

The situation as it stands in the world of cards

P.J. Lakeman and A. Knopjes

Introduction

Applications for Card developments have been found within payment functions, identification functions, registration functions and through various other (social) applications.

The information produced by the use of cards will be used more and more as a marketing instrument.

New user environments will be created in which the card plays an important role. Such environments include the use of cards in domestic situations (gas, electricity, water), in various forms of communication (telephone card, electronic banking, teleshopping and so on), but the cards will also be used in the transport and other forwarding sectors.

Not all of these user environments are equally sensitive to fraud committed with cards, but there remain sufficient interesting environments that can count on the close attention of criminals.

The starting points for the introduction of chipcard technology are cost saving, user convenience, improving the quality of service and the accessibility of services. Depending on the development of this technology, the consumer/cardholder will be given the right of self-determination regarding the amount of information they wish to carry with them.

Card developments: past, present and future

The American journalist Edward Bellamy foresaw a 'cash-free society' in his novel 'Looking Backward' as far back as 1888. In this novel he sets out a number of visions which, as things presently stand, will not come to pass. But the question remains of whether there will ever be a 'cash-free society'. Given the current developments in electronic and digital payment transactions, our society does in fact appear to be heading increasingly in that direction.

The first manifestation in which a card played a major role was the credit card, or the 'shopping card', which was already being used as a means of payment in America in the nineteen-twenties. The card could only be used in one shop and was settled monthly. Collaborations between shopkeepers gradually led the expansion of the cards' range of applications.

Around 1950 a number of American businessmen floated the idea of payment with

a business card in a number of exclusive restaurants. Their credit rating served as a guarantee of payment.

The foundation of 'The Diners Club' quickly followed, which brought out the 'Travel & Entertainment Cards' (T & E cards) on the basis of that payment system.

People could use these cards to pay for travel and entertainment. Cardholders paid a one-off contribution and the accounts were debited at the end of the month without interest being payable over that period.

The success of the T & E card led to The Diners Club developing into a credit card organisation, and it was not long before others followed in its footsteps. The Diners Club faced competition from the 'American Express' organisation, which put the same type of card on the market.

In the meantime, American banks also began to take an interest in the new payment method, which culminated in an enormous range of bank cards offering their holders continuous credit. The mutual competition reduced sharply in the nineteen-sixties, when a number of large banks entered into joint ventures. One of the larger banking organisations, 'The Bank of America', brought its first plastic payment card onto the market in California.

Following on from the success of the payment card, in 1975 or thereabouts The Bank of America called a separate card issuing organisation into being, which was given the name 'Visa'. This organisation faced competition with another credit card organisation which broke away from 'The Interbank Card Association'. This organisation is now known as 'Mastercard'.

Whereas America had been spellbound by the credit card for many years, it was not until the nineteen-sixties that the payment system began to catch on in Europe. Diners Club and American Express had for some time enjoyed success in a number of European countries with their Travel & Entertainment Card, but the development only truly got underway in 1968 with the foundation of the Eurocard International group, which opened Eurocard offices in various European countries. This group was later taken over by the Mastercard organisation, which explains why the name 'Eurocard/Mastercard' is still seen today.

However, the use of cards was and is not limited to payment transactions. Cards have been used in the health care sector for many years. These are embossed cards that contain various (medical) details.

The retail trade has also discovered the benefits of the card. These cards usually have a communicative layout showing the company's logo. A company uses the logo on the card to raise its profile among users. The card's appearance and status are intended to ensure that they are always carried by the customers.

Cards used to bear nothing more than a graphical depiction, but these days they come with various devices such as a magnetic strip or even a chip. This provides the suppliers of these cards with unprecedented opportunities. The supplier can gain insight into the buying behaviour of the consumer, for instance. The consumer is in turn attracted by the benefits offered by the cards, such as collecting points for

exclusive gifts. The 'flexible friend' has led to many people unconsciously changing their buying patterns.

There is no holding back the development of cards, irrespective of whether they are used for payment transactions, in the health care sector, in the retail trade or as an identity card. The multi-functionality of the cards sometimes gives rise to non-related companies or institutions jointly presenting services or applications to the consumer.

The developments will not only have consequences for the card users. The use of cards also leads to the growing acceptance of new concepts.

Concepts such as card issuer/supplier, cardholder/user and card recipient will become part of our everyday communication, but other concepts such as usage options (various areas in which it is possible to use the chipcard), transparency (official and administrative decision-making processes can be based on data in the chipcard) and multi-functionality (the many usage options).

A chipcard has three basic functions: data storage, data processing and data communication.

These three basic functions lead to countless ways of using a chipcard. The question remains, however, of whether all card users are willing to accept them. Various interests, such as economic, scientific and more general interests can influence the user's willingness to accept the card applications.

A situation can arise in which the cardholder is confronted with technological developments for which he is not (yet) completely ready. Given the interests that affect the development of chipcards, it is conceivable that situations will arise in which people feel more or less obliged to go with the flow. There is also the question of a situation that can arise if it turns out that the usage options of an individual cardholder are being misused.

The introduction of the chipcard and its multifunctional applications increases dependence on technology. For this reason, cardholders will have to be offered as many guarantees as possible concerning the safety and reliability of that technology. The cardholder's freedom of choice is an important issue in this respect. The creation of monopolies must be avoided at all costs. We also have to ask ourselves whether the consumer should become dependent on the chipcard to obtain certain services.

Another important question is: how many details can be taken from a cardholder? After all, certain details can result in new (application) details.

Cardholders can find themselves confronted with the misuse of one or more usage options with a chipcard, especially applications from which financial advantage can be gained.

As well as the protection of privacy that is provided for by public law in many countries, we must address ourselves to developments in criminal law. This is of great importance to investigating and prosecuting card crime. Barely any

information is available about the criminal and judicial problems that investigation and prosecution can come up against.

From this perspective (investigation) the police must consider the way in which it will approach 'fraud' with chipcards. As well as obtaining information about the technological developments, attention will also have to be paid to addressing the problems of conned cardholders. Through the misuse of technology the victim can find himself confronted with the improper use of the application options. It can prove difficult for a victim to give tangible proof of the card's misuse.

Some card types

Cards are found in our society in ever-increasing shapes and forms. The best known of these is the card used for payment transactions. The debit and credit card have now become part of everyday life. But the electronic purse is also gaining ground in today's payment transaction systems. As well as these applications, however, there are also a large number of better or less-known ones.

We will start by taking a look at the composition of cards, and then the various card types and their application options.

Card composition

The cards we are discussing in this book are of the ID-1 format. Cards have to meet the requirements of a number of specifications, such as the dimensions, including thickness. This standardisation has to do with the fact it must be possible to read the cards using a reader. The conditions a card has to meet are laid down in ISO standard 7810. The conditions relate to the basic material (the substrate) but also the physical protection. One reason for the standardisation of this format is the increasing application of technical facilities to verify the cards. Inter-operability is a precondition for the optimum use of the card.

Cards can consist of a single layer: single layer cards. But they can also be built up of several layers: multi-layer cards.

The single-layer cards are printed directly on the front and back. The printing is not protected, so that they are easily damaged. Single-layer cards are typified by telephone cards without a chip application.

Depending on its purpose, the multi-layer card consists of 3 to 7 layers. A transparent layer can be placed over the front and back of the card, which protects the printing from wear. The layer can also contain elements used to verify the authenticity of the card.

The layers are melded together into one by means of a heating process. Credit cards are a good example of multi-layer cards.

Four different substrates can be used to produce cards: polyvinylchloride (PVC), polycarbonate (PC), Acryl–nitrile–butadiene–styrol (ABS) en polyester (Ecocard).

Depending on the usage conditions, the average life cycle of a PVC card is 2 to 4 years. A PC card, on the other hand, can last for a good 10 years. A material is chosen according to the card's intended use.

PC cards are often used for identity and payment functions.

These days, nearly everybody has a string of cards, many of which have a short life span. Given the explosive development in cards, it is clear that old cards could eventually have a harmful effect on the environment. This is one of the reasons that an environmentally-friendly card has been developed: the Ecocard. However, this card is still rather expensive to buy.

Some card sorts

Magnetic card

The magnetic card has up to now been the most commonly applied readable card technology. The best known applications are those for payment cards, credit cards and cards that provide access to certain areas. The application of magnetic strips continues to be developed. There are holographic magnetic strips and magnetic strips with a 'watermark'. Information was first converted into ONES and ZEROS at the beginning of the nineteen-fifties. It was then that attempts began to store information in a magnetic strip. This soon led to the storage of digital information in magnetic strips. The entire operating principle of the magnetic strip for card applications is based on standards that were created at the end of the 1960s. Cards are now produced according to ISO standards. An infrastructure has been developed within the global payment transaction system for the use of the magnetic strip. It is estimated that 500 million new cards for payment transactions are issued globally every year.

RF (Radio Frequency) card

It was initially assumed that the RF card (also known as the non-contact chipcard) would not play a major role in the development of cards. Nonetheless, a considerable market for these applications has grown within the transport and access control sectors. Other applications are expected in the coming years, and it is expected that a combi-card with a contact and non-contact chip will gain ground significantly.

Price, safety and user-friendliness make an important contribution to the continued use of this technology. When they were first applied at the beginning of the 1970s, the cards still had to be held against the reader. Since 1994 there have been applications in which the cards work at a distance of 10 centimetres or more from the reader.

Key cards

The use of keys for controlling access to areas is one that is well known and

accepted. Only the people that are authorised to enter a certain area are allowed to hold a key to that area. The use of keys as a security system is relatively cheap. But if somebody loses a key the locks have to be quickly changed in order to be sure that unauthorised persons cannot not gain access to secure areas. It is often the case that a limited number of persons are authorised to enter certain areas or departments, which necessitates complicated key procedures. With traditional keys it is not possible to ascertain which key was used for which lock at what time. The industry has responded well to the need for controlled access, and a large number of automatic access and control systems have now been placed on the market.

Each authorised person is issued with a unique 'key' that is presented to the system and read. If the 'key' is recognised by the 'reader', the door opens automatically. This type of key application is known as a key card. The communication between the key card and the reader yields information that can be stored in a central processing unit (CPU). This is used to assess whether the 'keys' presented are valid. It is also possible to ascertain whether a given person is authorised to enter a certain area. Strict security requirements have to be put in place for the connection between the 'reader' and the CPU. The assessment of the authorisation often takes place at two different positions: at the reader and at the CPU. Security is required to prevent the transmitted codes being 'tapped'. A security system of this nature carries the following advantages:

- * The system can be operated from a single point;
- * All adjustments can be made centrally with a single action;
- * All information arrives centrally at the CPU and is processed there;
- * A key card can be given a Personal Identification Number (PIN) code;
- * The card can be used 'hands free' (i.e. the key is read without the need for contact);
- * Functions can be blocked from the CPU;
- * Management information can be obtained from the CPU.

The disadvantages of this type of system are:

- * Power cuts can cause blocking which hinders the ability to continue working;
- * The key card is a personal card that can also be used by 'other' (non-authorised) persons.

Optical Memory Card (OMC)

An OMC incorporates and uses what is known as the Write One, Read Many (WORM) technology. This gives the user various options, and the large storage capacity of the card is particularly impressive. Optical memory cards are put on the market by the companies Canon and Drexler. The OMC can store sound, images and text. It is produced according to the ISO standards 11693 and 11694. The OMC presently has a variable storage capacity.

Canon, for instance, has the 4.2 Mb standard card (with a storage capacity of approximately 1600 pages A-4), the 6.0 Mb Wide Card that was especially

developed for the storage of photographs, drawings, fingerprints and so on, and the 1.86 Mb Narrow Card that provides the user with less storage capacity but facilitates combinations with other technologies such as a chip and/or magnetic strip on the same card. These cards provide the issuers with more space for designs.

The information stored in the OMC is not sensitive to magnetic effects. The OMC can be used in extreme conditions: it has been used in Antarctica, in the jungle and in the desert.

OMC Applications

Immigration and Naturalisation Services (INS) and the next generation of aliens ID documents.

In America, the public service INS has begun using the OMC as one of the new aliens documents. One of the main reasons for choosing this technology was the large storage capacity provided by the WORM principle. This OMC card is a multi-layer polycarbonate card. The photograph of the cardholder is applied to the front of the card using dye sublimation. The card also has a holographic overlay to prevent the replacement of the photograph and dates. The cardholder's personal details are also applied using the dye sublimation method. The machine-readable strip (which meets the conditions set by the International Civil Aviation Organisation (ICAO) is applied using laser engraving. The card also has UV and infra red protection elements.

Chipcard

The chipcard is a piece of plastic with an attached chip that offers many functions. The chipcard is presently the best protected card.

The chipcard usually has a 'gold-coloured chip', known as the contact surface. The memory is installed underneath. The chip always has a fixed position on the a chipcard, laid down according to ISO standards.

Inserting a chip into a card is known as embedding. The sides of the contact surface are glued to the card. the memory is located under the contact surface in a 'cavity' and does not come into contact with the underside of the card. This makes it possible to bend the card without damaging the chip. In spite of the fact that the chip guarantees a high level of security, the card is given a printed surface. The printing generally has a marketing function for most cards. It is, however, possible to give the card one or more authentication marks, which raises the security of the card to a higher level. The authentication marks can be used for visual verification if automated systems go down.

In professional jargon reference is often made to chipcard and smartcard

technology. This does not express the actual difference between the chipcard and the smartcard.

Without going too deeply into technical details, a smartcard always has a microprocessor in addition to the memory. The presence of a microprocessor increases the card's functionality. A smartcard also offers greater technical functions for communication and safeguarding processes.

Hybrid card

A hybrid card is a card with several data carriers. Examples of a hybrid card include one with a magnetic strip and a barcode, both of which can contain data. Depending on the usage conditions or application options, people can opt for one of these forms of information storage.

It is reasonable to suppose that in the coming years a card in a hybrid form will become increasingly common in payment transactions. The reason for putting hybrid cards into circulation for payment transactions is that global infrastructure of payment transactions will be adapted to the chipcard technology.

As will be clear, cashpoint machines will have to be technically adapted to meet this development. That is why the debit and credit cards in France have already contained a chip for some years. The infrastructure for the use of chipcards is at an extremely advanced stage of development there. However, French chipcards cannot (yet) be used abroad. The French chipcards therefore have a magnetic strip on the back so that they can be used in countries other than France. As soon as hybrid cards are taken into use in a country it can be expected that criminals using false cards will avoid places where the chip application is used. They will instead concentrate on locations where the magnetic strip is still in current use, or will deliberately deactivate the chip.

The barcode

The barcode was invented in 1929 by John Kermode. The formula he used was relatively simple, where a stripe (or 'bar') equals 1. Two bars stands for 2 and 3 stands for 3 and so on. This technique was later refined in such a way that use was made of bars varying in thickness and with spaces between the bars. The barcode has been increasingly refined throughout the years, which has resulted in a wide variety of barcode types. Despite the fact that many barcodes look more or less the same, they are in fact highly diverse. There is the Codabar, for instance, that is often used for express services. The Interleaved 2 or 5 is used for container transport. The Code 39 is often used in the American defence sector. This code can be used for general alphanumeric data.

As well as the barcode with the familiar bar pattern, there are also two dimensional (2D) barcodes. These barcodes contain a lot more information than the traditional

ones. In a 2D barcode individual symbols are placed above each other instead of in bars. This considerably increases the amount of information that can be stored. We know, for instance, of applications where - in addition to personal details - biometric information such as a photo, a signature and a fingerprint are stored in a 2D barcode.

The chip

The overall production process for a chip is a very extensive operation. Given below is an outline of the production process for chips as used in the current chipcards.

Before actually producing the chip, we first have to establish the functions for which it will be used. It is also important to know all of the safety standards that the chip will have to meet before starting production.

The production process has to be checked at every stage.

After the preliminary functionality and security study, the next step is to design a template. The template is then tested against existing chip technologies.

After the development process the template is given an operating system which directly determines which standard functions the chip will bear. One or more security functions are often added at this point. The functionality and security are taken up in the operating system. The pre-programmed functions cannot be accessed after the production process. Functions can be added when the chip is being initialised. This simultaneously determines the structure of the chip, which is comparable to the structure found in many personal computers. Examples include: Dir/file/record, secure areas, codes, and so on. No changes can be made to the structure after the basic initialisation process. New functions can however be added to the chip after this process.

There are various ways of inserting the chip into the card. The most frequently applied method is to glue the chip to the card.

Cards in payment transactions

In many of the world's countries the credit card is the best known card used for payment transactions. The credit card is used for many payments in America and Canada in particular, as opposed to the situation in Europe where many payments are still made in cash. The question remains of what will happen when chip technology is introduced to payment transactions. Critics assert that the 'tried and tested' credit card will not immediately be replaced by a card with a chip application. This appears to be an example of 'modern-day nostalgia'.

In 2002 a single currency, the EURO, will be introduced within the European Union (EU). This means that there will eventually be a single European currency.

This will do away with exchange rates and their accompanying risks for companies and private citizens. In the near future, this will make it even more attractive to use a payment card for purchases or payments and to have accounts settled via an automated payment system within the EU. For practical reasons, consideration is already being given to introducing some of the small denominations of the EURO (the coinage) immediately as a 'digital' currency. This is aimed at use of the electronic purse.

Personalising and printing cards

There are many ways of personalising cards. The method used depends partly on the card's functionality. The substrate (the plastic) also affects the personalisation method.

Embossing

It is also possible to emboss cards. An embossed card bears a raised image that can be felt. The part of the card that is embossed has been laid down in ISO standards. There are also regulations concerning the size of the figures and letters and the mutual distances between them. These stipulations relate to both the distance between letters and the distance between lines. The depth of the figures/letters is also laid down.

The embossed sections of the card can be given a plastic layer (known as 'tipping'). This tipping process must ensure that the embossing is easily legible, but after the passage of time the legibility of the embossing can be adversely affected by wear. It is not possible to apply diacritic symbols. Embossing can form part of other authentication marks.

Embossing is one of the older ways of personalising a card. For many cards with a payment function embossing was the forerunner of the current magnetic strip technology. Despite the fact that the magnetic strip has been used on the cards for a long time, we still see embossing as an alternative to (temporarily) failing systems. It is expected that embossing will remain a feature of payment cards well into the future. Nostalgia goes hand in hand with the current developments.

Despite the many requirements that embossing has to meet, this technique is still imitated on a fairly large scale. Use is made of embossing machines that are freely available on the market. The fact that the letter types used in these commercial machines are different from the original embossing is barely acknowledged. This has led a number of companies to develop their own non-standardised letter type (e.g. the MC on the cards issued by MasterCard).

Non–impact print technology

The development of non-impact print technology is an important step, not only because of the security the technology offers, but also because this step makes it possible to control the entire identification and authentication process from the moment that the product is introduced. Communication is raised to a new level. The personal details and digitised photo and signature information are available before the card is manufactured and can therefore be stored in a database. This means that when subsequent applications are made the card issuing authority can ascertain whether the applicant is the same person whose photo and signature have been stored. This is a completely digitised process from the application of the identity card to its issue.

Thermographic personalisation can be divided into two categories:

- * Thermotransfer, purely for text (personalisation). This takes place in the final stage of production. It is possible to apply the information in several colours, and diacritic symbols can also be applied.

- * Dye Diffusion Thermal Transfer, D2T2 for short. This technique is used for attaching passport photos to identity documents. It is also used for limited editions of specific cards that usually have a marketing function.

The equipment needed for D2T2 techniques is freely available on the market. They are therefore vulnerable to counterfeiting.

There is presently a perceivable development in the manufacturer of counterfeit cards in which use is made of Dye Sublimation (digitised) technology instead of the traditional printing techniques. The images created using the Dye Sublimation technique are built up of three standard colours: yellow, magenta and blue.

Text and/or images are applied to the layer with both the thermotransfer process and the D2T2 process. This information can be coated with a transparent laminate to prevent counterfeiting. One or more authentication marks, such as kinematic effects, can then be applied to this laminate.

Laser personalisation

The use of laser techniques involves burning the personalisation data (personalisation, passport photo, etc.) into one or more card layers.

It is also possible to adjust the density of the laser in such a way that the parts applied using the laser technique cannot be perceived. To achieve this effect, the laser is set so that it does not mark the 'top layer'. This laser engraving method is used to apply the details to many European debit cards in such a way that they can be perceived. However, using this process causes a limited amount of 'damage' to the transparent top layer. As mentioned above, it is also possible to apply the information in several layers, which makes counterfeiting extremely difficult.

After all, the old data have to be removed before they are changed. If the information is applied in/through various layers, counterfeiting causes serious damage to the card. The use of laser technology remains an expensive business. When using laser technology it is not necessary to protect the cards with a

transparent laminate. The laser engraving equipment is produced or supplied by specialist companies that are active at the top end of the high security printing market.

Role of the Secretary General of Interpol

Governments throughout the world have always taken great care to protect the reliability of their country's own currency. This is clear from the severe penalties for counterfeiting.

The Interpol Secretariat-General (SG) in Lyon plays an important role in the fight against counterfeit money on the basis of the Geneva Convention of 1929.

In spite of the fraud committed using payment cards (debit and credit cards), there is no prospect in the shorter term of a similar convention for payment cards. The government (still) gives higher priority to the reliability of its own currency than to protecting the interests of the card industry and the consumer.

There does not appear to be any way of ensuring that sufficient attention is paid to payment card fraud in the shorter term. However, we must not rule out a scenario in which this situation will be changed by the present developments in electronic payment transactions (such as using the electronic purse).

Interpol is anticipating the technological developments, especially regarding payment card fraud. The credit card industry indicated as far back as 1992 that it was willing to cooperate in setting up a central information point for gathering data on payment card fraud.

The first International Conference on Credit Card Fraud was held in October 1994.

Two important recommendations were made at this conference. The first relates to the laws and regulations of the Interpol member states concerning (plastic) payment cards. Efforts must be made to ensure that sufficient provisions are included in the legislation to make it possible to tackle any type of fraud with payment cards. In more concrete terms, the authorities must ensure that the legislation includes provisions that combat the counterfeiting of payment cards and/or the use of counterfeit payment cards. In view of the border-transgressing nature of payment card fraud, the mutual coordination of laws and regulations is of overriding importance.

The second recommendation was to convene a working group to look into the possibility of developing a classification system for counterfeit payment cards. This second recommendation has now been substantiated in the form of the 1st International Working Group On Counterfeit Payment Cards. The working group came to the conclusion that it must be feasible to develop a classification system for cards on the basis of the systems already present in Hong Kong, Canada and the United States. Given the great variety of payment cards in world-wide circulation,

the working group established that it would only be possible to develop a system for classifying completely counterfeited payment cards. Other variants, such as white plastics, re-encoded and counterfeited cards will therefore not (yet) form part of the future Interpol system.

A notable aspect here is the public-private collaboration between Interpol and the world's biggest card companies. The developments within Interpol will in part be actively supported by private industry. This collaboration can be regarded as a strategic step on the part of the card companies. Interpol has in any event indicated that it wants to take a different course regarding the manner in which relations are maintained with the private sector.

Counterfeit, forged or white plastic.

Experiences regarding the forging or counterfeiting of cards has up to now mainly concerned cards used for payment transactions. The ingenuity with which the forger counterfeits the cards leads us to believe that this tendency will continue. This means that account of counterfeits must also be taken in the field of chipcard applications.

Future studies will therefore concentrate mainly on the IT side of the card. Visual forgery characteristics will become subordinate to this. It will be necessary to work more closely with experts from the private sector for the technical analysis of the information medium in the future. Investments will also have to be made within the police force and the judiciary into specific training in the field of information technology.

Counterfeit types

What counterfeit types do we come across with payment cards?

The forgeries can be divided roughly into four categories:

- * The forging of original credit or debit cards;
- * re-encoding (overwriting existing magnetic strip data);
- * skimming (copying the entire content of the magnetic strip data to another magnetic strip other than that on the original card);
- * the use of "white plastic";
- * manufacturing completely counterfeit credit or debit cards.

Depending on the method of forgery used, criminals can make use of these methods in two ways:

- * one or more persons who are aware of the fraudulent nature of the card join a conspiracy in financial transactions;
- * or the forger assumes that the forgery has been executed in such a way that he does not expect it to be detected by people and/or devices.
- * there are of course other possible forms of fraud in payment transactions in which no use is made of cards at all.

Forged

With forged cards use is made of original cards with a number of authentication marks. Many of these original cards are obtained by criminals via a circuit that can get hold of cards that are lost or stolen. The fact that original cards are used means that the forger does not have to concentrate on imitating a number of authentication marks. These authentication marks have already been provided by the card's producer. The problem that the forger does come up against is the changing of the account holder's visual data. This information is often applied by means of embossing or laser engraving. Embossed details are 'flattened out'. The forger can imitate this process by using a simple domestic iron. If he owns an embossing machine, the forger can then apply 'new' details to the card. Another method is to use what are known as 'rub-over letters' which can be placed over the original flattened out details.

The forger is faced with a much more difficult task if he has to remove details that were applied using laser engraving. Because the data have been burnt into the transparent top layer or in several underlying layers the forger has to find a way of eradicating them, which leads to the layers being seriously damaged.

As well as removing the embossed or laser-engraved details the forger will also have to adjust the signature strip. A signature strip is generally superficially checked by the person it is presented to. That is why the forger often leaves the signature strip alone: it continues to bear the signature of the rightful holder. Another method is to affix a strip of paper to the card bearing the signature of the 'new' holder. The signature strip on an original card often bears one or more authentication marks such as UV reactive inks. The signature strip imitated by the forger often does not bear any authentication marks, so that this can be detected relatively easily by a thorough and correctly executed check.

Cards with forged visual details cannot be presented at places where a magnetic strip is used in addition to the visual checking of the card.

Re-encoding

The magnetic strip on payment cards was originally intended to make it easier to use them for payment transactions, but it has also proved extremely effective against fraud committed with embossed cards.

The trading and acquisition of equipment that can be used to apply and read magnetic strip data makes it easy for criminals to manipulate cards with one or more magnetic strips. This equipment is known in the jargon as 'readers and writers'. These readers and writers can be used to read off data from a magnetic strip, copy the 'read' data and then apply them to another card. This form of forgery increased significantly in the 1980s. Often used for this form of forgery are lost or stolen cards, but this method can also be used to copy the data of another

holder onto a payment card issued to its holder.

Skimming

Skimming is one of the last forms of fraud with which card companies are confronted. Original magnetic strips are copied and transferred to the magnetic strip of a 'white plastic', for instance.

White Plastic

White plastic is simply a piece of white plastic with a data carrier. This is perhaps the forger's simplest and cheapest way of simulating cards. The question is whether this can be regarded as a completely counterfeit card. In the case of white plastic, only a small part of the card functions: the information carrier. An added advantage for the forger is that the 'piece of plastic' is freely available, which makes things especially easy for him. If the information carrier also happens to be a magnetic strip, it is easy to transfer data onto it.

Using white plastic is only possible to a limited extent. The person to whom it is presented will be extremely dubious about it. After all, a card without any form of printing will certainly ring alarm bells when presented to a shopkeeper. On the other hand, if a white plastic card is introduced to an automatic system the criminal faces only a very small risk as visual checks are often not carried out in these situations.

It will be clear that for this form of forgery the 'illegal' user must know the access code. If a cashpoint machine is the target, he will have to know the PIN code accompanying the account number.

Counterfeiting

Depending on the wishes of their customers, card producers will make use of the graphic techniques that they have available. Mutually co-ordinated, refined graphical techniques are used for cards with what can be described as 'security printing'. These techniques can be used to make high quality products. The cards also have extra devices that are designed to make counterfeiting difficult.

Unfortunately, the forger has the necessary resources at his disposal too. These resources make it possible to produce counterfeits that can be described as 'deceptive'.

Besides the use of conventional graphical techniques we are also witnessing a shift towards the use of digital techniques. Using relatively inexpensive equipment such as a PC, a scanner and a colour printer, it is possible to manufacturer counterfeits reasonably cheaply and quickly. It is not only debit and credit cards that are made using this printing method.

Many identity documents and driving licences in card form are also counterfeited using digital printing techniques.

One of the results of this digital development is that traditional graphical techniques are now hardly ever used for making counterfeit money. Looking at the data for 1995 in the Netherlands it is notable that only 8% of counterfeit Dutch currency was manufactured using traditional graphical techniques. It therefore follows that 92% was manufactured using digital technology. The availability and usage options of colour photocopiers play an important role here. In many countries screen printing techniques are still used in addition to digital printing techniques for counterfeiting payment cards.

There is as yet no easy answer to the question of how criminals will anticipate the developments in the use of chipcard and smartcard technologies. It is by no means improbable that criminal organisations will employ specialists, as is customary in the private sector.

Bona fide parties will strive for perfection, while criminals will strive for acceptance. And there is a world of difference between the two!

Furthermore, national governments will have to ensure that the diversity of various cards does not become too great in a country (and the Netherlands is a case in point here). In spite of the goal of 'multifunctional use', public authorities want to add an individual identity to the card. This is not helpful to those who are expected to check the cards. Moreover, there is a considerable loss of capital every time that people set about 're-inventing the wheel'.

That is why our guiding principle is: aim for uniformity in the verifiability of cards, and don't turn the person that has to check them into a card player!

Training and informing the police

Criminals too have responded to changes in society. Today's crime is characterised by a large degree of mobility and continuity. No limits are placed on the criminal's territory. Criminals have a vested interest in being able to act anonymously.

The police are reasonably familiar with the forms of crime that are facilitated by the present mono-functionality of documents. We can be sure that multifunctional cards will attract a lot of interest from the criminal underworld. As well as protecting the chip technology and the card itself, it is also important that issued cards can be properly checked for authenticity both digitally and physically.

It is of great importance to provide the public, and especially those that have to check the cards - including the police - with reliable information. The idea that our society can rely solely on technology can and must never be allowed to take root. The human factor will always form part of the verification process. As well as providing reliable information, attention should also be paid to this social development in police training. A good quality service requires good quality members of staff. Permanent education is therefore an important instrument for ensuring that members of staff are adequately qualified.

The quality of police training is guaranteed by operating a construction in which a balance is created between knowledge of the subject matter and didactic qualities. In Netherlands, the National Police Selection and Training Institute (LSOP) is primarily responsible for police training. The criminal investigation college in

Zutphen forms part of the LSOP. This college possesses all the necessary didactic and technical qualities. However, the new course aimed at card issues is developed and given by visiting lecturers. These visiting lecturers are drawn from various disciplines and give the courses significant added value. The Central Criminal Information Department (CRI) also makes an important contribution to the new training courses. The development of teaching material in the area of cards is hindered to some extent by the dynamic period in which the graphics industry presently finds itself. Conventional graphical techniques will have to make way for digital applications. The accessibility, quality and cost price of this digital equipment are aspects that have developed emphatically in the favour of the forger.

Conclusion

A notable feature of present developments in chip and smartcard technology is that the IT (Information Technology) side of the card continues to be used to indicate the amount of attention paid to security or its level. The authors of this article, however, take the view that the IT aspect is only a part of the overall security. The value and the level of the security are determined by the overall concept.

Cards should be divided into categories according to their application. The categories can then be taken as an indication of the security level.

A card that is attributed a recognised identification function by the government will have to be placed in the highest category. Biometry could function as a standard security feature of cards in the highest category. The use of biometry is an important weapon in the fight against the misuse of cards, and accordingly against crime.

Sources

1. Fraudepreventie, handboek tegen bedrog en malversatie bij bedrijven en overheid. ['Fraud prevention, handbook against deception and embezzlement'] Edited by: P.C. van Duyne, L.H.J.M. Sloesen RA, A. van Vliet and A. Wielenga.
2. Identiteitsvervalsing, ['Identity falsification'] part 4 of the criminal investigation reference book series. Edited by A. van Vliet, A. Knopjes and J.M.J Broekhaar.
3. CardTech/SecurTech, proceedings of the Card and Security Technology Conference 1996 and 1998.
4. Cheating at cards RMPD, by Bryan Clough
5. Card Fraud the threat to payment profitability by John Newton, Laffety publications Dublin 1996.
6. Materieel strafrechtelijke aspecten creditcard fraude, ['Substantive criminal

aspects of credit card fraud'] Mr. J. Wotte (a thesis).