Dissertation

Credit/Debit/Cash Card Fraud and Abuse - an Outlook on Prevention and possible Value added

By
Achim Hartmann

A: EXECUTIVE SUMMARY

The plastic payment card market has had tremendous growth over the last decade and there are by now 97 million payment cards in circulation in the UK only, with a predicted 130 million cards by the year 2000. As the industry life cycle comes into its mature stage competition becomes fiercer and consumer bargaining power is growing. Possible sources of value added have been mostly exploited. However, one of the less exploited sources of value added is the security aspect of plastic money.

There are a number of different card types and every one has its advantages and its disadvantages. Cards can be divided into categories by its technical features („smart card" or magnetic stripe card) and by the way the issuer charges the account (charge-, credit-, and debit-card).

Regardless of the type of card, the payment circle remains the same. It consists of the issuer of the card, the cardholder, the merchant and the acquirer. Most fraud occurs at the point of sale (POS) but the merchants cover only one third of the damage whereas the issuers cover the remaining two thirds. This puts the issuers on the receiving end of fraud. It is therefore not surprising that a perfect creditworthiness is a condition to posses a payment card. This is the reason why only 20 million citizens in the entire UK have a payment card. This situation is unlikely to change if the security standard remains at the current level since fraud is increasing again after a decrease some years ago.

In order to combat fraud effectively current technologies have to be developed further and new technologies have to be implemented. Magnetic stripes, encryption and hot card file verification are examples of the first and smart cards and biometric verification are

examples of the latter. There are a number of typical „attack" patterns and corresponding counter measures but so far security systems can not guarantee a 100% security.

If any one issuer is to build a sustainable competitive advantage, the security aspect offers itself for further exploitation. Not only is it a good method to decrease losses due to fraud but it is also a valuable marketing tool as empirical evidence shows. The leader in terms of security has therefore a big advantage in establishing a cost leadership and in differentiating himself form his competitors. But at the moment banks and other issuers hesitate to implement innovative solutions to battle fraud although some countries have shown a high readiness for the introduction of new methods (South Africa, Czech Republic and Russia). Furthermore have there been first attempts to establish future standards for new technologies by many countries e.g. UK and EC. Traditionally banks have been cautious about admitting losses due to fraud in order to avoid damaging their image but even the banks' annual reports are mentioning the problem by now. This indicates that the future development will be one towards innovation and fraud detection and prevention.

B: CONTENTS

B1: STRUCTURE

REMARK: FOOTNOTES ARE GIVEN AT THE BOTTOM OF THE PAGE AND ARE SOMETIMES ON THE NEXT PAGE

B2: FIGURES AND TABLES

C: RESEARCH METHODOLOGY AND INTRODUCTION

The research for this dissertation has been done for the most part in accordance with the research proposal[1]. Both primary and secondary research have been extensively used. The City Business Library in Moorgate has proved to be a solid platform to work form. A good proportion of the bibliography has its roots directly or indirectly in the City Business Library. This includes not only secondary research but also primary research. CardClear for example was a primary research target as a result of research made on the FT databases of the last three years.

Personal contacts have helped to conduct primary research and to get hints about secondary research. This includes Mr Wieslaw Bicz, the C.E.O. of Optel a biometric device producer (ultrasonic fingerprint scanner) on the one hand and Mr Samy Forbin the head of IT and electronic security at CIC, France's third largest bank on the other hand. But there are plenty of other sources available if one knows no relevant persons. Most biometric device producers have a web-site and with some fantasy they are easy to find e.g. www.fingerprint.com. Banks on the other hand have been reluctant to give out figures and even Samy Forbin claimed to ignore the amount lost due to fraud. What they have given out are numbers of market shares, number of branches, number of ATMs etc.

After knowing roughly what information would be needed for the report it proved very useful to design and distribute a questionnaire that established the missing parts of the research[2]. The questionnaire was distributed to 59 people of which many were friends. The acquisition of information in the streets proved unexpectedly difficult with many people

being reluctant to answer the questionnaire properly. The reason was probably the delicate topic provoking people's suspicions and the technical nature of the topic leading to misunderstandings despite the extreme simplification of the topic e.g. many people did not understand the question: Does any of your cards have a microchip on it? As a result some questionnaires were of no use because they were too incomplete or impossible to interpret e.g. ticking Yes and No for the same question. This lead to a shrinkage and a distortion of the sample. Originally the acquisition of data in the streets was intended to be a quota sampling to even out the uneven distribution of social classes among personal contacts and friends who had filled in the questionnaire. The average age of the sample is now unfortunately only 27 years and 56% are students of which many go to private universities. The sample is therefore younger and wealthier than the average UK population. On the other hand this is not too bad since this social group represents the future generation of profitable clients and the vast majority has already some kind of payment card. They are a generation brought up during an IT and communication revolution and are much less afraid of technological innovation than the older generation. This group is definitely more likely to support the implementation of a new approach to security for payment cards then the rest of the population.

Part D of the dissertation describes the situation as it is at the moment whereas part E describes and critically evaluates the use of methods to improve the situation. Whereas part D is mostly based on acquired data part E is based on a more technical description and evaluation of the methods.

[1] Please refer to Appendix F for a copy of the research proposal

Part F finally, is based on data acquired through primary research and conclusions found with the help of well known academic models.

[2] Please refer to Appendix E for a copy of the questionnaire and a listing of its results

D: PLASTIC CARDS AS MEANS OF PAYMENT AND RELATED SECURITY ISSUES.

D1: THE PLASTIC CARD MARKET

The industry has come up with three basic variants of plastic cards if used as means of payment: the charge-card, the credit-card and the debit-card. On a charge-card all the bills are accumulating on the card account. They are regularly settled, normally once a month. This gives the client a minor discount since goods and services can be bought and paid for later.

The classic credit-card usually has a limited credit. The client can settle the account at the regular paying intervals or he can pay by instalments. If he chooses to pay by instalments he has to pay interest which is normally higher than the interest of a current account. The minimum amount payable is only around 5%-10%. Therefore, this card tempts clients to make debts. However, most clients are using their credit card as a charge-card.

The debit-card is not a credit-card in its original sense, because it does not involve any credits since any purchase is directly credited on the client's account. The credit limit is the agreed account overdraft.

There are many more cards that allow for some kind of payment but they will not be given further consideration. Cash cards however will be mentioned at a later stage of the report.

It is difficult to recommend one card in particular since the needs of every individual are different. The issuing institutes have tried in the past to come up with innovative ideas in

order to satisfy customer needs. Nowadays a credit-card comes mostly with a package of special services and different kinds of insurances. But their usefulness is sometimes questionable. In a survey conducted by FINANZtest (6/95) only six out of 1200 credit-card users have used an insurance being part of the credit-card service package. An example of one of these exotic insurances is an air travel luggage delay insurance whereas claims can only be made if the flight ticket has been paid with the corresponding credit card.

With 73 card issuers in the UK alone, competition is fierce and customer bargaining power is high. Issuers have tried to differentiate themselves from competitors through offering special services to their card holders in order to gain a competitive advantage. But those services have mostly been easy to copy and have therefore not been able to help any of the issuers to build a competitive advantage. Furthermore has the industry achieved such a high market penetration that it has become virtually impossible to attract new customers without taking them away from a competitor. The industry is therefore in its mature stage. Consolidation is taking place and critical size is crucial. Collaboration and strategic alliances are found throughout the industry. Table 1 demonstrates the size of the plastic card market as means of payment.

As table 1 shows, the global amount of cards in circulation is now more than one billion cards. However, this amount of cards is held by a very small minority of the world's population. The main reason for that is the missing financial infrastructure in vast parts of the globe and the lack of creditworthy customers.

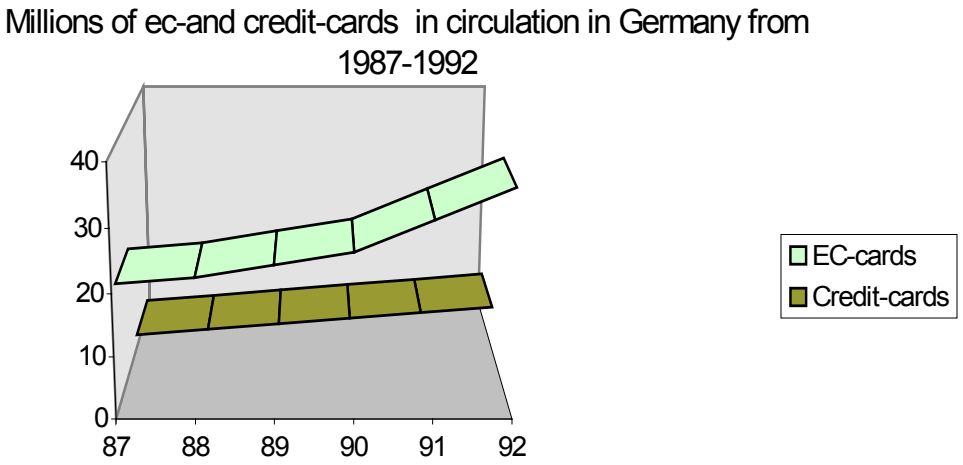
Table 1[3]:

Credit-card market				
	Card holders		Points of sale	
	Europe	Global	Europe	Global
American Express	N/A	41.5m (12/96)	N/A	4.5m (12/96)
Diners Club	2.5m (6/97)	7.6m (6/97)	1.3m (6/97)	3.6m (6/97)
Eurocard/MasterCard	34m (12/96)	435.1m (12/96)	3m (12/96)	13m (12/96)
JCB	N/A	34.9m (12/96)	N/A	4.4m (12/96)
Visa	101m (3/97)	540m (3/97)	3.6m (3/97)	14m (3/97)

[3] Taken from the German periodical: Geld on-line. 5/97. Heinz Heise Verlag GmbH. Page 134.

Figure 2 shows the fast growth of the market represented by the increase of ec-cards (Eurocheque guarantee cards) and credit cards in Germany between 1987 and 1992.

Figure 2[4]:



D2: THE DIFFERENT KINDS OF CARDS (PHYSICAL DISTINCTION)

In 1974 the at the time already well established magnetic card got concurrence from a newly developed and patented „Portable and independent system for the storage of data". This was the beginning of the smart card and marked an important step in the future

[4] Taken from the 3rd international Card Conference handout from 16 till 17 June 1993 in Hamburg

development of the plastic card. Roland Moreno, a French business journalist, is widely seen as the father of the smart card, although a patent for chip-cards was already given in 1970 in Japan.

Nowadays there are mainly two kinds of cards in circulation: the traditional cards with a magnetic stripe and the cards with an integrated circuit on them.

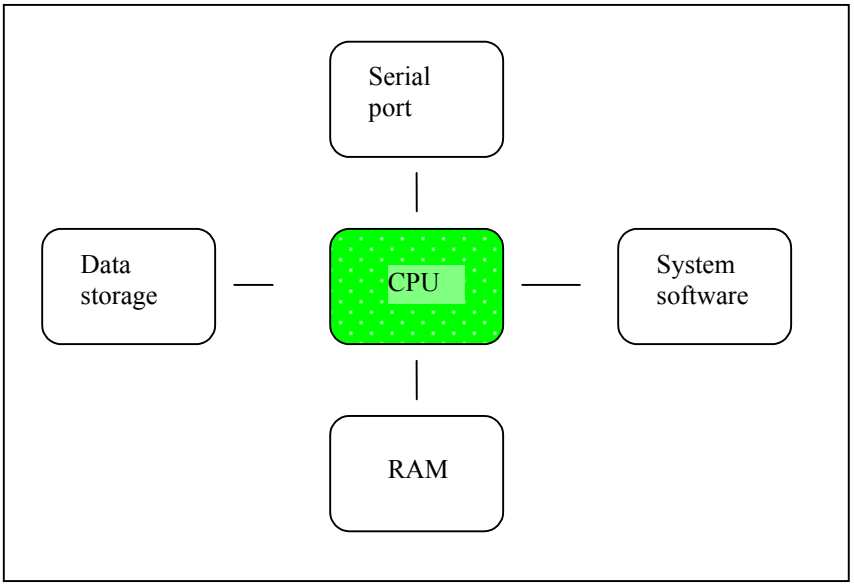
Cards with magnetic stripes are all very similar. It is by far the most frequently used method to store information on a card although the use of ICs on cards is rapidly increasing. This method offers a low price, fast and easy to program solution to store information on a card. The disadvantages, however, offset the advantages. First of all there is a very limited space for information on the card (just over 1kbit). Most cards have so called LOCO (Low Coercive Force) magnetic stripes in order to allow for changes of data e.g. changeable PIN. This leaves the card holder with a high risk of loosing data and facilitates the fraudulent distortion of data. Devices to read and write on magnetic stripes are widely available. Copying the data on the magnetic stripe it had before the maximum withdrawal was made can therefore reset a cash card with a daily withdrawal limit. This makes the abuse of cards much more profitable since an account can literally be plundered.

Due to the advanced technology used on chipcards there are different cards for different purposes out of which the most important ones will be examined.

The chipcard has two main distinctive hardware features: the kind of memory it uses and the way it communicates. The memory is either ROM (Read Only Memory), EPROM (Erasable Programmable ROM) or EEPROM (Electrically Erasable Programmable ROM). Most modern cards have EEPROM since the data on the card often needs to be changeable. The communication between the card and its environment can happen with the help of

contacts or without contacts. Most cards work with contacts for security reasons (avoidance of eavesdroppers). Every card with an IC has a CPU, a memory (RAM), a serial port, ROM (system software) and a storage for data (normally EEPROM). Figure 3[5] underneath visualises the basic structure of a one chip microprocessor:

Figure 3:



Depending on how these different elements are programmed and on what hardware is used it is possible to make out four major groups of cards:

1) A data storage card: reading and writing of data, no security functions.
2) An intelligent data storage card: contains protected areas (e.g. with the help of a PIN).
3) A multifunctional processor chip card: sophisticated security features, capable of working with algorithms.

[5] Taken from Wigan, Winfried; 1991. Die Karte mit dem Chip. Berlin: Siemens-Aktiengesellschaft.

4) Super Smart card: with integrated display and keyboard.

Cards used as means of payment fall within the third category and will be given further consideration in part E2 of the report.

In order to clarify the differences between a magnetic stripe card and a chipcard used as a debit card, table 4[6] might be helpful:

Table 4:

	Magnetic stripe card	Chipcard
Storage capacity	app. 1 kbit	8 kbit
Reserves	none	64 kbit
Security	in reading device	on the card
Encrypting data outflow	no	yes
Manipulation	easy	difficult
Price	low	high, but with a strong downward trend

[6] Taken from Wigan, Winfried; 1991. Die Karte mit dem Chip. Berlin: Siemens-Aktiengesellschaft.

Required investment in the system (network)	high	low
Verification	Trend towards on-line resulting in reliability problems, higher transaction costs, slower verification and costly systems.	Trend towards off-line
Signal transformation	magnetic-electronic	none
Data processing	impossible on card	possible on card

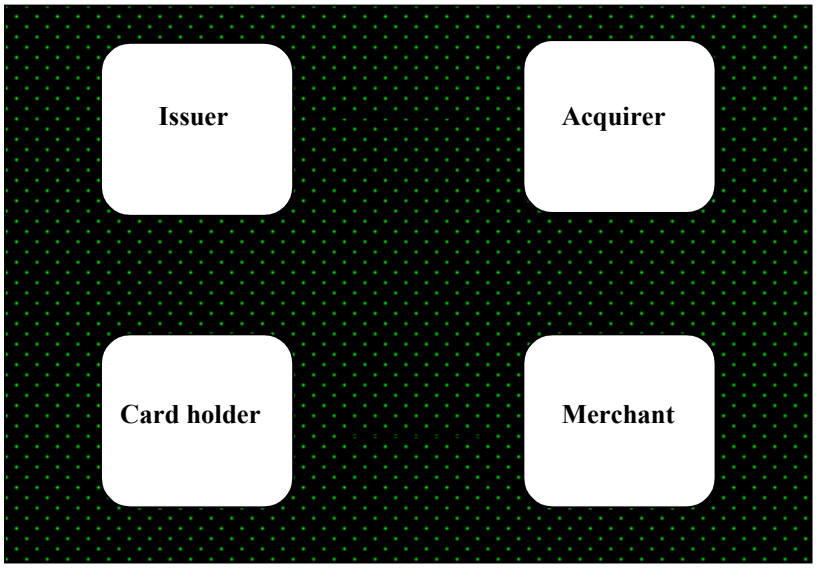
D3: THE VULNERABLE POINTS OF THE PAYMENT CIRCLE

The payment circle is an important mechanism in determining the way business is done with reference to the use of electronic money. Figure 5 gives an outline of the payment circle.

Figure 5[7]:

Issuer: there are 73 issuers in the UK. They range from banks over building societies to credit card companies.

Card Holders: there are at the moment 97 million cards in circulation in the UK at present. These cards are held by a minority of the UK population (around 20 million people). The predicted number for the year 2000 is 130 million cards.



Merchant: There are about 200,000 merchants who accept cards as means of payment in the UK.

Acquirer: there are six acquirers in the UK. Their function is to collect the transferred data and to ensure the smooth handling of the factoring process. Acquirers are all large issuers with the required resources to manage data intensive operations.

The payment circle is not the same in every country e.g. there are no acquirers in the United States.

The total damage that occurred in the UK due to the abuse of cards has been over £145 million last year. Two thirds of this amount was covered by the banks representing a cost of over £97. The remaining third has been covered by the merchants. But where has the majority of all fraud occurred? The vast majority of all fraud and abuse has occurred at the point of sale, the merchants. And still they only cover a third of all cost that occurred directly as a result of card abuse As figure 5 shows, issuers and merchants have no direct contact. But it is in the issuing institute's best interest to be generous with the payment of compensations. The example of the issuing institutes of the ec-card in Germany shows how a good reputation can be damaged through a tough policy on compensations. In an article from „Der Spiegel „[8], the policy of some German issuers is severely criticised for their attitude towards the payment of compensations. The bottom line of the issuers' policy was simply that the system was absolutely safe. Any payment claimed not to be received by the card holder was declared to be an attempt to mislead the issuer to enrich oneself. The other often heard argument was that the card must have been improperly handled (carrying the PIN in the wallet or giving it to friends) and that no responsibility can be taken by the issuer. This attitude often left fraud victims with personal losses of over DM 10,000 (£3,000). After repeated arrests of card fraud gangs it came out that many clients had told the truth about their miraculous payments and the issuers had to abandon their policy. There is no safe system after all and the issuers have to acknowledge it by paying compensations after a careful consideration, of course. This will often lead the issuer in the frustrating situation of not being sure about a client being a thief or a victim. This policy

[7] Taken from the prospectus of CardClear Plc

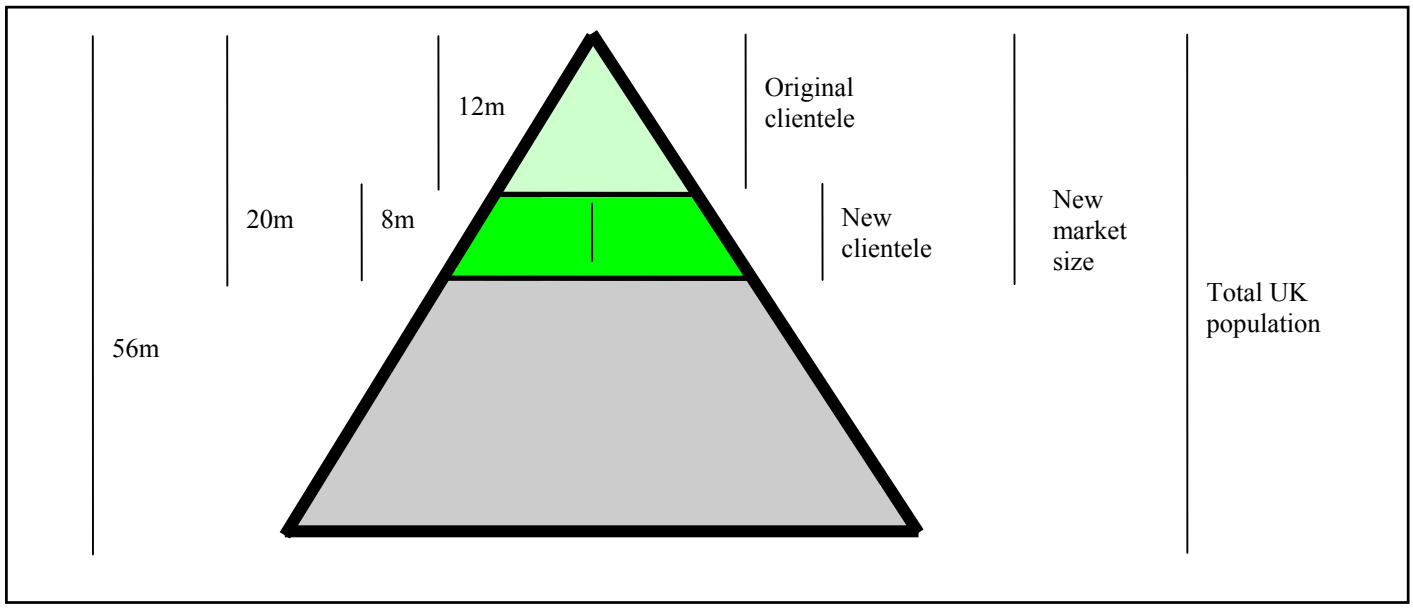
might tempt clients sometimes to behave deceitful, but a strict no refund policy is simply marketing suicide.

One of the reasons why most fraud is conducted at the points of sale is the existence of price floors. A price floor is a minimum price under which the card used to pay for the purchase will not be checked on-line (normally £50). Most purchases under fifty pounds are made in the retail sector. This sector is characterised by low margins. An on-line card verification costing normally 4p would depress margins further. Empirical evidence confirms these findings: 40% of all fraud in the UK is conducted in the retail sector. Out of the worst hit ten retailers, eight were petrol station chains which have a typical average purchase value of under fifty pounds.

A considerable obstacle for further growth is the high market penetration. The major problem, however, was that the 97 million cards were held by only 12 million people out of a total population of 56 million. This meant that the average card holder possessed already eight cards. The reason that only a minority of the total population was holding cards was the issuers judgement about credit worthiness. Finally the issuers decided to include poorer socio-economic classes in order to expand the market size. The total percentage of the UK population „allowed" to hold a debit or credit card was now around 40%, representing around 20 million customers (please refer to figure 6 for a visualisation).

[8] Der Spiegel. 11/86. Springer Verlag. Pages 88-101.

Figure 6:



This new clients included members of other socio-economic classes than only A[9] and were given debit cards such as Maestro or Cirrus. But since the admission of those new clients represented a risk of card abuse, it was decided that a zero floor limit would be introduced for this particular clientele. However, the admission of the new clientele has had commercial reasons but there are worries about its feasibility in terms of the prevention of card abuse.

For merchants who know the system it is easy to abuse credit and debit cards, hence the existence of criminal organisations who receive goods illegally, acquired through the use of stolen cards with merchants as their middlemen. However, this is a rare exception. Theft

[9] For a description of the socio-economic classes refer to Appendix A

of cards and abuse of confidential information happens in every step of the payment circle. But such leaks are difficult to eliminate and amount only to a minority of losses.

D4: THE INCREASE OF FRAUD

With the overwhelming success of plastic money, fraud and abuse have become a worry just as the counterfeit and theft of real money have always been. The facts are clear. As the number of cards in issue rises, so does the risk of fraud. As more cards are issued to more people making more purchases, fraud is likely to continue to increase and new types of fraud will emerge.

Figures 7 and 8[10] are showing the 1996 UK fraud profile and the UK bank losses from 1993 to 1997 with losses due to counterfeit shown separately.

Figure 7:

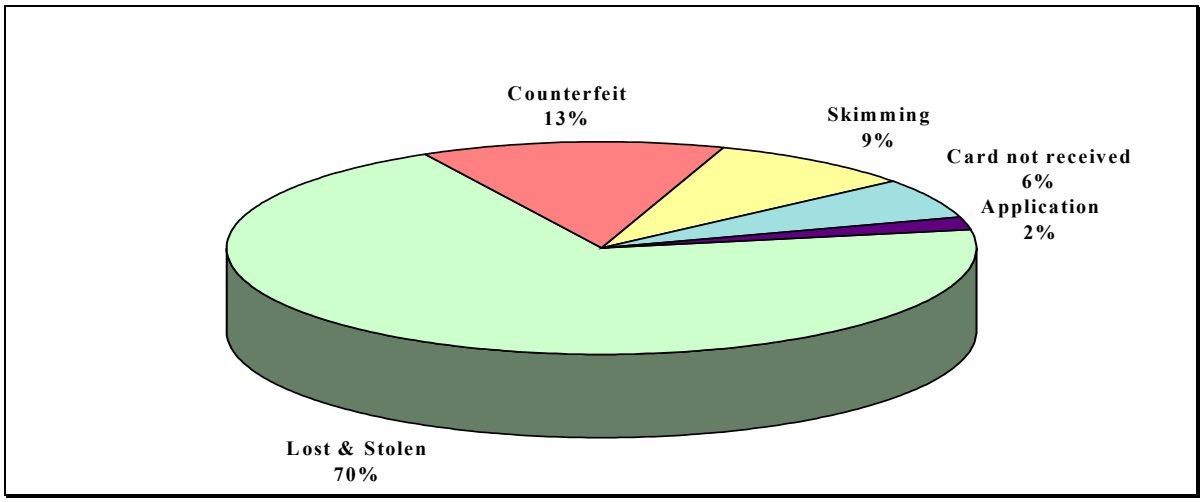


Figure 8:

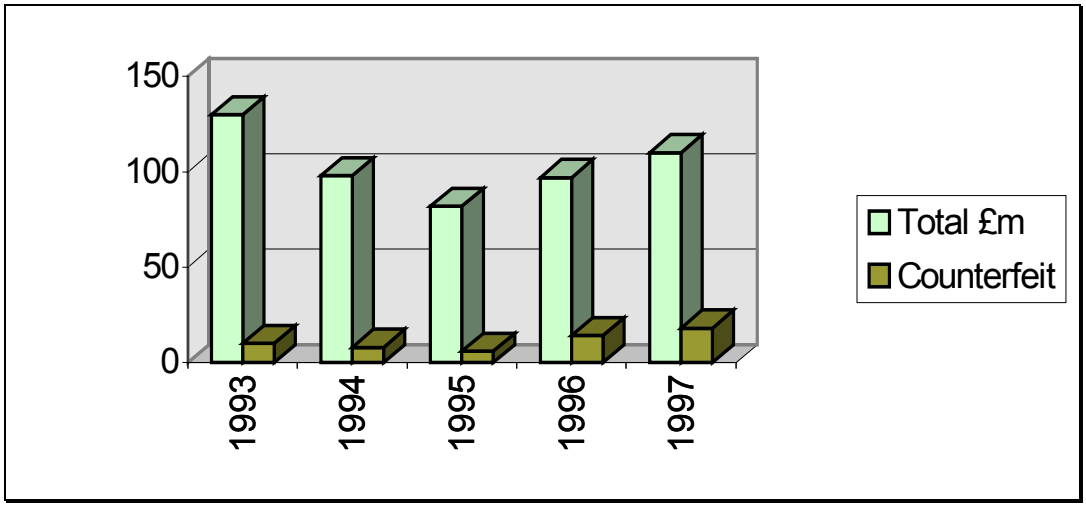


Figure 7 shows that lost & stolen cards still represent 70% of the fraud problem. What the figure does not show is that skimming (cloning of a card without the knowledge of the original owner) and counterfeit are increasing whereas the category lost & stolen is remaining at the same level. This is especially worrying as the Pre-status fraud (fraud that takes place before the card is reported stolen or lost) is already very high accounting for 45% of all fraud. A considerable proportion of this 45% are the six hours it takes to actively suspend a card after it has been reported stolen. It seems therefore a good idea to introduce chipcards (they are more difficult to reproduce) the way France did to fight the growing problem of counterfeit. France had a similar situation at the beginning of the 90's with an all time high fraud rate of 0.188 percent of total turnover and a total amount lost

[10] Copied from a report of CardClear Plc

the fraud rate and the fraud amount dropped considerably to 0.079% and $72m respectively. With reference to the acceptance of the program by cardholders and retailers, two surveys completed in December 1991 and 1993 pointed out a quite good acceptance of the newly introduced PIN check procedure by both and a level of technical incidents on the chipcards comparable to the level on magnetic cards. Nowadays the fraud rate is still falling whereas the fraud amount is again rising due to the increasing volumes of plastic money transactions.

Sales director Steve Callagham of CardClear Plc, a company that has specialised itself in card fraud detection and prevention, holds against that merchants in the UK were reluctant to adopt a change towards chipcards and that they were in general not worried about security issues. The UK is at the moment one of the only countries in Europe that has not introduced smart cards in the banking and financial sector. Other sectors on the other hand have adopted the standard already years ago e.g. telephone cards.

E: METHODS TO PREVENT THE INCREASING ABUSE OF PLASTIC CARDS

In order to discourage fraud and to decrease the losses suffered due to fraud, the industry has adopted certain standards that can be categorised. The following section of the report will critically evaluate the following methods of fraud prevention: magnetic stripes, micro chip cards, biometric methods, encryption and finally the verification with the help of hot card files.

E1: MAGNETIC STRIPES

A magnetic stripe is the most common method to store data on a card. Its advantages are the low price and the simplicity of customisation. On the other hand it is an ageing technology that has been stretched far beyond its original capacities. The major problem about this method is that it offers no security on the card itself because the card has no intelligence. This indicates that the PIN the user enters has to be verified by the machine that reads the card since the card itself can not compare the PIN it has on the magnetic stripe with the PIN the user enters. This again is the reason why cards with magnetic stripes tend to need an on-line verification which is slower and more expensive than an off-line verification.

The next problem is the simplicity of the manipulation of data stored on the stripe. Since most cards in use have LOCO stripes they are easy to read and copy. Hardware to read

magnetic cards is widely available and any PC is therefore relatively easy to convert into a universal magnetic card reading and writing terminal. Complete card readers are already available for £25.

So what about the PIN? The PIN as such is not on the card itself for reasons of security. So how does the card reading machine know the PIN that corresponds to the card it reads? The machine reads the data on the stripe and calculates the PIN with the help of a 64-Bit DES (Data encryption standard). The result is the four digit PIN. The DES is a highly sophisticated encryption method and the key to its 64-Bit version has to date not officially been figured out. But there have been repeated unconfirmed rumours about people having found the key. One of the more credible ones was told by „Der Spiegel[11]", Germany's most popular left-intellectual periodical. The story was that an information technology student managed to find the key to the 64-Bit DES after having worked on it for several months. This student was shortly after assigned to the board of IBM, which also happens to be a major producer of black box technologies used in ATMs. So far it has been confirmed that the key for the 56-Bit DES has been found and it seems only a matter of time until the corresponding 64-Bit key will be found. After a spectacular lawsuit in Germany, German banks have decided to use a 112-Bit-triple-DES key in the future to calculate the PIN.

The periodical Geld on-line[12] has also published a very critical article in May last year concerning the calculation of the PIN with the help of the DES. In this article Prof. Dr. Manfred Pausch a specialist in this area said that the nature of the key is such that there is an uneven distribution of digits. If one knows these irregularities and some further specialities of the system the odds for guessing the PIN right at the first time are 1:150.

[11] Der Spiegel. 11/1994. Springer Verlag. Page 81.

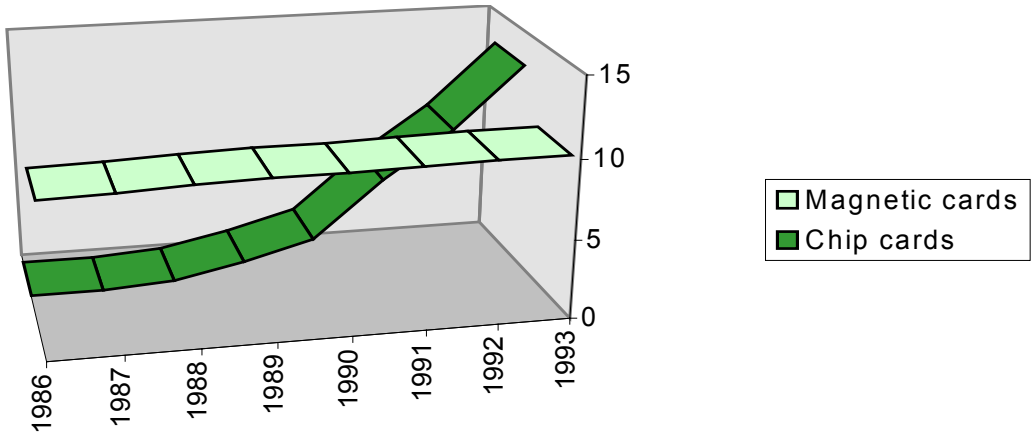
This contrast sharply with the statement of the banks that the odds for guessing the right key to calculate the PIN on the base of the data recorded on the stripe is 1:72,000 trillions. But there has also been one very positive development that could considerably improve the security of magnetic stripes. In 1994, two professors of the Washington University in St.Louis have patented a method to differentiate between an original and a copy. The basis of this principle is that every magnetic stripe has a unique magnetic micro pattern comparable to a magnetic finger print. After the two professors had made this observation, they developed a sensor that can read and identify the magnetic finger print of a card. This sensor can easily be integrated in existing systems and would make it possible to distinguish between a copy and the original since the magnetic fingerprint is impossible to copy. Combined with the application of other physical authenticity marks it is possible to establish an acceptable protection against counterfeit of magnetic cards. Unfortunately, the patent has not been put into practise on a large scale to date.

E2: MICROCHIPS

Cards with microchips have been on the march for the past decade in most countries. To show how the chip card has replaced the magnetic card consider figure 9[13] that has taken Germany as an example (millions of cards in circulation):

[12] Geld on-line. 5/97. Heinz Heine Verlag GmbH. Page 143.
[13] Taken from Wigand, Winfried; 1991. Die Karte mit dem Chip. Berlin: Siemens-Aktiengesellschaft.

Fig 9:



To gain an overview of its early history of development please refer to Appendix B. The basic structure and features of a smart card have already been outlined in part D2 of the report. In order to gain insight into a more detailed description of the chip's structure please refer to appendix C. This part will explain general security aspects with reference to the chip card and the supporting IT system in general.

The main advantage of a chip card is the fact that it is smart as opposed to a magnetic stripe card. Its microprocessor allows it to communicate with the outside world. This is the basis for an off-line verification being faster and cheaper than an on-line verification. When the user enters his PIN it will be tested against the PIN stored in the EEPROM. Therefore, only a simple system is needed to verify the accordance of the entered PIN with the PIN on the card. The chip does the hard work of encrypting and decrypting the data. But this vital advantage is only applicable to the verification process. In the whole verification process data is never easily accessible and manipulatable as opposed to magnetic cards. The security is therefore already in the card and not only in the machine as

already mentioned in table 4. The scarcity and high price of components, complete cards and equipment certainly help to prevent fraud as well.

Another strength of chips is its small size which makes it very difficult to reproduce it or even to find weak points in it. The chip industry has on top of that found many ways to construct a chip to make it very difficult for attackers to crack the chip. But all that has not made the chip fraud proof. Mr Wieslaw Bicz, C.E.O. of Optel, a Polish biometrics specialist has expressed worries that the structure of a microchip can be explored, leading to its eventual understanding and possibly to a correct interpretation of the data it contains. This worry has been confirmed in Geld on-line[14] where a cryptography student was said to have cracked a high security chip with features similar to those of smart cards. But not only is the physical security not fraud proof, the algorithms used in chip cards seem to be breakable as well. Mr Steve Callagham said in an interview that the keys to the algorithms used on the chip cards can be found on several Web-sites. This would make it easy to get the PIN of any chip card using the same encryption method.

Requests on spending limits, clearance of transactions and other bank details are the same for magnetic cards and chip cards because this is an outside information requirement. If a purchase goes on-line or not depends in that case on the price floor.

E3: TYPICAL FRAUD PATTERNS

There are a number of typical fraud methods and corresponding countermeasures used to prevent fraud from happening.

[14] Geld on-line. 5/97. Heinz Heine Verlag GmbH. Page 131.

- Taping of a line. The attacker has therefore accessed the connection between chip card and terminal or chip card and system. He can read all data that goes through that line but he can not change or intercept the data. This is called a passive attacker. The corresponding countermeasure is the encryption of the data flow. The attacker can than still read the data but it ha been rendered useless for him.
- Change of data during its transmission. In this case the attacker is active. He can change, manipulate, add or cut pieces out of the data flow. Encrypting the data makes it more difficult for the attacker to recognise the relevant parts to manipulate. Furthermore there is a so called MAC (Message authentication code) that enables the receiver to recognise changes in the message.
- Unauthorised access on data in the chip during the production and/or customisation process. The attacker want to access and manipulate now or later data on the chip. This again is an active attack. To protect the chip form internal attacks during its production and customisation, key hierarchies are used and security concepts based on it.
- Manipulation of the dialogue partner. The attacker pretends to be the dialogue partner. The best way to avoid that is to use a dynamic authentication in which the user demands verification of his dialogue partner. This does not work with a chip card since it does not have the required processing capacities.
- Reproduction of smart cards. It is assumed that the attacker already has the relevant data and a chip card to load it on. This is made impossible by establishing a write protection on the chip with the help of a producer's key. Before the customisation the key has to be entered like a PIN.

- Simulation of the card. If the data exchanged was always the same it would be sufficient to tap the line once and then replay the recorded data in order to simulate the card. By giving the security relevant data an accidental character this becomes impossible.

E4: ENCRYPTION

Originally encryption has served to protect data from being read by a third party which refers to a passive attack. However this situation has changed and data has nowadays to be protected against active attacks as well.

Encryption can be subdivided into two main categories: the symmetric algorithms and the asymmetric algorithms.

The oldest and the best known encryption method is the symmetric one. Symmetric means that he sender and the receiver use the same key to encrypt and decrypt the data transmission. The advantage of symmetric data encryption is the wide availability of good algorithms and its speed. The major disadvantage of it is the high effort needed for the administration of the keys since the number of different keys required for a growing number of network participants increases exponential after the formula: keys required = number of participants*((number of participants -1)/2)). A network consisting of 1,000 participants who all encrypt their data and all want to make sure that only the receiver can decrypt the message requires therefore already nearly half a million different keys. The earlier mentioned DES is an example for a symmetric algorithm. Another practical application of symmetric algorithms is the MAC (Message Authentication Code). In this case the message is once sent in its encrypted and once in its readable form. The receiver

then decrypts the message and checks if the two messages match. If they do, the receiver can be sure that the message has not been altered.

If asymmetric algorithms are used every participant has one private key and one public key. If A wants to sent an encrypted message to B, A has to encrypt the message with B's public key. Once the message has arrived at B he decrypts it with his private key. Of course, it is not possible to know B's private key by knowing B's public key which makes the encryption asymmetric. This avoids the need to keep the encrypting key secret since it is useless to decrypt. Furthermore are only two keys per participant needed, meaning that for a network consisting of 1,000 participants only 2,000 keys are required. The disadvantage of this method is its time requirement and the lack of commercially available algorithms. A typical application of the asymmetric encryption is the electronic signature. One can think of it as am asymmetric MAC. Whereas a transmission can only be checked for its authenticity with a MAC, a electronic signature makes it impossible for the receiver to fake it and the origin of the data transmission is therefore detectable. Applying symmetric and asymmetric encryption methods to the problems discussed in part E3 of the report helps to eliminate a large part of all fraud of data.

E5: BIOMETRIC METHODS

The days of the PIN are now surely numbered. What was a convenient, easy to implement method of controlling access has now reached the stage where it is also easy to defraud. Biometrics, where an individual's identity is verified by a unique physical or behavioural characteristic, looks set to become imminent successor to the PIN. By 1999 the world

market for biometrics for just physical access control applications is estimated to be worth US$ 100 million. Appendix D shows the market trends of biometrics.

As the movement of people around the world becomes quicker and easier, these travellers will expect to be able to access services from their home country, such as banking, with as much ease as they do whilst at home.

The PIN is the least secure of three levels of security. It is „something that you know", although in many cases it is something you have forgotten or written down to remember. The second stage is something that you have (e.g. a plastic card) which is possibly linked to something that you know. The third and ultimate tier is to use something which you are- biometrics- which can be linked to either something which you have, something you know or even both.

The problem with the PIN is that it is difficult to remember, especially if more than one needs to be remembered and they are chosen for the user. Paradoxically, if the user chooses their own PIN, they are very likely to choose something easy to guess such as the partner's birthday. When a password, or PIN is chosen for the user, the problem of having to remember it is sometimes overcome by writing it down. This, of course, defeats the point of having something which is something one person and only that person knows. One in three people write down their PIN for their bank card, according to a UK poll conducted by MORI. Another source estimates that nearly one in five people have been unable to get money out of an ATM at some point because they have been unable to remember their PIN. This and other behaviour patterns will be looked at in more detail in part F of the report.

Biometrics, too, have one significant drawback, however. Unlike in the case of a PIN or card, a computer can not give an absolute yes or no answer to whether the user is the one he pretends to be. A PIN is either 1234 or not and the same is true with card serial numbers etc. A dynamic signature, a voice, a face and many other biometric characteristics, will vary every time they are checked. In most cases it will not vary much but some leeway must be build in to allow the authorised user to produce a 99% accurate signature and still be verified. A biometric system, therefore, can not say with a 100% accuracy that the person in question is the right one. To combat this, biometric systems are designed to allow for a certain variance. The size of the variance depends on the purpose of the installation. In a financial installation it might be sufficient to require only 95% accuracy so that valued customers would not be falsely rejected but so that potential criminals would also be deterred. In a military establishment, an accuracy of 99.9999% may be needed to ensure that there is no possibility of an imposter being given access. This would, however, mean that authorised users may often be rejected by the system.

Before a person can be verified by a biometric verification device, they must first be enrolled. This is the process during which a new user must produce one or more samples of the characteristics to be used. These readings will then be compared and sorted to give one average reading or all the readings will be kept to indicate in what manner the user's characteristics can vary. This template is then stored in memory either in the individual verification terminal, on a plastic card or in a host system.

Different biometric types are better at ensuring a low rate of rejection of authorised users than are others. This also means, however, that they are not so good at rejecting unauthorised users. A trade off of one requirement against the other must be made. The

inaccuracy of a biometric system in rejecting authorised users is known as a Type 1 error and the corresponding inverse error is known as a Type 2 error. Whilst some systems come very close to zero on one of these, the other is usually correspondingly high. Other systems have a medium score on both. Another important factor is the memory size of the template. One biometric system requires only nine bytes of data which could be easily stored on a magnetic stripe card. Others require the data storage capabilities of a smart card or a host computer.

There are at the moment six different types of biometric systems commercially available. Fingerprint, hand geometry, retinal eye pattern, facial recognition, voice comparison and dynamic signature verification are now available from a wide range of suppliers. The following are descriptions concerning the way the devices work their reliability and their price range[15].

FINGERPRINT VERIFICATION: Fingerprint verification systems are heavily associated with law enforcement. On the side this is good, because it proves to the public that these systems work, but on the other side, the introduction of fingerprint verification may put some people off using it. The way fingerprint systems operate is by identifying the location of small marks, known as minutiae, which are found in the fingerprint. The readability of the fingerprint depends on a variety of work and environmental factors. These include age, gender, occupation and race. A young, female, Asian mineworker is seen as the most difficult subject. A system that works on the basis of ultra-sound can overcome these limitations.

[15] All numerical information is taken out of: Newham, Emma. 1995. The Biometrics Report. London: SJB Services

The system is user friendly and easy to use since all the user needs to do is to place his finger on a platen, sometimes positioned correctly by finger guides. The majority of fingerprint systems incorporate „live and well" detectors to ensure that the finger being scanned is connected to a live person.

Performance figures for one of the longest established fingerprint verification devices are quoted as having a false acceptance rate of 0.0001 % and a false rejection rate of less than 1%. Template size requirements differ between each supplier' system, ranging from 24 bytes and upwards of 1,000 bytes. The costs for a single fingerprint verification unit range from US$695 to US$3,000.

HAND-BASED VERIFICATION: Hand geometry systems have the advantage of a very small template: one system only requires nine bytes. Whilst many characteristics of the hand could be chosen for biometric verification, only two have so far been commercialised. One approach uses the geometry of the hand whereas the other uses the geometry of two fingers. These systems are relatively easy to use with some incorporating guide posts to ensure that the hand is placed correctly. Hand geometry has had no major problems being accepted in most societies except for Japan. The geometry systems are not affected by environmental factors such as dirt and grease although large rings need to be removed if not worn at the enrolment stage. Some systems will allow the user to use either hand, while others are easier with one hand but the other can be used on hand geometry systems if necessary. It is possible for the other hand to be placed upside instead because the geometry of each hand is a mirror image of the other hand.

Hand and finger geometry systems tend to be seen as good all rounders with one hand geometry system having a false acceptance rate of under 0.1%. The cost for a single hand

geometry unit is US$2100 whilst the components for a finger geometry system are US$900.

THE EYE: Of all biometrics commercially available, retinal scanning has the lowest false acceptance rate at an effective 0%. Retinal scanning operates by taking a circular image of the back of the eye using a very low intensity infrared camera. Using a retinal scanning device requires some practise and the use of an infrared beam has caused some public acceptability worries in the past. Iris scanning systems have also very good performance results. Because of its close links to the brain, the eye is one of the first parts of the body to decay after death, making the successful use of a dead or false eye unlikely.

The templates for both eye scanning verifications are comparatively small. The retinal scan template requires about a 100 bytes and the iris scan about 250 bytes. The systems cost around US$3,000 and US$6,000 respectively.

FACIAL RECOGNITION: People are already used to being recognised by their face, since this is the usual way of recognising a person. This indicates a high user friendliness. Systems currently available require the user to be standing straight on to the camera as if posing for a photo. Distance from the camera, background, facial expression, lighting, changes to hair styles and spectacles all effect some systems. Ultimately, facial recognition systems will be able to identify a person as they walk naturally towards a door.

An error rate of 2.5%is being quoted by one supplier for its mug-shot type system. The size of the template stored by facial recognition systems differs with each supplier but is relatively big. It ranges from five hundred bytes to 2,000 bytes. The cost for a facial recognition system is ranges from US$2,000 upwards.

VOICE VERIFICATION: Voice verification has the advantage that it is not intrusive and that people are used to using the equipment required. Two types of voice verification systems are available. Access can be controlled using a standard telephone linked to a voice verifier on a host computer. Stand-alone units are also available which perform verification internally.

The verification performance can be affected by background noise. This can occur when the user is situated in a busy location and also from electrical noise on the telephone network. Voice verification systems analyse the characteristics which produce speech and not its sound or pronunciation. This makes it safe from mimics but not from high quality digital tape recordings. To overcome this, words or numbers chosen at random can be spoken.

One telephone-based technology provider quotes error rates of 1% for its system. A stand alone provider is quoting a false acceptance rate of 0.9% after the first attempt and a false rejection rate of 4.3% after three attempts.

The templates sizes for voice verification systems varies between the different suppliers since some just require the user to say one word whilst others need whole sentences. The templates are usually upwards of 1,000 bytes.

The cost of systems ranges between US$1,000 and over US$10,000.

DYNAMIC SIGNATURE VERIFICATION: Signature verification has the advantage that people around the world are used to verifying their identity in this matter. Signature verification devices record the way in which a signature is written rather than its appearance. This is measured by a special pen, a sensitive tablet upon which the signature is written with an ordinary pen or with a tablet and stylus purchased as a standard computer peripheral.

Unfortunately some systems are unable to cope with people whose signature changes radically each time it is written.

Dynamic signature verification devices are easy to use acceptable to the public and difficult to circumvent. One product tested by Sandia National Laboratories was found to have a false acceptance and false rejection rate, after two attempts of 058% and 2.1% respectively.

The template size is quite small at around fifty bytes but to reproduce the signature image, more information needs to be stored.

The cost of a single signature verification unit ranges from US$320 on upwards.

The following table[16] gives a basic comparison of biometric methods, where 1 = worst and 5 = best:

Table 10:

*The figure has been split between pen-based and tablet-based devices with the first figure given to pen-based devices and the second to tablets.

**The ratings for voice systems have been split with the first rating relating to on-line telephone based verification and the second to off-line stand alone systems.

[16] Taken from: Newham, Emma. 1995. The Biometrics Report. London: SJB Services.

	Reliable	Compact	User friendly	Accuracy	Price	Template size
Eye pattern	3	2	2	5	3	4
Fingerprint	3	3	3	4	3	2-4
Hand geometry	3	2	4	5	3	2-5
Signature	2/4*	3	4	2	5	4
Voice**	1/4	5/3	4	2/4	3	3

E6: VERIFICATION WITH THE HELP OF HOT CARD FILES

Verification of cards with the help of hot card files at POS is an important tool to make sure that stolen and lost cards that have been reported and cancelled can not be used fraudulent. This is especially vital since most card fraud takes place at POS. Table 11 shows the value of fraud for different categories in 1993[17].

[17] Taken from: Newham, Emma. 1995. The Biometrics Report. London: SJB Services.

Table 11:

Fraud category	£ millions
Value of fraudulent POS transactions	95.8
Value of fraudulent ATM transactions	2.5
Value of other card fraud	31.5
Total value of fraudulent transactions	129.8

What a hot card file is and how it can be operated is explained in the catalogue of CardClear the card fraud prevention company that is the clear market leader in the UK. A hot card file is simply a file that holds all the card numbers reported stolen, lost or otherwise involved in fraud. The next step is to make this hot card file available to the POS. There are two ways of doing this on-line or off-line.

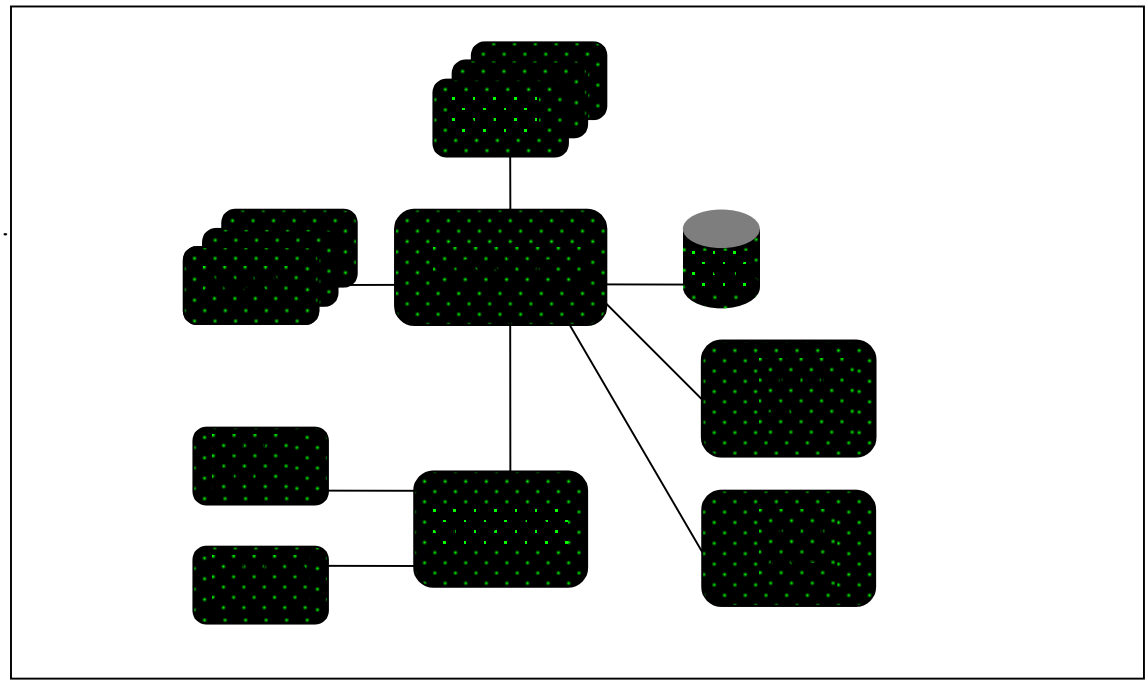
An on-line version offered by CardClear is outlined in its prospectus:

„CardExpress is an on-line authorisation service connected to the retailer's point of sale. Each plastic card transaction is sent to CardClear's central CardExpress hub. All transactions regardless of value are checked against CardClear's hot card file, which holds millions of card numbers, giving a response in under one second. All transactions above

the floor limit are passed on to the merchant acquirer for immediate authorisation and a response is given to the retailer in 5-7 seconds."

To gain a general insight into the on-line version consider figure 12[18]:

Fig 12:



The benefits of this method are:

- High speed authorisation
- Protection for all card types
- Cheque guarantee card protection
- Elimination of manual authorisations

[18] Taken from CardClear's prospectus

- Reduced risk through hot card file use
- Enhanced customer service

The off-line concept offered by CardClear is described as follows:

„The hot card broadcast is an electronic hot card warning service delivered to the retailer's point of sale. Details of hot cards are received directly by computer link from all major card issuers. Updates are continually broadcast by CardClear to every protected retail site in the country. The hot card file holds millions of card numbers."

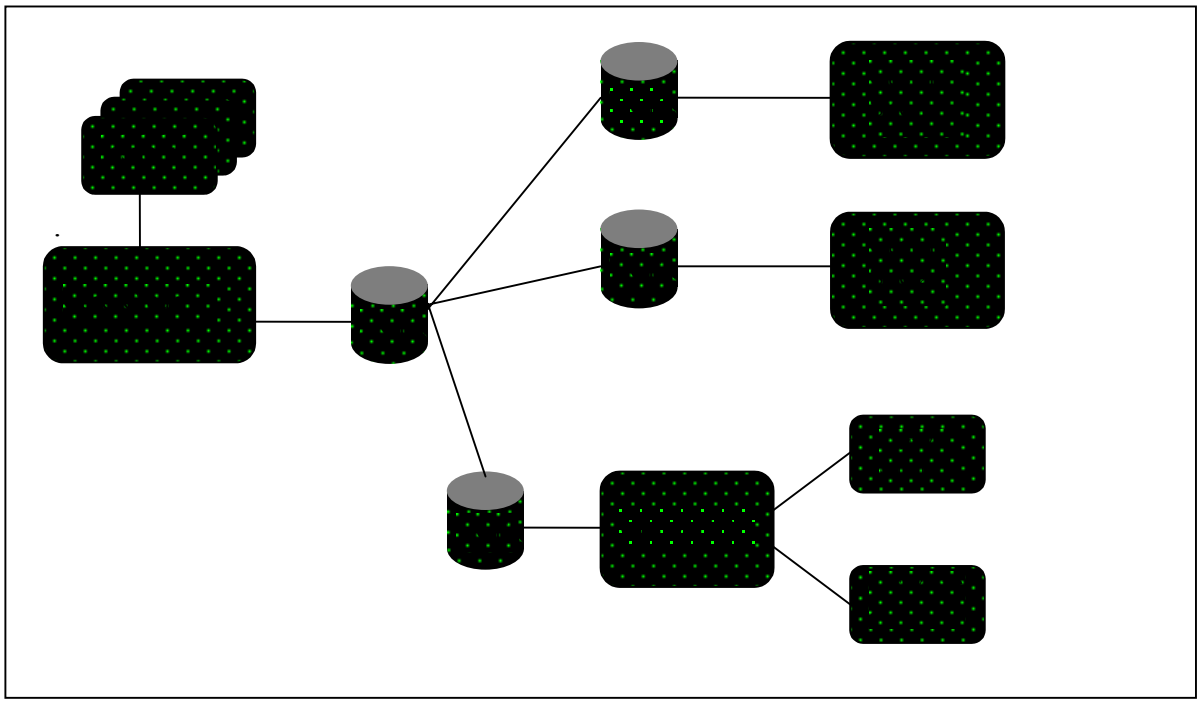
The benefits of the off-line method are:

- Reduces cheque fraud
- Reduces chargebacks on card transactions
- Protects retailer's own label and staff discount cards
- Avoids delays at point of sale
- Remote and central delivery options (central delivery is delivery to the HQ of big retailers per ISDN whereas remote delivery is the delivery to every retail outlet of smaller chains per TV aerial link.
- Deter criminals
- Avoids reliance on cumbersome paper hot card lists
- Helps expose collusive staff and reduce shrinkage[19]

The off-line version is visualised by figure 13[20]:

[19] The benefits of both concepts are suggested in CardClear's prospectus
[20] Taken from CardClear's prospectus

Fig 13:



The big advantage of the on-line version over the off-line one is the fact that data can be exchanged in both directions: from and to the retailer. The leads to a faster diffusion of up to date information and the whole network can benefit from fraud detection faster. Furthermore are there some new cards on the market that need on-line verification every time they are used (zero floor and smart card products). Other cards need sometimes an on-line verification because of a spot check. On-line verification helps also to put in place the rejection of suspicious purchases. This system analyses the purchase behaviour of any client and refuses purchases that do not fit in this pattern or that are geographically hardly or not possible (e.g. purchase with the same card in Los Angeles and Hong Kong within one hour).

Off-line verification may be needed if the infrastructure for an on-line verification of certain cards is not existent. Additionally it is not always cost effective to on-line authorise every transaction.

That hot card files are very effective in combating the card abuse and fraud problem was confirmed in an article from Der Spiegel[21]. In this article the author describes how a criminal organisation got caught thanks to on-line verification. Their method was to buy luxury goods in Germany with stolen credit cards from America while pretending to be diplomats. They chose their targets with great care avoiding any POS with on-line verification. About 60 German merchants were involved in this organisation as well. The organisation was finally exposed when a group of four members tried to pay with a stolen card not realising that the petrol station was on-line. But the estimated damage to that point was already DM40m (£13m). Nearly one thousand stolen cards were confiscated and 400 suspects put on the wanted list. Assuming that the hot card file would have been up to date, the use off an off-line hot card verification had exposed the criminal organisation as well.

F: ADDING VALUE TO PLASTIC CARDS THROUGH BETTER HANDLING OF SECURITY ISSUES.

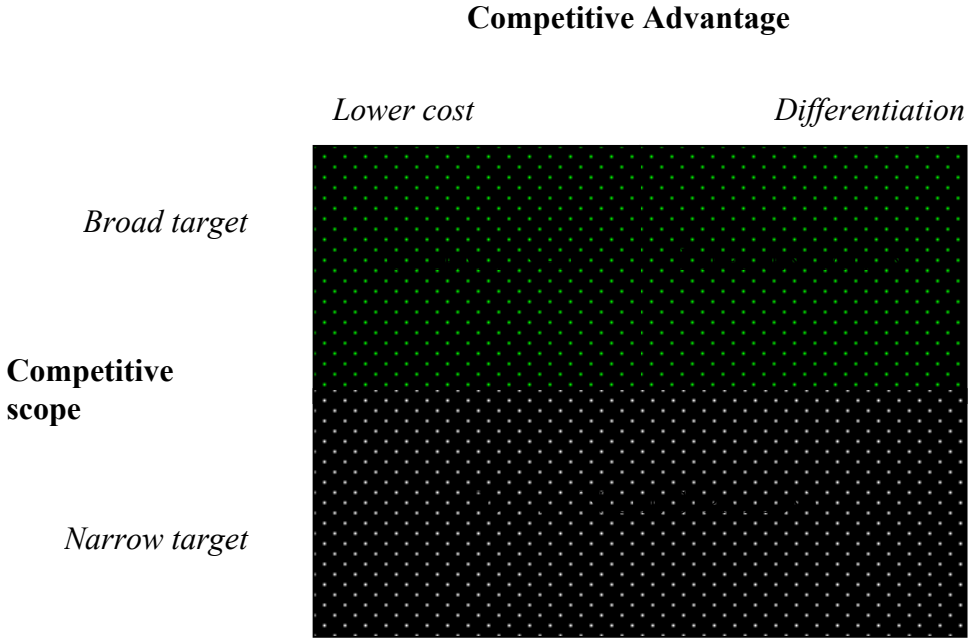
F1: POSSIBLE SOURCES OF VALUE ADDED

As outlined in the payment circle the card industry is in a dilemma: the market is mature and saturated at the same time as a large proportion of the population is refused credit or debit cards because of a lack of financial trustworthiness. Those persons considered financially trustworthy have in general more than one card. This has been confirmed by the findings of the survey. The average number of cards held was just under three (including cash cards). Those persons who have lately been admitted to hold payment cards (zero floor limits) are less profitable clients than the other cardholders since every transaction must be authorised by the issuer. This indicates that a further relaxing of admission criteria is improbable in an industry were margins are tight.

In order to build a sustainable competitive advantage, issuers have to differentiate themselves from their competitors, they have to build up a cost leadership or they have to follow a niche strategy. Porter's theory about generic strategy options suggest that there is a danger that a company engages in each strategy but failing to achieve any of them, hence it gets stuck in the middle. In Porter's opinion, a company in such a position would be put at a disadvantage because there is a leader in any segment being in a better position. Porter has brought this together in figure 14[22]:

[21] Der Spiegel. 11/94. Springer Verlag. Pages 81

Fig 14:



Two generic strategies seem especially feasible: differentiation and cost leadership.

A cost leadership can be achieved through the implementation of innovative fraud preventing systems, such as smart cards, biometric verification and extensive use of hot card files. Taking Bank of Scotland the fifth biggest bank in the UK as an example, the following numbers can be estimated. Bank of Scotland has a market share of about 10%. This means that about £9.7m out of the total loss of £97m that banks suffered last year can be attributed to Bank of Scotland. A reasonable decision would be to invest a third of that amount (Bank of Scotland's loss) in order to reduce fraud by a third or more since investing in security becomes marginal as the investment grows. If they were to launch a hybrid card for example (magnetic stripe plus micro chip) they could make sure that the

[22] Taken from Lynch, Richard. 1997. Corporate Strategy. Great Britain: Pitman Publishing.

card works at all standard POS at the same time as it works with a growing number of merchants using smart card technology as a verification. The majority of clients does probably not even realise the difference (apart from the fact that their card now has a golden spot on it) but the uncertainty factor of abusing it would be much greater because criminals are aware of new technologies. If Bank of Scotland was the only bank to implement such a change it is likely that card swindlers try their luck with other issuers instead of risking a conviction by trying to overcome the security of Bank of Scotland. The past has proved that room to manoeuvre tempts criminals to try their luck and that the elimination of such fraudulent manoeuvre space itself already prevents many fraud attempts from happening. Additionally Bank of Scotland could start to apply biometric verification methods. Taking the information out of part E5, the cheapest method is the dynamic signature verification where one unit is already available for US$320. Equipping Bank of Scotland's 15,000 ATMs with a dynamic signature verification facility would therefore cost the company US$4.8m for hardware and a considerable proportion of that amount to put in place a system to support the new biometric system (the numerical information from part E5 is already three years old and cheaper devices are probably available by now).

The problem with introducing new systems to crack down on fraud is that they are relatively easy to copy by competitors. However, if any issuer succeeds in acquiring the patent or exclusive right for the usage of a technology or specific product it is possible to build a sustainable competitive advantage through cost leadership. On the other hand, it is improbable that this happens because the industry is dependant on standards and it will probably be one technology only that eventually establishes itself on the market for the

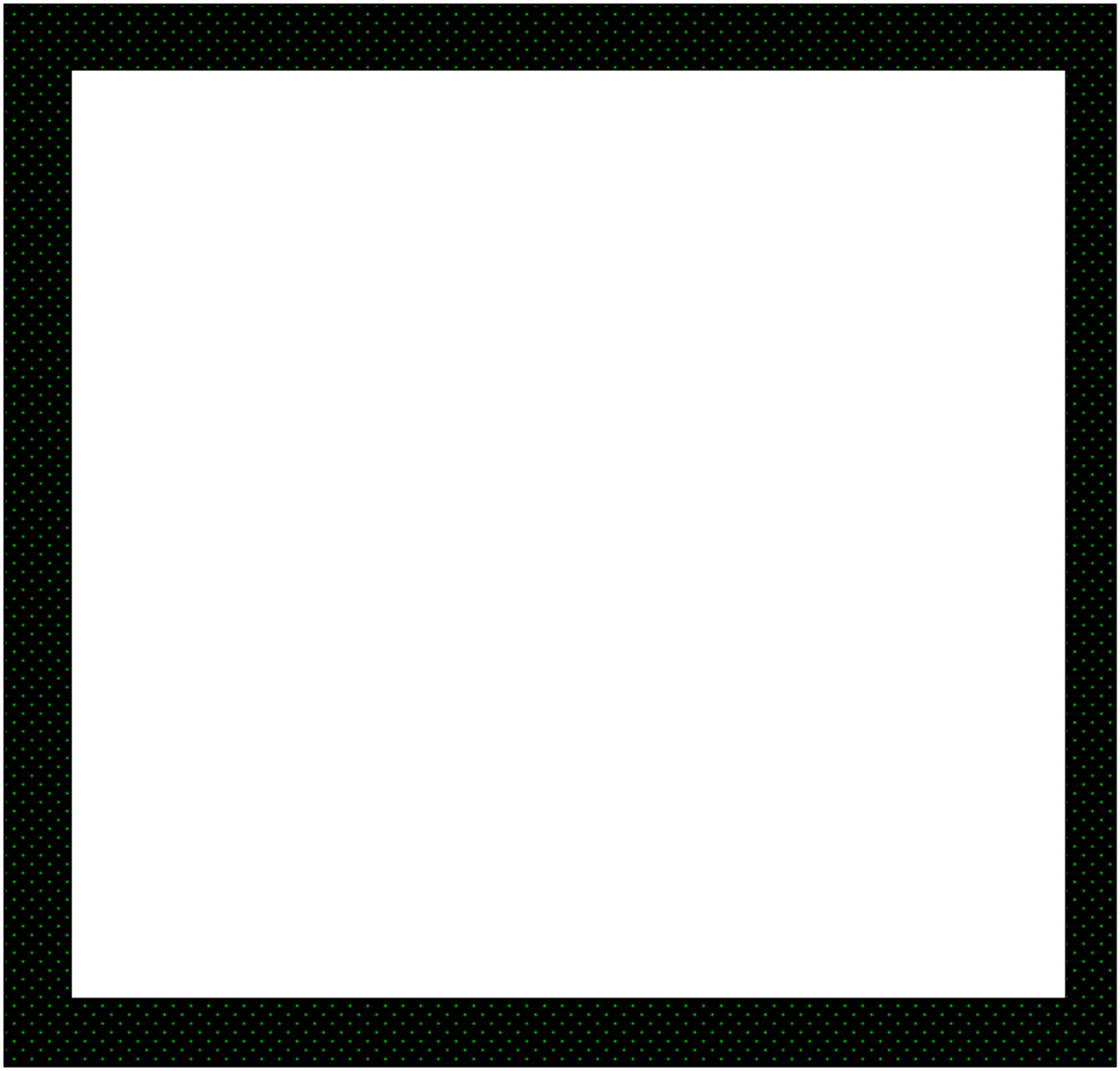
biometric verification of payment cards. This assumption is confirmed by the way the introduction of the smart card took place in France. In 1984 all banks which operated bank card systems (approximately 400) were grouped together in one organisation called „Le Groupment des Cartes Bancaires". This organisation then decided on standards and a general strategy for the country to tackle the increasing fraud problem. Regardless of the way the change of card verification is going to take place, an investment in new verification methods is promising to yield a positive NPV although it might take some time to break even (e.g. the UK has approximately 245,000 ATMs).

A by no means less important aspect is the marketing aspect of new security methodologies, indicating the feasibility of a differentiation strategy. In order to see where more value added through better handling of security issues can be created for an issuer, refer to the value chain in figure 15 on the next page.

In the survey described in part C of the dissertation the value of more secure transactions has proved to be of great marketing value: 75% of people answered the question: „would you consider changing your card issuing company or bank if another company or bank was to issue a 100% secure card?", with a yes. The reason for that is probably the negative perception about the payment security. In the survey only 27% considered cards as secure (57% reasonably secure, 9% insecure, 7% risky). Out of a list of 10 criteria ranked by importance security was in 3rd position after speed of transaction and the range of services available[23]. This indicates that a better security of transfers really is a tool to get clients of competitors. On top of that 10% of people asked have claimed to have been victimised by card fraud and 17% out of these suffered a financial loss as a result of it (average = 260£).

[23] Please refer to Appendix E for more detailed information

Fig 15[24]:



So most clients have not suffered any financial damage (under 2%, which is still an enormously high rate considering that the UK has 20 million cardholders) as a result of fraud but most banks certainly have. This is not surprising if one considers the way clients handle their PIN. 7% of people carry their PIN in their wallet. 44% have already given their PIN to another person and 24% would give their PIN (after the loss of their card) to someone on the phone if they claim to be their issuer. This is slightly less disastrous than the numbers stated by Samy Forbin during an interview. Mr Forbin is currently head of IT and electronic security at CIC, France's third largest bank. Samy Forbin made clear during the interview that the weakest part in the verification process is the human part, hence the PIN. But he did not find the idea of an introduction of biometric verification methods feasible because the project would not represent a positive NPV at the present moment in terms of direct savings of compensations of fraud victims. Samy Forbin's opinion on this topic was that the existing microchip technology should be exploited further rather than starting something new. What he thought of was the creation of an electronic identity, which means that a card should not only store financial details for the banks but also details for the NHS, the drivers license, the Inland revenue etc. The arising problem of confidentiality of data (your doctor or the inland revenue should certainly not have access to data concerning your bank accounts) can be overcome by allocating certain parts of the chip memory to certain domains e.g. drivers license. Against this speaks data from the Biometric Report[25] that shows a table of what people do not want to have on their cards:

[24] Taken from Lynch, Richard. 1997. Corporate Strategy. Great Britain: Pitman Publishing

Table 16:

UNWANTED DETAILS ON AN UNIVERSAL CARD	
Photograph	51%
Fingerprint	31%
Driving license	4%
National insurance details	7%
Details of all banking accounts	5%
None of the above	4%
Other	0.5%
Do not know	3%
Do not have a credit or cash dispensing card	20%

Finally, there are biometric methods to verify users of payment cards to add marketing value. Various banks around the world are watching the development of biometrics and

[25] Taken from: Newham, Emma. 1995. The Biometrics Report. London: SJB Services

few have even gone as far as to say that biometrics are the way to go, but even fewer have actually installed a system. Bank customers in the C_ech Rep_blic ar_ issued_with an optical memory card and have their fingerprints verified when they perform a transaction at the point of sale, while some Russians have their hand geometry measured when they withdraw cash over the counter at their bank. ATMs are the area where South Africa leads the way. All of the main South African banks are looking at biometrics in some form or another for securing payment of wages form ATMs or for general transactions performed at them.

The UK banks have been following developments in the biometric industry with interest for some time. In August 1992, a guideline document was issued containing details of what the UK banks would be looking for in a biometric device if they were to implement them at the point of sale. Performance requirements for a biometric verification device at the point of sale was published by Barclays bank, which heads the Plastic Fraud Prevention Forum (PFPF) within the British banking association, APACS.

The document stated that the devices must be available for a maximum of £150 and that the purchase price for that device must include a smart card reader. Also, it must be possible to perform verification in under three seconds. Most stringently of all, because the banks can not afford to turn away genuine cardholders at the POS, the false rejection rate was set at a maximum of less than 0.001%. This may sound very strict but even this could lead to hundreds of people feeling wronged by their bank each day in the UK alone. The required false acceptance rate on the other hand was far looser with as much as 5% being allowed. It is important to remember, however, that this document was never intended to be a concrete set of requirements since the aim was to publish a guide showing what the

banks would be looking for if they were to implement biometrics for cardholder verification and to find out what products already on the market could satisfy them. Since the document was released, and replies examined, Barclays has conducted some limited testing of fingerprint verification devices

However, since the report emphasises user friendliness of the biometric verification device, it should have been given some measurement of the required public acceptance. Figure 17 shows the public acceptance of some biometric devices established at the survey against the acceptance given in the Biometric Report three years ago:

Table: 17:

1 = worst 5= best

BIOMETRIC REPORT	SURVEY 1998	BIOMETRIC REPORT 1995
Digital Fingerprint verification	4	3
Face recognition	3	N/A
Voice recognition	3	4
Retina scan	3.5*	2
Iris scan	3.5	2
Hand geometry	3.5	4
Dynamic signature verification	2.5	4

*Half points have been used in the survey in order to give a better picture of the findings

Fingerprint verification is widely accepted and worries have decreased over the last three years. It is now the best accepted biometric device. Face recognition is very well accepted as well and is likely to increase in popularity with the increasing availability of teleconferencing and video hard- and software. Voice recognition has decreased in popularity. It received just under three points in average for user friendliness. The reason for the lower ranking is that people might find it intrusive to speak to a device in front of other people to identify themselves. Biometric methods using eye patterns have greatly increased in acceptance. People trust new technology and like being passive during the verification (there is no action needed apart from keeping the eyes open). Hand geometry verification is still as popular as it has been three years ago. Its popularity has been underlined by its use for a huge physical access control project for the Olympic village during the games in Atlanta. Dynamic signature verification finally has had a drastic drop in public acceptance. The reason is probably that people find it intrusive to having to get their signature right under pressure. The pressure comes from the need to stand a more detailed verification conducted by a computer since many signatures wary quite a bit from time to time.

If one single issuer manages to make the right choice in terms of technical features and user friendliness they might well set the standards for future verification methods. This again gives them the power to impose those standards on others, forcing them to follow the security policy of one leader. This gives the leader a good head start and possibly the chance to build a sustainable competitive advantage. Using the findings of the survey (security ranked in 3rd out of ten and a willingness to consider to change the issuer for a 100% secure card in 75% of all cases) it is probable that any leader in terms of innovative

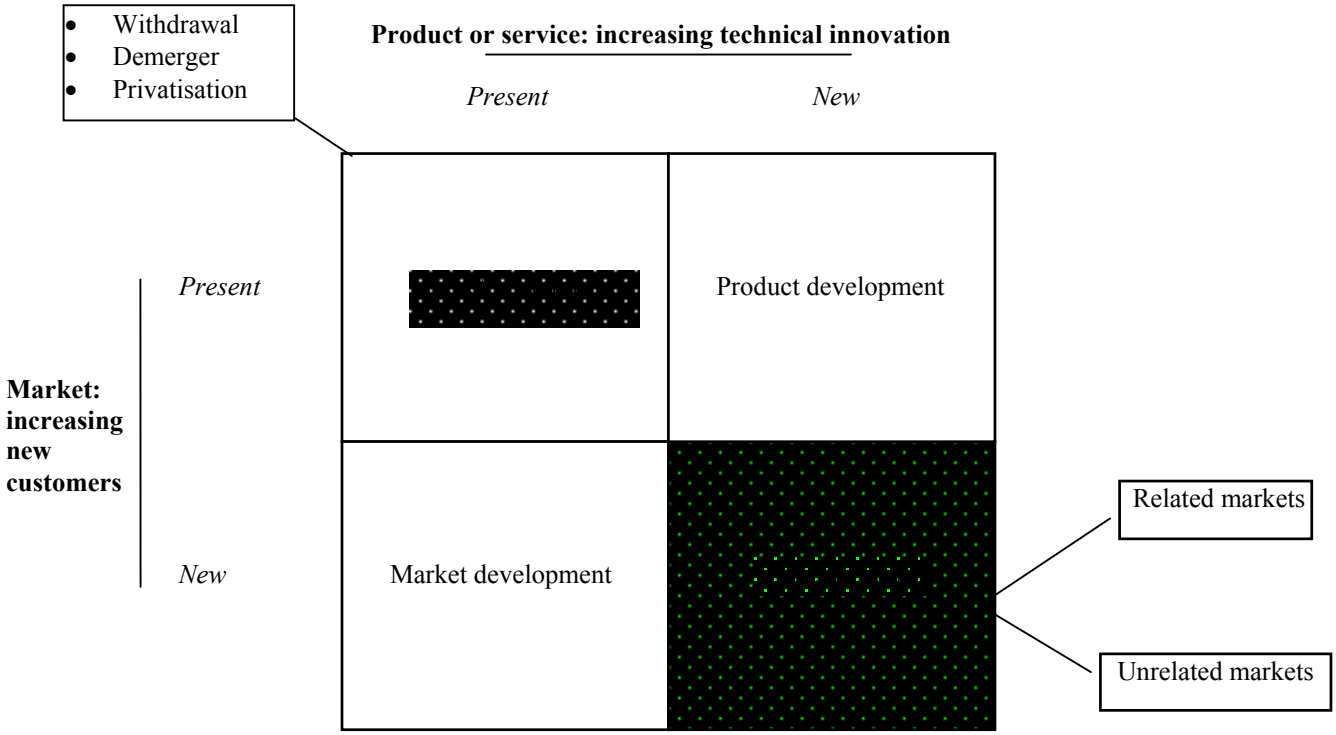
plastic card security will attract customers from his competitors. This is one way to attract revenues. The other one is to admit more clients if the security standard allows it in order to enlarge the market. South Africa has shown the way to go in this respect. So far the Standard Bank of South Africa for example has put in place two systems equipped with fingerprint technology form the Taiwanese company Startek Engineering: an automatic pay-roll system and a system to secure ATMs. The installation of these two systems has enabled Standard Bank to issue cards to clients who would have been considered otherwise as too risky and they have used biometrics too fight the problem of a high illiteracy rate in South Africa. If biometrics are coming in western Europe it is a good idea to take South Africa as a reference.

Having considered the two generic strategies of cost leadership and differentiation it becomes obvious that they are closely interlinked rather than independent. This clashes with Porter's theory whose opinion is that the three generic strategies are fundamentally different from each other. Nevertheless, the generic strategy options matrix is a good tool to show the impact made on the issuer's strategy by the implementation of a new security policy.

F2: THE FUTURE

After what has been said in part F1 it can be assumed that the most probable thing to happen after a further revision of the security standards of card payments, is a market diversification. The market expansion matrix visualises this assumption.

Fig: 18[26]



The EC funded CASCADE project (Chip Architectures for Smart Cards and secure portable devices) is another hopeful attempt to make payments more secure. Part of the funds available is to go into biometric algorithms on a smart card chip so that the biometric template does not need to leave the security of the smart cards memory. This will be made possible by using powerful new processor chips being developed by the group of companies involved in the project. The significance of the project is that it will lead to increased security and faster cardholder verification through the use of low-cost technology. The anticipated penetration of biometry in Cascade based smart cards and related terminals is given in table 19[27]:

[26] Taken from Lynch, Richard. 1997. Corporate Strategy. Great Britain: Pitman Publishing
[27] Taken from: Newham, Emma. 1995. The Biometrics Report. London: SJB Services

Table 19

Year	1996	1997	1998	1999	2000
Biometric capable cards (millions of units)	24	37	54	76	100
% using biometry	0.5%	3%	6%	10%	10%
POS terminals fitted with Cascade biometry	400	1.5k	3k	6k	10k
ATM terminals fitted with Cascade biometry	10	50	1k	2k	3k

As one can see the project is delayed but at least it is still under way. Independent from the Cascade project Steve Callaghan from CardClear assumes that biometry will enter the banking sector within the next two years. Additionally security improvements are mentioned in the annual reports of all of the five leading UK commercial banks (ranked by market share based on deposits: NatWest, Barclays, Lloyds, Midland, Bank of Scotland)

These developments mentioned and the applications listed in Appendix D are not meant to be exhaustive. Since fraud has become a global „business" it has also to be fought against globally. It is difficult to track down every latest innovation because the development

differs from country to country and moves on fast. Attitudes differ also enormously among the banks and issuers. The population knows often little or nearly nothing about the real extent of plastic fraud. Whereas some banks simply deny that they face fraud problems to keep their credibility, critical periodicals like „Der Spiegel" exaggerate in the other direction calling fraud a „threat to the system". It will therefore be important in the future to know what the population thinks of the problem before implementing a solution for it.

G: BIBLIOGRAPHY

PRIMARY RESEARCH:

Interviews:

Mr Samy Forbin. C.E.O. at CREDINTRANS, a wholly owned subsidiary of CIC Banques.

CIC is France's third largest bank.

19 Cité Voltaire, 75540 Paris Cedex 11, France.

Tel: 0033 1 46 59 22 44

Mr Wieslaw Bicz. C.E.O. at Optel.

Optel is a biometrics developer and specialised in a patented ultra sonic finger scanner.

ul. Otwarta 10a, 50-212 Wroclaw, Poland.

Tel: 0048 71 22 22 29

Mr Steve Callaghan. Group sales director of CardClear Plc.

CardClear is the leading UK company in the plastic card fraud prevention and detection sector.

Card Clear House, 30 St John's Road, Woking, Surrey GU21 1SA, UK.

Tel: 01483 728 700

The customer service centres of NatWest, Lloyds, Barclays, Midland and Bank of Scotland have all been of assistance in gathering information about market shares, market size, sending annual reports, etc.

Survey:

There has been one survey in the form of a questionnaire. The sample size was 59 and the original data sheets are still available. For a copy of the questionnaire please refer to Appendix E.

SECONDARY RESEARCH:

Books:

Beutelspacher, Albrecht; Kersten, Annette; Pfau, Axel. 1991.

Chipkarten als Sicherheitswerkzeug.

Berlin; Heidelberg; New York; London; Paris; Tokyo; Hong Kong; Barcelona; Budapest: Springer Verlag.

Jobber, David. 1995.

Principles and Practice of Marketing.

London: McGraw-Hill Book Company.

Lee, Henry; Gaenssten, Robert. 1991.

Advances in Fingerprint Technology.

New York: Elsevier Science Publishing.

Lynch, Richard. 1997.

Corporate Strategy.

London; Hong Kong; Johannesburg; Melbourne; Singapore; Washington DC: Pitman Publishing.

Newham, Emma. 1995.

The Biometrics Report.

London: SJB Services.

US Department of Justice, FBI. 1984.

The Science of Fingerprints.

Washington DC: US Government Printing Office.

Wigand, Winfried. 1991.

Die Karte mit dem Chip.

Berlin: Siemens-Aktiengesellschaft.

Periodicals:

À la Card Journal. 3/92.

Hoppenstedt & Wolf.

Biometric Technology Today. 11/96; 1/97; 2/97; 3/97; 4/97.

SJB Services.

Der Spiegel. 11/86; 11/94.

Springer Verlag.

Geld on-line. 5/97; 8/97.

Heinz Heine Verlag GmbH.

Protector. 6/94.

Protector Verlag.

Internet:

B³¹d! Nie zdefiniowano zak³adki.

B³¹d! Nie zdefiniowano zak³adki.

B³¹d! Nie zdefiniowano zak³adki.

B³¹d! Nie zdefiniowano zak³adki.

B³¹d! Nie zdefiniowano zak³adki.

B³¹d! Nie zdefiniowano zak³adki.

B³¹d! Nie zdefiniowano zak³adki.

Other:

-Annual reports of NatWest, Barclays, Lloyds, Midland and Bank of Scotland.

-CardClear's prospectus.

-Handout from the 3rd International Card Conference in Hamburg (6/93).

-Patents from Siemens, Optel and Sonident.

H: APPENDIX

APPENDIX: A[28]

Categories	% of population	Groups	% of population
A Thriving	20	Wealthy achievers, suburban areas	15
		Affluent greys, rural communities	2
		Prosperous pensioners, retirement areas	3
B Expanding	12	Affluent executives, family areas	4
		Well-off workers, family areas	8
C Rising	7	Affluent urbanities, town and city areas	2
		Prosperous professionals, metropolitan areas	2
		Better-off executives, inner city areas	3
D Settling	24	Comfortable middle agers, mature home owning areas	13
		Skilled workers, home owning areas	11
E Aspiring	14	New home owners, mature communities	10
		White collar workers, better-off multi-ethnic areas	4
F Striving	23	Older people, less prosperous area	4
		Council estate residents, better-off homes	12
		Council estate residents, high unemployment	3
		Council estate residents, greatest hardship	3
		People in multi-ethnic, low income areas	2

APPENDIX: B

[28] Taken from: Jobber, David. 1995. Principles and Practice of Marketing. London: McGraw-Hill Book

1974: Roland Moreno patents the smart card

1978: First large field study of smart cards in the banking sector. The card was produced by the company Bull and had two separate chips (storage unit and microprocessor).

1981: Foundation of the INTAMIC (International Association of Microcircuit Cards) with the aim to establish standards in order to market the smart card.

1983: Deutsche Telecom introduces first prepaid telephone cards.

1984: Introduction of the chip card for telephones in France by France Telecom

1985: The first chip card produced by Thomson and Bull is introduced.

1986: AT&T introduces the first chip card without contacts designed to work in public phones.

First field study of super smart cards in Japan (with integrated display and keyboard).

1989: In the German city of Regensburg the GZS (Gesellschaft für Zahlungssysteme) organises a field study in a shopping mall for cashless payment involving the emission of 40,000 multifunctional chip cards.

APPENDIX: C

company.

The structure of a chip card can be divided into two parts: the logistics part and the storage part.

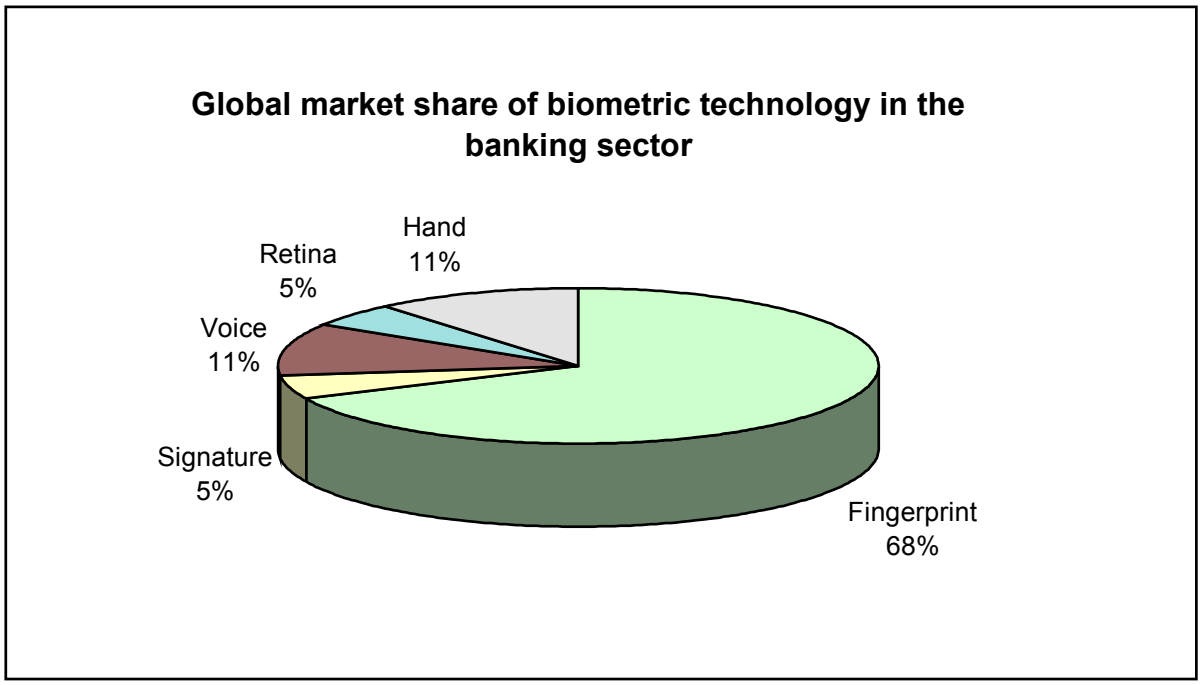
The logistics part has two main functions: it supervises the data exchange between the terminal and the card and it controls the access to the memory with the help of encryption methods.

The storage part has three separate functional areas: the open part (free access to data), the protected part (access through logistics part), and the secret part (access only through the corresponding security requirements being normally the microprocessor). The open part contains normally the card number, currency, account number, validity and the data resulting from the input of incorrect PINs. The protected part contains all confidential data and can only be accessed through a key. This data includes normally the identity of the card holder and financial parameters. The secret part can only be accessed through the microprocessor. This indicates that even the terminal has no direct access to this part. This part contains the PIN and all the parameters to control the functions of the other parts of the microchip.

APPENDIX: D[29]

Access control: Still the most dominant application, taken eve further with the use of hand geometry at the Atlanta Olympics and fingerprint technology at Walt Disney theme parks. Following the price reductions biometrics should displaced other access control technologies. MasterCard and Visa's response to access control trials.

Banking : Chase Manhattan trials voice technology and reviews dynamic signature verification. Russian, Czech and South African banks already have installed biometrics. Banking is set to be the highest growth market for the coming years. Progress by Visa and MasterCard is keenly awaited.



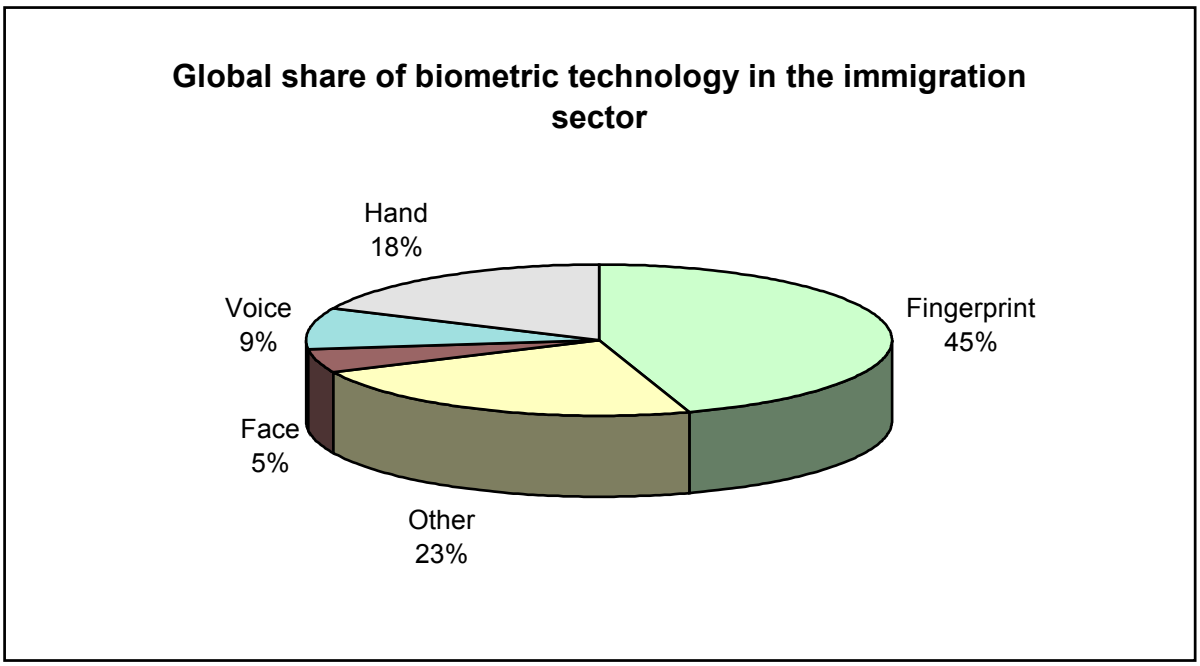
Computer access: Oracle database secured by finger scanners, but the true potential is yet to be fully realised .

[29] The article is taken from Biometric Technology Today. 11/96. SJB Services: pages 14-15.

No single biometric has dominated and the market is wide open. Consumers will be enticed by new products as prices are slashed.

Immigration: INS expands the use of fingerprinting in INSPASS and IDENT. Face recognition at Brisbane Airport and fingerprinting in Taiwan.

Frankfurt Airport will draw attention to biometrics throughout Europe. Australian facial recognition may divert attention from hand and finger technologies.



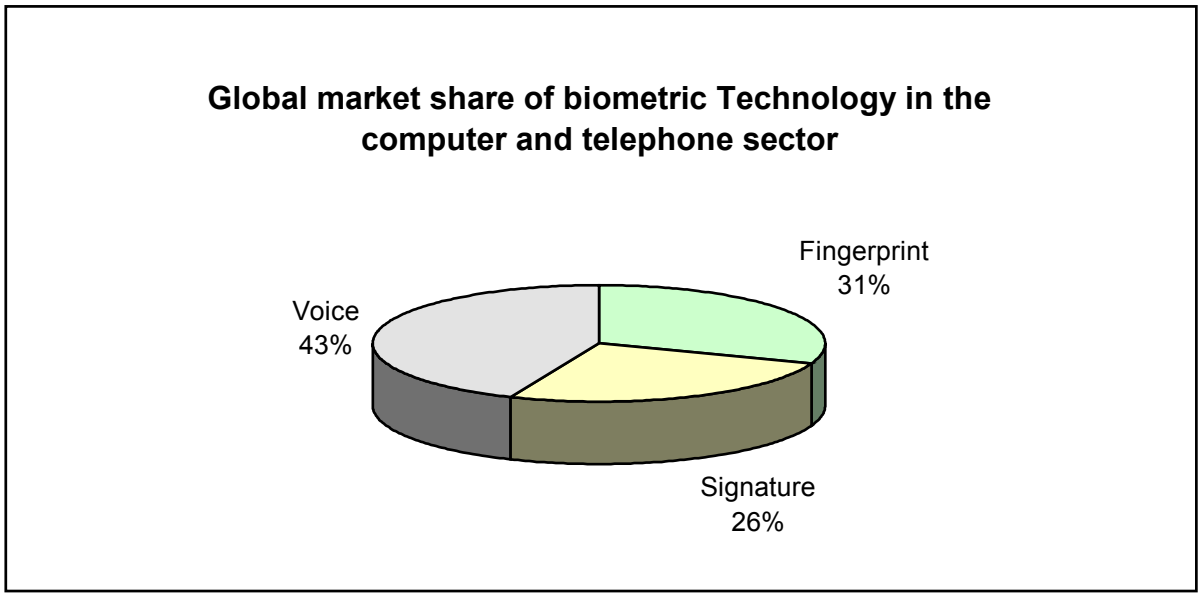
National identity: Jamaican national identity and voter registration scheme.

The South African national ID system will potentially be the largest biometric application enrolling up to 43 million people.

Prisons: US and UK prisons embrace hand and finger technology.

Telecommunications: US telecommunication company Sprint continues to forge ahead with the use of voice verification.

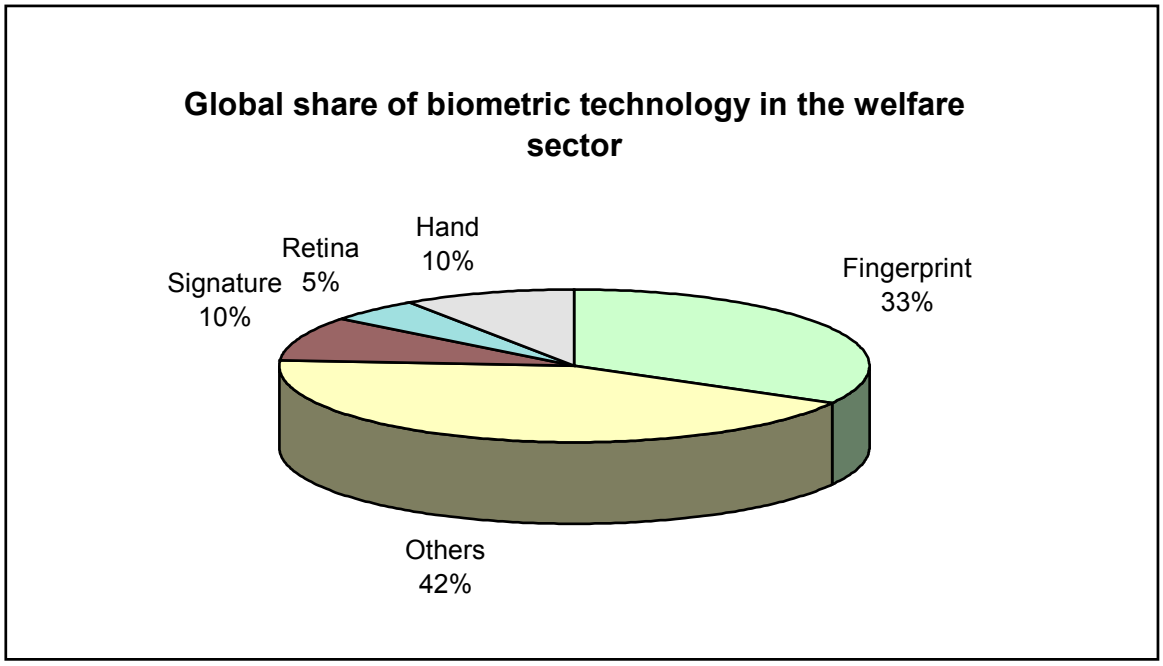
Perhaps the only area where a single biometric technology works alone, the European CASCADE trials could take calling card voice verification to new heights.



Time and attendance: Fingerprint technology used to monitor the attendance of 100,000 staff at Woolworths supermarkets in Australia. Voice verification will continue to be popular as will integrated time and attendance systems from a number of biometric vendors.

Welfare: ZASS the Spanish scheme is still the largest application of biometrics.

Electronic benefits could revolutionise the secure transfer of benefits. The success of the north-east coalition of States may also prompt other US states to merge benefit systems.



APPENDIX: E

Fraud and abuse of Credit/Debit/Cash Cards has increased in line with the rise of plastic cards as means of payment.
This questionnaire aims at establishing the perception of card holders about security issues.
All information gathered will be used for a dissertation on credit card fraud.

Age : ____ Profession : _____

Gender : _____ District of residence : _____

Employment status : employed ☐ unemployed ☐

1) Do you posses any credit/debit/cash cards ? Yes ☐ No ☐
   If yes, how many : credit : _____ debit : _____ cash : _____
   If no, questions 2, 5, 8 and 9 are irrelevant for you.

2) Have you ever been a victim of card abuse or card fraud ? Yes ☐ No ☐
   If yes, have you suffered a financial loss ? Yes ☐ No ☐
   If yes, how much ? (meaning that the issuing institute or bank has not covered the damage) : _____

3) Do you consider the use of cards as a means of payment in general as :
   secure ☐ reasonably secure ☐ insecure ☐ risky ☐

4) Would you consider changing your card issuing company or bank (or getting a credit/ debit/cash card if you do not have one) if another company or bank was to issue a 100% secure card ? Yes ☐ No ☐

5) Does any one of your cards have a microchip on it ? Yes ☐ No ☐
   If yes, who is the issuing company or bank and what type of card is it e.g. debit card or credit card : _____

6) Which of the following methods do you consider acceptable in terms of user friendliness if used for credit/debit/cash card verification? Please tick the appropriate number.

Method	Not familiar with this method	Acceptance Low				High
Digital fingerprint scan	☐	1	2	3	4	5
Face recognition	☐	1	2	3	4	5
Voice recognition	☐	1	2	3	4	5
Retina scan	☐	1	2	3	4	5
Iris scan	☐	1	2	3	4	5
Hand geometry scan	☐	1	2	3	4	5
Dynamic signature verification	☐	1	2	3	4	5

7) Please rank the following ten reasons for being with your bank.
1 = most important, 10 = least important

Friendly staff _____
Range of services offered _____
Good branch network _____
Speed of transactions _____
Security _____
International presence _____
Private banking _____
Pensions _____
Insurance _____
Many cash-machines (ATMs) _____

8) Do you carry your PIN-code in your wallet in any form ? Yes ☐ No ☐

9) Have you ever given your PIN-code to a friend or any other person ? Yes ☐ No ☐

10) Assuming that you lost your card, would you give your issuing institute or bank your PIN-code, if they called you and asked for it in order to cancel your card ? Yes ☐ No ☐

11) Comments: _____

_____

_____

Thank you very much for your time for answering these questions.

RESULTS

Average age: 27 years

Male: 61%

1) 97% of people asked have a card. The average number of cards is 1.08 credit cards, 073 debit cards and 0.73 cash cards.
2) 10% have been a victim of card fraud but only 17% suffered a financial loss. The average loss was £260.
3) Only 27% consider plastic cards as secure (57% reasonably secure, 9% insecure, 7% risky).
4) 75% would change their issuer for a secure card.
5) Most European countries have smart cards by now. England, however, does not.
6) Biometric methods are already widely known. Depending on the biometric method between 60% and 92% claimed to be familiar with the method. Acceptance was good ranging from 2.7 to 3.8.
7) The ranking for the ten criteria was the following: 1. Speed of transactions, 2. Range of services offered, 3.Security, 4.Good branch network, 5. Many ATMs, 6. Friendly staff, 7. International presence, 8. Private banking, 9. Insurance and 10. Pensions.
8) 7% carry their PIN in their wallet
9) 44% have given their PIN once ore more to friends or other persons.
10) 24% would reveal their PIN to somebody who calls on the phone and claims to be the issuer (who needs the PIN in order to cancel the card) after the card was lost.

APPENDIX: F

RESEARCH PROPOSAL

RESEARCH QUESTION

As I found it very difficult to find any literature about the very specific topic of finger print scanners and related topics as well as it would have been very difficult to interview somebody about this specific device I decided to broaden the question. The new research topic will be: **credit/debit/cash card fraud and how to prevent it.**

BACKGROUND

Card fraud is global multi-billion dollar business. Because the card companies are suffering from fraud they are keen to prevent it. The result is an industry worth nearly as much as the criminal counterpart. This is why the competition is fierce and getting even fiercer. Therefore, the first part of the dissertation will consist of an analysis of the market in terms of how fraud is conducted and who is suffering from it. The general mechanisms of how credit/debit/cash cards work will be explained in order to show weaknesses in the process in terms of security.

The second and more important part will explain the methods used to prevent fraud. This will include methods that are not used yet. That is where I will bring in the finger scanner. It will probably be a relatively big part in relation to others simply because I have very

good information about this device. The French model of the smart card will also play an important role because I have a contact to the French CIC bank's security department which is basically a wholly owned company specialised in security issues. In the end there will be a conclusion which summarises the findings of the dissertation.

METHODOLOGY OF RESEARCH

The first thing that I will be doing is to organise the two most important interviews. The first one with Mr Bicz in Warsaw who is the technical supervisor of the finger print project and the inventor who started the project by approaching venture capitalists in the first place. Although he is a technician he is the one who has many visions of how the device can be used. I will probably meet him right after my finals in December. What I want him to do is to explain me the device in a simple way (I already have the patents and the underlying descriptions but I understand absolutely nothing because I am not a physics student). Because he has been out there for quite a while now, I am convinced that he is aware of the market he is about to enter with that product. I will ask him about the market structures and problems they are likely to face once the product is ready to be launched. If he can not give me enough information about the market I will try to contact the venture capitalists or/and the technology fund in Warsaw which is about to finance the project in exchange for a 40% participation.

The second interview is the one with Mr Forbin who is my contact at the CIC security department. He lives in Paris and I will try to interview him as early as possible next year, may-be even before the next semester has started. I will try to collect as much information

from him about the French smart cards as possible. May-be I can get his opinion about the finger print scanner. He will certainly have a wide knowledge about the market and its trends (figures on fraud offences, investment figures to prevent fraud, technical limits and developments, figures from different banks and credit card companies, names of competitors, clients needs, legal restrictions and constraints). An interesting issue is that the United States now want to adopt the smart card but in another format. The benefit to refit the ATMs will mainly go to American companies. I know from a short conversation that Mr Forbin is trying hard to keep the French smart card standards. If the information obtained is insufficient I will have to try to find these information through secondary research.

Both of these interviews are very likely to happen since I came to the contacts through connections. In the unlikely event that I can not conduct one or both interviews, it will become more difficult to collect data but it will not make it impossible. Furthermore are there other good sources of primary research. It is a company called Card Clear which is listed on the Alternative Investment Market (AIM) in London. It is a medium sized company with a projected £500,000 pre-tax profit for this year. This company has specialised in credit card fraud prevention and detection. It was frequently mentioned in the quality press over the last year (found nearly 20 articles in the McCarthy at the city business library). I have not established or tried to establish contacts yet but it should be possible to approach a company that is listed at the AIM. The standards of the AIM require annual reports which I think is not a problem to organise.

An other source could be Scotland Yard and Interpol. I hope that I can get statistics and information about macro economic impacts of card fraud.

The last idea is to create a questionnaire and send it to recent victims of credit card fraud. With the mailing included (second class) every name will cost me about 40p. With a reply rate of maximal 10% I would have to mail about 500 contacts in order to get a reasonable sample size of 50. The cost for that would be over £200 which is the absolute maximum I can and want to spend. A faster and cheaper solution would be to go and acquire the data personally in the streets. The problem would be to find people who have been victimised by credit card fraud.

SOURCES OF SECONDARY RESEARCH

Until now I have found some sources of secondary research. Those are:

1) Banking Technology. A magazine which comes out once a month and which has some very interesting articles about credit/debit/cash cards, fraud, latest news in the market etc.
2) Cards 2000. Technical development, fraud issues, history and market analysis are covered in this book.
3) Credit Cards. Like cards 2000 but more history and details about what a specific card can do for you.
4) Credit, Debit and Cheque Cards. All the legal aspects of holders and companies are covered in this book, but the aspects of a third person abusing the card are very limited.
5) Regulating Fraud. This book covers fraud in general. It gives future prospects, studies attitudes and impacts, prosecution and trial of commercial fraud.

TIME FRAME

As mentioned before I will have done my two most important interviews at the beginning of next semester. During most of the semester I will complete the reading and any other primary research. I will try to do the actual writing of the dissertation about one month before the first hand in date of May 1. This means that I am definitely aiming to hand in the dissertation at May 1.

FRAMEWORK OF REPORT

I intend not to give a structure for the report because the outcome of my primary research and the availability of required secondary information will have a great deal of impact on the structure of my report. It would therefore be a very artificial report and probably not correspond to the real outcome. The only thing which is pretty sure is that there will be two parts as described under Background.