue that gives the appearance of dividing the iris in a radial fashion
- rings
- furrows
- freckles
- corona.

Iris recognition technology has been developed to convert these visible characteristics into a template for future identification purposes.

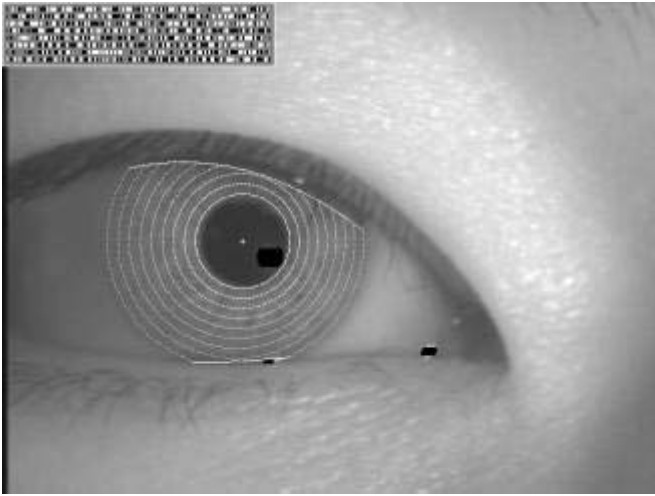
Iris recognition technology is commonly regarded as having in excess of 150 'degrees of freedom', as opposed to 13-60 for traditional biometric. The higher the number of 'degrees of freedom', the greater the accuracy of that particular biometric test. Accordingly iris scanning is a comparatively accurate form of identification when compared to other biometric tests such as finger printing. Further, iris-scan technology is capable of matching over 500,000 templates per second making it a more efficient means of identification.

#### **5.1.2.1 Iris Scan Process**

The first step is location of the iris by a dedicated camera no more than 3 feet from the eye. After the camera situates the eye, the algorithm narrows in from the right and left of the iris to locate its outer edge. This horizontal approach accounts for obstruction caused by the eyelids. It simultaneously locates the inner edge of the iris (at the pupil), excluding the lower 90° because of inherent moisture and lighting issues.<sup>31</sup>

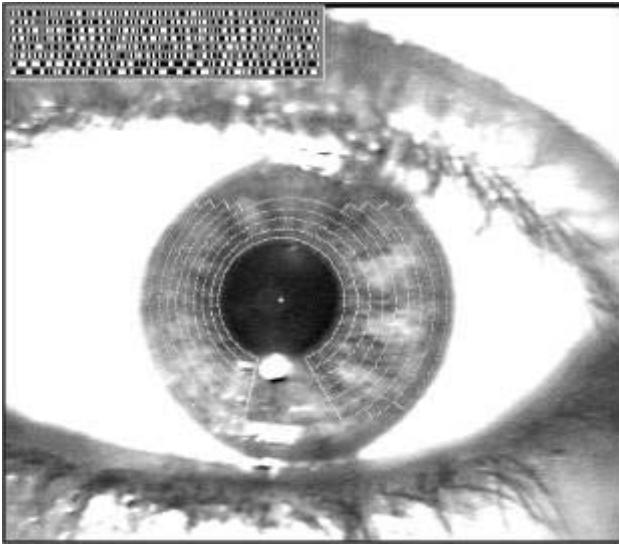
---

<sup>31</sup> Ibid.



**Figure 6 - Iris scan**

The monochrome camera uses both visible and infrared light. Upon location of the iris, as seen above, an algorithm uses 2-D Gabor wavelets to filter and map segments of the iris into hundreds of vectors (known as phasors). The wavelets of various sizes assign values drawn from the orientation and spatial frequency of select areas (referred to as the "what" of the image), along with the position of these areas (referred to as the "where"). The "what" and "where" are used to form the basis of the template. Not all of the iris is used: a portion of the top, as well as 45° of the bottom, are unused to account for eyelids and camera-light reflections (see Figure 7 below). Such iris scanning technology provides exceptional detail, well beyond that of pictorial or point-based representations. When utilizing templates for future identification, the database will not be comparing images of irises, but rather hexadecimal representations of data returned by wavelet filtering and mapping.



**Figure 7 - Iris scan**

#### **5.1.2.2 Iris Recognition and Payment Security**

Iris recognition technology requires reasonably controlled and cooperative user interaction. The subject must first submit to having their iris scan stored in a database, and then each time it is relied on to gain access, the subject must hold still to enable the match to take place. Users may initially struggle with the process, but as iris scanning becomes more main-stream, user resistance will decline.

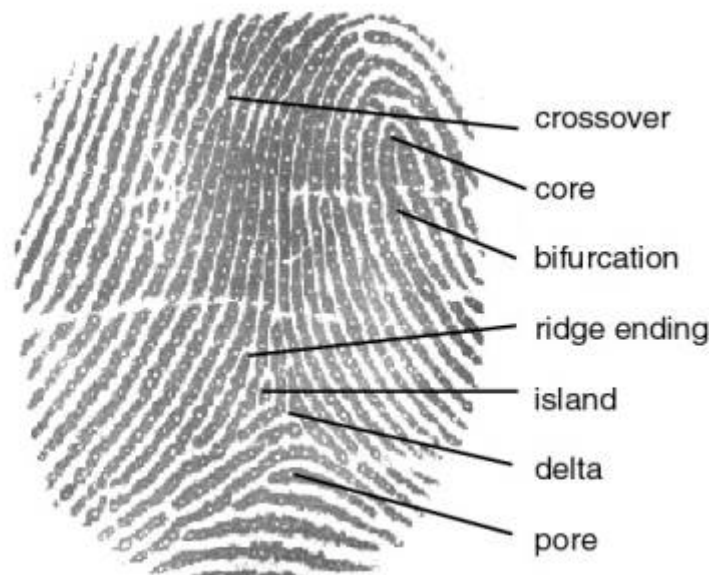
The main concern with using iris scan technology at this stage of development is that the claimed accuracy of identification using iris scanning is based on ideal iris images. In a real-world situation, such as scanning to gain access to bank accounts, subjects will not be in laboratory-type environments thus impacting on the accuracy of the iris scan.

### 5.1.3 Fingerprint Recognition

The human fingerprint is comprised of various types of ridge patterns. Fingerprints are typically classified according to the Henry system which identifies the following:

- left loop
- right loop
- arch
- whorl
- tented arch.

The fingerprint below is an example of a right loop.



**Figure 8 - Fingerprint characteristics**

The characteristics that are used for fingerprint identification purposes include:

- ridge endings - the points at which a ridge stops
- bifurcations - the point at which one ridge divides into two
- dots - very small ridges

- islands - ridges slightly longer than dots, occupying a middle space between two temporarily divergent ridges
- ponds or lakes - empty spaces between two temporarily divergent ridges
- spurs - a notch protruding from a ridge
- bridges - small ridges joining two longer adjacent ridges
- crossovers - two ridges which cross each other.

The primary identification feature is however the core, which is the inner point, normally in the middle of the print, around which swirls, loops, or arches center.

#### **5.1.3.1 Fingerprint Process**

The steps, known as feature extraction, used to convert a fingerprint's features into a template are as follows:

To highlight the prominent features of the fingerprint, lighter areas of the image are discarded, and darker areas are made black. The ridges are then thinned, via a reduction in the number of pixels, to enable precise location of endings and bifurcations.

At this point, even a very precise image will have distortions and false characteristics that need to be filtered out. Failure to do so will obviously taint the matching process. For example, an algorithm may search the image and eliminate one of two adjacent characteristics, as the same characteristics are very rarely adjacent. Anomalies caused by scars, sweat, or dirt appear as false characteristics, so are also discarded.

The points at which a ridge ends, and the point where a bifurcation begins, are the most rudimentary characteristics of a fingerprint. In addition to using the location and angle of certain characteristics, they can also be classified by type and quality.

However, measuring quality may only introduce an unnecessary level of complication.

Once the template fingerprint exists, it is necessary for the subject to provide a sample of their own fingerprint against which the template can be tested. Some biometric devices require users to sweep their fingers across them while others require that users place their fingers on the sensors and hold them still until they are authenticated.

### **5.1.3.2 Fingerprinting and Payment Security**

To date, using fingerprint technology for identification purposes has been used primarily in crime investigation, but rarely in biometric authentication.

There are several options available in which fingerprint technology can be utilised to enhance payment security. The two key factors for user-acceptance of the technology are:

- the placement of the biometric sensor from an ergonomic standpoint; and
- the type of device that the user interacts with.

Examples of the devices that may be deployed using fingerprint technology for payment security include<sup>32</sup>:

#### **1. Desktop peripherals**

Desktop peripherals include biometrically-enabled mice and other handheld devices that computer users interact with when they operate a desktop computer. Because the standard size of desktop peripheral is typically small, the biometric sensor must also be small enough to fit on the device. However, the sensor's ability

---

<sup>32</sup> Ibid.

to acquire images effectively also diminishes as it is made small enough to fit on the peripheral devices.

## 2. Embedded desktop solutions

Embedded desktop solutions include biometrically-enabled keyboards and other primary components of computers that computer users interact with when they operate a desktop computer. Because the embedded desktop devices are larger than desktop peripherals, sensor size is not as significant a consideration. The sensors can be large enough to acquire images without compromising the ability of the device to operate effectively. Since desktop devices like keyboards are relatively cheap, the addition of an embedded sensor should not significantly increase its cost.

## 3. Embedded physical access solutions

Embedded physical access solutions include biometrically-enabled keypads and other devices that users interact with to gain access to restricted areas (eg opening doors). Because physical access solutions are often used to protect items of value and because making the device small typically isn't a concern, the sensors can be large enough to meet this security requirement. Several other factors, including the location of the device (indoors or outdoors), the type of client (military, government or commercial) and purpose of the device will also be important in determining how the embedded physical access solution is deployed.

## 4. Embedded wireless handheld solutions

Embedded wireless handheld solutions include biometrically-enabled cell phones and other mobile personal communication devices that require owner authentication to use. Like desktop peripherals, embedded wireless handheld solutions, wireless devices are small and, consequently, the biometric sensor must also be small enough to fit on the device. Similarly, the sensor's ability to acquire

images effectively diminishes as it is made small enough to fit on the wireless device.

## **5.2 Smart Cards**

Many industry analysts such as the American Bankers Association are proposing that the smart payment cards are finally poised to change the future of electronic payments. The smart card combines a secure portable payment platform with a selection of payment, financial, and non-financial applications. The smart card's reach potentially goes beyond that which we currently know as the debit and credit card model. Visa International believes in the very near future, consumer and business cardholders alike will be able to choose from a variety of smart card enabled, lifestyle-driven features which can be utilized with PCs, mobile phones, or other Web-enabled devices.

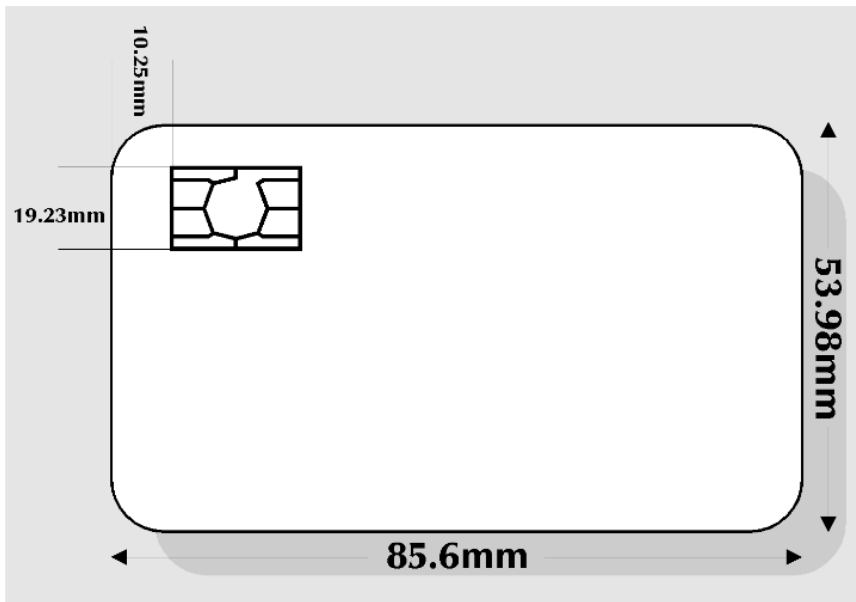
### **5.2.1 What is a Smartcard?**

The smart card is a widely used and ambiguous term. ISO uses the term Integrated Circuit Card (ICC) which includes all devices where an integrated circuit is contained within the card. The card is the same size as normal bank credit or debit card (85.6mm x 53.98mm x 0.76mm)

The cards themselves come in two main forms: contact and contactless. The contact card is more common and is easily identifiable by a gold connector plate.<sup>33</sup>

---

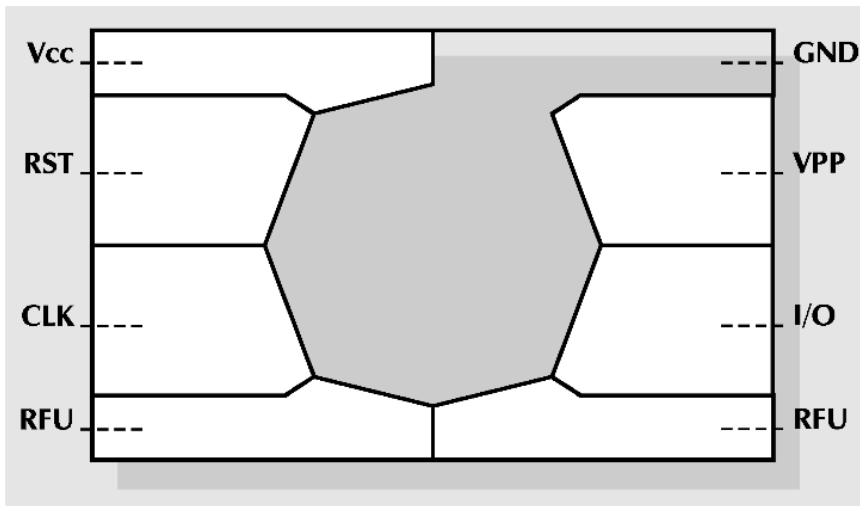
<sup>33</sup> <http://www.smartcard.co.uk/resources/articles/intro2sc.html>



**Figure 9 – Contact Smartcard**

In contrast the contactless card may contain its own battery, particularly in the case of the “super smart card” which has an integrated keyboard and LCD display. However generally speaking power is sourced by an inductive loop using low frequency electronic magnetic radiation.

As the name suggests, the contactless card utilizes technology to transfer data between the reader without physical contact. The main advantages of this type of card are that the contacts will not wear out and the contents are safer as static electricity cannot destroy the integrated circuit. However this card has more limited applications than the contact card.



**Figure 10 – Points on a Contact Smartcard**

As the figure illustrates the contact card has 8 point of contact however only 6 are actually used to communicate with the outside world. The Vcc would usually run at 5 Volts but now with advances in semiconductor technology is more likely to run at 3 Volts or less which also allows lower current levels. Reset is the signal line that is used to initiate the state of the integrated circuit after power on. The clock speeds run at 3.57 MHz and 4.92 MHz which aligns them with colour television sub carrier frequencies of NTSC and PAL. These frequencies are chosen because of the availability of cheap crystals to form the clock oscillator circuits. The Vpp is used for the high voltage signal necessary for programming the EPROM. Lastly the serial input/output connector is used for interchanging data between the reader and the card.

The chip itself is primarily used as portable storage memory usually using a combination of either ROM, PROM, EPROM, EEPROM and RAM. A typical storage capability of the card would usually be out 32K, which is about 80 times greater than the conventional magnetic strip.

The control logic used in smart cards is used for communication protocols but possibly more importantly it also offers some protection of the memory against fraudulent use. This allows the IC to offer a very tamper resistant domain for the card to operate in, even more so than some cryptographic processes. The security logic can be used to control access to the card's EEPROM memory and only persons who have the access codes have the ability to change the contents of this memory.<sup>34</sup>

The elimination of cash is seen as the holy grail for governments, internet merchants and financial institutions. Even though for years now there has been talk of a cashless society, a cashless society seems as far away as a paperless society.

Smart cards can be used as an electronic purse which can store a nominated cash value on the card. This can then be spent in the same way as cash, at participating retailers. This enables smaller payments (i.e. \$0.80) which would usually not be paid by credit/debit card to occur without the inconvenience of carrying cash.<sup>35</sup>

The benefits to consumers include:

- Convenience – easy access to services with multiple loading points
- Flexibility – high/low value payments with faster transaction times
- Increased security

The benefits to merchants include:

- Immediate/guaranteed cash flow
- Lower processing costs
- Operational convenience

---

<sup>34</sup> Ibid.

<sup>35</sup> Vishal P. 1997, "Smart Cards – The Smart Way for Banks to Go?", *The International Journal of Bank Marketing*, Vol.15 No.4, p 134-139

To date, single-function, generic e-purse cards, which have been released in various countries around the world have seen technical success but commercial catastrophe in terms of usage rates. 80+ million purse cards in Europe are used on average once every six weeks. Although the benefits of the cards are there for both consumer and merchants, numbers talk and this 30 year old technology is still struggling to become a viable option.

### **5.2.2 Risks of the Smart card**

We live in a fast-paced technology-driven world and although the smart card offers greater security and features than its magnetic strip counterpart, it does not offer increased security in identifying the user as the true owner of the card. It also opens the door to new fraud measures. If the digital encryption systems are discovered, fake cards can be produced, which the purchaser terminals would accept as genuine. The fraudster would also be able to produce cloned cards and devices with an interface emulating an integrated circuit contractor.<sup>36</sup>

Unfortunately another obstacle for the smart card is that different cards are usually not interchangeable. Memory cards would usually have different interface characteristics and data formats than microprocessor cards between the terminal and card. Even where cards look similar, it is rare that interchangeability is possible.

However with a recognized standard and with the use of biometric identification stored on the actual card itself, a commercially viable evolution in payments could be possible.

---

<sup>36</sup> Chinn R and Wendel C. 2001, "Comments: Strategy, Structural Flaws Are Stifling Smart Cards", *American Banker*, Vol. 166 No. 41, p 9.

### 5.3 Proximity Payments

Convenience, flexibility and security are keys for the successful implementation of a new payments system. According to American Express, several wireless technologies have potential as new payment methods, but the one most likely to succeed is radio frequency.

In a speech at the Ninth Annual Financial Services Technology Forum: Online 2003, Mr David Bonelle (vice president of Amex's advanced payments enterprise development group) detailed why he thought radio frequency payments would take off and other technologies such as Wi-Fi, Bluetooth, infra-red and cellular-based payments would not. Most major card companies including Amex, Mastercard and Visa are backing it through an established standard, ISO1443.<sup>37</sup>

Currently tests are being done at Amex's New York cafeteria and on consumers in the Phoenix area. The device itself is a small piece of plastic, which fits on to a key chain. The card is designed for small purchases such as snacks sold at convenience stores and has a \$150 a day payment limit. Currently 230 local merchants are trialing the technology. The transaction works just like a normal card purchase but instead of taking an average of 15.3 seconds for normal PIN based transactions, it takes only 8.9 seconds.<sup>38</sup>

Although Mr Bonelle was dubious about infrared and cellular based technologies, Visa International is pursuing both. With infrared technology there has to be a direct line of sight between the device and the payment terminal. Whereas radio frequency uses short-wave radio technology to pass data from the card to the terminal and, unlike infrared, it can pass through material. Even though this is more convenient than pulling out your mobile and keying the appropriate codes,

---

<sup>37</sup> Scottsdale, A. 2003, "Radio frequency makes noise in payments biz", *American Banker*, September 2003, p 18.

<sup>38</sup> Ibid.

infrared is seen as more secure as radio waves travel in a 360 degree field, allowing easier capture by criminals.<sup>39</sup>

At the time of writing, Radio Frequency Identification (RFID) and payments have been experiencing a lot of controversy. Privacy groups have been expressing very negative opinions about the surveillance possibilities the chips will bring.<sup>40</sup> I believe that the social barrier of making this technology available and widespread will be greater than technical implementation of such devices.

---

<sup>39</sup> Anonymous, 2003, "Infrared proximity payments", *The Nilson Report*, January, p 1.

<sup>40</sup> London, S. 2003, "An eye on the shopping trolley", *Financial Times (London)*, October 1, p 13.

## Chapter 6 - Revolutionary Ideas in Payments

### 6.1 Dual-Currency Systems

In recent decades, there has been growth in dual-currency systems in countries all around the world. The two currencies generally consist of a national currency, which is also supplemented by a complementary currency.

Briefly, all contemporary national currencies are bank-debt created fiat currency. This means there is no commodity backing. Additionally, all conventional money is created through the fractional banking system, and as a consequence is debt-based. Finally, since the dollar-gold equivalence standard was repealed in 1971, there is no international standard of value anymore.<sup>41</sup>

On the other hand complementary currency is created for different purposes, meaning they abide and operate under very different rules.

#### 6.1.1 What are Complementary Currencies?

Complementary currencies are agreements within communities to use another sort of exchange for goods and services within that community. Complementary currencies do not eliminate the need for a national monetary system but rather complements the existing one to provide greater liquidity. Their main aim is not for savings or investment but rather to facilitate transactions.

Currently there are known to be over 5,000 complementary currencies operational around the world. In the developed world, the WIR in Switzerland has been in operation since the 1930s and examples in Japan date back to the 1950s. This

---

<sup>41</sup> Bernard Lietaer, Co-architect of the Euro

type of currency has experienced exponential growth in the last 5 years, especially in Japan, Australia and continental Europe.

### **6.1.2 How are Complementary Currencies different from Conventional Money?**

Currently the most well known complementary currency systems are loyalty programs. Frequent Flyer points started as a marketing gimmick, but today you can use your British Airways frequent flyer points to purchase goods from Sainsbury's, the country's largest supermarket chain.

Complementary currencies are typically not designed with a "store of value" function so they are not typically associated with savings. Several of these systems use a demurrage charge, which is similar to a parking fee, which ensures the currency is always circulating and not hoarded. A well designed system will not create inflation and the system remains transparent for all who use it.

### **6.1.3 Example of How Dual Currency Systems Work**

In 1932, during the middle of the great depression, the town of Wörgl in Austria made economic history by introducing a dual-currency system. The town at the time was in a critical economic position. Of its 4,500 people, 1,500 were without a job and 200 families were penniless and they were prepared to try anything.

Michael Unterguggenberger, the mayor of Wörgl, had a long lists of works that the town needed to accomplish, however the financial position made it nearly impossible. Projects needing to be done included repaving the roads, street

lighting, extending water distribution across the town and planting trees along the street.

Instead of starting these projects with the 40,000 Austrian schillings in the town's coffers, he decided to deposit them into a local savings bank to guarantee the issuing of a complementary currency known as "stamp scrip". This required a stamp to be stuck on all the circulating notes every month for them to remain valid, the stamp amounted to 1% of each note's value. The money from this was used to run a soup kitchen that could feed 220 families.

As nobody wanted to pay the 1% hoarding fee, everyone who received the notes spent them as fast as possible. The 40,000 schilling deposit enabled anyone who wanted to exchange the scrip could so but for only 98% of its value in schillings. This offer was rarely executed by any of the people in Wörgl.

Only the railway station and post office refused to accept the local currency. As locals started to spend more money locally, they made more money and when people ran out of ideas for spending the money, they were paying their taxes early which resulted in a two fold increase in town revenue.

Over the 13 month period during which the dual currency ran, Wörgl not only completed all necessary works projects but was also able to build new houses, a reservoir, a ski jump, and a bridge. The people also used scrip to replant forests, in anticipation of the future cash flow they would receive from the trees.

As towns learnt of the success in Wörgl, they too started to implement similar systems. Central Bankers in Austria began to panic and created laws making it illegal to create such currencies.

## 6.2 Attention Economy

The economies of first world nations have shifted dramatically over the last thirty years. No longer are the core of industries in production, transportation, and distribution of material goods, but primarily income is now generated through managing our dealings in information of some sought. This is colloquially known as the "information economy".

However, by definition, economics is defined as the study of how society uses its scarce resources and we all know that information these days is anything but scarce. We are almost in information overload, yet we are constantly increasing our generation of it. What is scarce is the ability to draw someone's attention to a particular piece of information. In any one day, a person can only devote a certain amount of time or attention to a particular article, web site or advertisement. Therefore more realistically you could call it the "attention economy".

If you look at information, it can be measured in bytes and baud rates. Attention is far more complex - it is a process that occurs in the mind. Take the scenario of surfing the internet. You usually know what you are looking for, but you are being constantly bombarded with pop-ups trying to take your attention towards other sites. Your mobile telephone then rings, you check who is calling you and decide if you want to direct your attention to that person at that moment or call them back.

Thomas Mandel and Gerard Van der Leun in their 1996 book *Rules of the Net* wrote that "attention is the hard currency of cyberspace." In my opinion this is spot on. I believe that the flow of money (not fraudulent) on the internet is equivalent to the flow of attention and one day may replace it all together.

This is obviously a peculiar concept at first, however conceptually it makes perfect sense. Attention is one of mankind's most primal desires. Without it, most of us would not be able to function. Although some want more attention than others, we

all crave it. However not all attention is the same. Some of us want to be recognized as a TV star and some of us like the work we do and the feeling of appreciation from others that stems from that.

Attention is one of our only very limited resources, but how can it dominate the economy? From a traditional economist's point of view, material products are scarce and always will be. However in reality, this is not how first world societies live. Mass production has enabled abundance like at no other time in history. As an example of this, one of Australia's biggest industries is now the "dieting industry". Food has become so plentiful that eating too much is now more of a concern than not having enough.

However attention is different, it is scarce and is strictly limited. No matter how brilliant you are at multitasking, your true focus of attention can really only be on one thing at a time.

But how does this relate to money? If you look at advertising, you pay for an ad for which there are no guarantees that an audience will take notice. Many audiences learn to switch off during advertisements except the more interesting ads, but even then may not focus on the product or service itself. However the ads that do attract the most attention will also have the best chance at being successful. In an attention economy this will be how we transact.

This trend of rewarding attention is fast becoming commonplace in our society. If you take the example of a sports star, or an entertainer, they attract a lot of attention and are paid accordingly. But recently we have started to see a dramatic increase in the level of remuneration of professionals. For example a CEO is very much more an attention-getting motivator compared to being an actual boss these days and they are now paid relatively more money than at any other time. Whereas on the other hand fast-food servers and cleaners who do not grab the public's attention have found their relative financial standing eroding.

This might all sound very outlandish, but to bring it in to perspective I would like to raise the following points. As you have already read, cyberspace is prone to fraud when used for the electronic transfer of funds and it would seem the ways of protecting these transactions are reactive and are therefore one step behind the criminals.

History also offers a parallel for understanding major shifts in our thinking of how wealth is created and sustained. At the height of the feudal order in Europe, everyone had taken for granted that working the land would always be the primary way to generate wealth. Possessing the right bloodlines (which cannot be sold) was how property at the time was transferred and neither the serfs nor lords could ever see this changing. Yet as the industrial revolution took hold, and food production became just another industry and not even a highly important one, there was a major shift of wealth to entrepreneurs who capitalized on the industries of the industrial revolution.

However if attention is to replace money as we know it, what will we use to purchase material goods? How can attention get you a new car? How will a company like General Motors give you enough attention to build a car for you. If you were to actually look at the car itself most of the cost is involved with the development of the car and materials used. In the future we are likely to see increasing development in the automation.

If you consider most people involved in this process would be connected to each other through cyberspace. It is not that foreign to foresee a time when corporations as we know them disappear and at that time it will make a lot more sense to speak of a complex car making community, made up mostly of entourages surrounding thousands of stars and smaller stars. As is common among entourages, much participation would be less than full time, and the

majority of members would belong to other communities as well, and even to other entourages.<sup>42</sup>

Making people in the car community who may or may not belong to other communities, able to trade in their attention for goods and services that someone else can provide them.

---

<sup>42</sup> <http://www.wired.com/wired/current.html>

## **Chapter 7 – Conclusion and Future Recommended Work**

Fraud is definitely the weak link for an otherwise extremely convenient method of transferring funds for goods and services. Credit card usage has experienced double-digit growth every year in the last, so it is in consumer and industry interest's to ensure its longevity. As discussed to date, electronic payment security has missed out on a lot of technical innovation improvements seen in other industries. But as levels of fraud continue to increase, so too will the cost to the consumer. If this problem is not addressed, credit cards and electronic payments may become an unviable option for consumers.

I believe some of the solutions offered are on the right track of easing fraud as shown by the US grocery chain study, however this must be coupled with affordability. Currently the start-up costs for these type of system are quite high and therefore do not offer a financially sound solution for smaller businesses. Over time I believe the costs for such systems will significantly reduce enabling biometrics and or radio frequency identification to form the backbone of electronic payment security.

Although unlikely, I believe any move made to improve credit card security would best be introduced via a collaborative project undertaken by all the major credit card companies. One of the major strengths of the current system is its overall generic nature, allowing businesses to accept all major cards, whilst utilizing the one piece of technology. However, any major improvements in credit card security are most likely going to result in an increased competitive advantage for the company which introduces it. Hence a collaborative project between these companies may be unlikely outcome.

To take this knowledge base forward I would like to see more research addressing short to medium term security improvements through biometrics, smart cards and

RFID, with a longer term look at how systems like dual-currency systems and “attention economies” can shape the next wave of paying for goods and services.

## References

Alexander, M. 2003, "Web fraud undetected? Not for long", *USBanker*, June 2003

Anonymous, 2003, "ATM-users say they would welcome biometric efforts", *Credit Union Journal*, June 2

Anonymous, 2003, "Australian police close 'ghost' bank sites, make some arrests in ongoing investigation", *BNA's Banking Report*, September 2003

Anonymous, 2003, "Infrared proximity payments", *The Nilson Report*, January

Anonymous, 2003, "Proceed with caution; Technologists must become aware of the privacy issues raised by RFID", *eWeek*, September 2003

Bankston, K. 2001, "Biometrics: toys or tools?", *Credit Union Journal*, January

Bellis M. 2003, "The History of Money and Credit Cards",  
<http://inventors.about.com/library/inventors/blmoney.htm>

Blank, C. 2002, "At Grocery Checkout, No Wallet Needed", *New York Times*, 25 July, Late Edition (East Coast)

Breitkopf, D. 2003, "ATM makers tout new fraud-fighting features", *American Banker*, June 10

Chinn R and Wendel C. 2001, "Comments: Strategy, Structural Flaws Are Stifling Smart Cards", *American Banker*, Vol. 166 No. 41

Clayton, H. 2003, "Hole-in-the-wallet machines", *Financial Times (London)*, August 2

Costanzo, C. 2003, "No bulletproof shield against new e-scams", *American Banker*, October 2003

Davenport, T. 2003, "FTC: ID theft costs \$50 billion", *American Banker*, September 2003

Goldhaber, M. 1997, "Attention Shoppers! The currency of the future won't be money, but attention", *The Conde Nast Publications*, December 1997

[http://www.biometricgroup.com/reports/public/reports\\_iris-scan.html](http://www.biometricgroup.com/reports/public/reports_iris-scan.html)

<http://www.computerworld.com>

<http://www.wired.com/wired/current.html>

Jones, C. 2003, "Millions swiped by credit crooks", *The Courier Mail*, June 13

Lee, J. 2003, "Identity Theft Victimized Millions, Costs Billions", *New York Times*, September 2003

London, S. 2003, "An eye on the shopping trolley", *Financial Times (London)*, October 1

Marshall, R. 2002, "Prepare for paperless payments", *Financial Times*, December 20

Potomac, 2003, "Fighting the phantom menace: Junk e-mail linked to identity theft and fraud", *Card News*, May 2003

Punch, L. 2003, "A problem yet to be solved", *Credit Card Management*, April 2003

Punch, L. 2003, "Fraud-control tug of war", *Credit Card Management*, June 2003

Simpson, B. 2003, "Throwing out the good with the bad", *Credit Card Management*, July 2003

Scottsdale, A. 2003, "Radio frequency makes noise in payments biz", *American Banker*, September 2003

Snel, R. 1999, "On-line banking: Factors found to affect accuracy of biometric identification systems", *American Banker*, April 1

Tedeschi, T. 2002, "Retail Executives are Uniting to Fight Credit-Card Fraud in the Online-Bazaar", *New York Times*, October 21

Vishal P. 1997, "Smart Cards – The Smart Way for Banks to Go?", *The International Journal of Bank Marketing*, Vol.15 No.4

Wade, W. 2003, "Con artists stealing data via phony bank sites", *American Banker*, June 2003