ARTICLE:

CIVIL LAW LIABILITY FOR UNAUTHORIZED WITHDRAWALS AT ATMs IN GERMANY

By **Assistant Professor DDr. Gerwin Haybäck**

The liability for unauthorized withdrawals at automatic teller machines (German: Geldautomat; Austria: Bankomat) (ATMs) and point of sale terminals (POS) is caused by the manipulations of unauthorized third parties, sometimes because of the incautious behaviour of the cardholder, where the loss of a card is exacerbated as a result of the PIN being recorded with the card in some way. The bank may also refrain from taking precautions, such as providing an effective shield to terminals, refusing to record a transaction with the use of video or CCTV,[1] and failing to provide for increased program code and internet safety. The aim of this article is to discuss what can be considered a fair allocation of risks. It deals with system security and different methods exercised by criminals in order to detect the personal identification number (PIN). The prima facie evidence granted in favour of the bank is a controversial issue discussed in relation to substantive law and case law.[2]

Introduction

The first time a card holder may become aware that an unauthorized transaction might have occurred at an ATM or POS, is when they notice an unknown debit posting on their current account.[3] Accordingly, the card holder will probably inform the card issuer that the posting is an unknown withdrawal against their account, and the debit should be refunded.

The card issuing bank, on the other hand, will probably respond by pointing out that only the card holder knew the PIN, which can be four numbers (as in the UK for instance) or four or five numbers (as in Germany for instance). This means it is assumed that the card holder has complete control over the card (also known as bank card, payment card, bank customer card, debit card). The card issuer may well reach the conclusion that either the card holder must have withdrawn the respective amount at the ATM, or they authorized a third person so to do, or they were so negligent as to permit an unauthorized third person to obtain possession of the card and PIN. Where the card holder loses control over their PIN or card, or both PIN and card, it may be that third persons have obtained the card and discovered the PIN, then they attempt to remove as much cash as possible before the card is retained. Whatever happens, the law of evidence and how the pleading are drawn up will be of great importance in establishing which party is put to proof to prove their case.

Occasionally, a criminal will obtain possession of several charge or credit cards, and within a short period of time, the maximum amount is removed because the criminals know that the card is blocked only after two (or more) hours.[4] The card issuer notices the theft only after some time.[5] Consequently, the ATM card is frequently blocked too late. Therefore, it is important to establish

[1] *Although a video recording of a transaction does not prove anything if the ATM clock and video clock are not synchronized, for which see a murder case where the wrong people were arrested in the USA in Stephen Mason, editor, Electronic Evidence: Disclosure, Discovery & Admissibility (LexisNexis Butterworths, 2007), 3.20-3.22.*

[2] *Prima facie evidence in Germany is similar to a presumption in English jurisprudence.*

[3] *See in detail Gerwin Haybäck, Risikohaftung bei missbräuchlichen Bankomatbehebungen: Ein österreichisch-deutscher Rechtsvergleich (Neuer Wissenschaftlicher Verlag GmbH Nfg KG, 2008), 45 and following.*

[4] *See the report: 'Bankomat: Kartensperre schützt nicht' ('ATM: Card blocking does not protect'), available at: http://www.klartext.at/downloads/presse/bankomat kartensperre nuetzt nicht.PDF.*

[5] *Note by editor: card issuers purport to have mechanisms in place to detect fraud of this nature, so if a card issuer fails to implement the mechanism where large amounts are removed from an account that is not within the normal spending patter of the card holder, the fault may be with the card issuer, not the card holder. Fraud detection is a pattern recognition problem and it can be carried out either using expert systems where people write the rules, or training a system by providing data, and for it to establish the rules. However, detecting fraud is far more complex. It is necessary to consider what types of fraud are known, then to be alert to a change in fraud patterns that avoid the previous patterns, then when new patterns are detected, the new patterns must be countered. It is necessary to understand that in attempting to detect fraud, the early cases of a new type of fraud may not be detected for some time. A significant problem when dealing with allegations that a customer is responsible for a withdrawal from an ATM, is that nobody in this field will explain what they are looking for, or publishes any analysis on how good they might be at identifying patterns of fraud.*

criteria for the distribution of risks and charges between the contracting parties. The allocation of risks concerning the damages caused by third parties is of importance, especially if the offender is unknown or has no assets when caught and successfully prosecuted. On the one hand the card holder is obliged to use the two components (card and PIN) together. On the other hand, the card holder always has to keep the two components strictly separated for security reasons. The most frequent attacks are to manipulate an ATM, or to create a cloned card. Occasionally, criminal energy focuses upon discovering secret numbers.

Concerning the substantive law of contract, it is necessary to determine the duties of care the card holder is required to comply with. Second, consideration must be given to the standard of care and security that should be the responsibility of the credit services sector. This article primarily deals with the security of the PIN system. In addition, the question of liability concerning the PIN (as the present electronic instrument of identification) is discussed. The analysis deals with the liability for damages in civil law, not criminal law.

Liability and the German EC system

The German EC ATM system is a participant of the European Europay ATM system and the Global Maestro system.[6] There arrangements permit transnational withdrawals at ATMs and POS payments for goods and services. When the EC card (including the Maestro logo as well as the electronic cash logo) is used at an ATM, a legal transaction takes place within the single mandate between the card holder and the card issuer. In accordance with section 665 of the German Civil Code (Bürgerliches Gesetzbuch), these mandates comply with the authority to make a payment from the account of the card holder:

> § 665 Abweichung von Weisungen
>
> Der Beauftragte ist berechtigt, von den Weisungen des Auftraggebers abzuweichen, wenn er den Umständen nach annehmen darf, dass der Auftraggeber bei Kenntnis der Sachlage die Abweichung billigen würde. Der Beauftragte hat vor der Abweichung dem Auftraggeber Anzeige zu machen und dessen Entschließung abzuwarten, wenn nicht mit dem Aufschub Gefahr verbunden ist.
>
> Section 6654[7]
>
> Deviation from instructions
>
> The mandatary is entitled to deviate from the instructions of the mandator if he may assume in the circumstances that the mandator would approve of such deviation if he were aware of the factual situation. The mandatary must make notification to the mandator prior to such deviation and must wait for the decision of the latter unless postponement entails danger.

The EC card is a payment (debit) card, in accordance with the provisions of section 676h of the German Civil Code. Subsequently, the card issuing bank is entitled to demand reimbursement of expenses for use of a payment card only where it was not abused by a third party. Apart from the possibility of excluding claims for expenses, there still remain the card issuer's claims for damages against the card holder, in accordance with the general regulations (sections 280 and 281 of the German Civil Code).

Risks associated with the PIN

Methods to detect the PIN

As the result of the experience with ATM systems at the time of writing,[8] it is known that taking cash out of a bank account at ATMs is much safer than relying on the cheque guarantee card system.[9] Experienced criminals can forge a signature in such a way that the average recipient of a cheque cannot discover the deception.[10]

An unauthorized withdrawal using the correct PIN is a forgery, although it follows that the PIN itself can be only correct or incorrect. Card issuers fail to understand this logic, and therefore it is incorrectly assumed that

[6] *The agreement was concluded between the Federal Association of the German Volksbanken and Raiffeisenbanken, the Federal Association of the German Banks, the German Sparkassen- and Giroverband as well as the Federal Association of Public Banks of Germany (all of them incorporated societies), in force from 1 December 2003; see Karsten Schmidt, Zu E. Bankkartenverfahren; 1. Vereinbarung über das deutsche ec-Geldautomatensystem, in: Münchener Kommentar zum HGB (Handelsgesetzbuch is the Commercial Code), 2nd edition, (beck on-line, 2009).*

[7] *Translation taken from http://bundesrecht.juris.de/englisch_bgb/index.html.*

[8] *The history of the eurocheque system is covered in Ewald Judt and Alfred Scholz, 35 Jahre Geldausgabeautomat – 20 Jahre Bankomat in Österreich, ÖBA (2000) 839.*

[9] *For contributions that deal with the advantages and disadvantages of the eurocheque system, see Ewald Judt, Der eurocheque: 1968 – 2001 – ein Nachtrag, ÖBA (2003) 136; fundamentally Gerwin Haybäck, Zur Risikoverteilung bei Euroscheckfälschung, ÖBA (1997) 251.*

[10] *Michael Bucher, Die Risikoverteilung bei der Benutzung elektronischer kartengesteuerter Zahlungssysteme, (P. Lang, 1992), 180; Günter H. Roth, Grundriß des österreichischen Wertpapierrechts, Wien: Manz, 2nd edition (1999) 85 and following: checking the signature on forged EC cheques.*

Where a third person obtains the PIN, it is assumed that the card holder has been engaged in careless behaviour, despite the ease by which a PIN can be obtained by a third person.

the card holder has a duty of care to prevent the passing of the PIN to third persons. Where a third person obtains the PIN, it is assumed that the card holder has been engaged in careless behaviour, despite the ease by which a PIN can be obtained by a third person. The PIN is the most important identifier of the (authorized) card holder at ATMs and POS terminals. Card holders are contractually bound to keep the PIN safe, and are not entitled to inform anybody voluntarily of the PIN.[11] This requires a discussion as to how a third person is able to detect the correct PIN. The three most frequent causes are breach of secrecy, spying to obtain the PIN, and guessing the PIN.

Breach of secrecy

The card holder has a contractual duty to take care of their card and PIN. The issue is to establish what those duties might be. Both the prevailing opinion as well as the conditions for the use of the Maestro Card oblige the card holder to keep his PIN confidential and never pass the PIN to others.[12] In particular, the PIN must not be noted on the card or otherwise stored together with it, even in an altered form.[13] Should the card holder keep the Maestro card and code close together, they undermine an important component of the Maestro safety system.[14]

In 1999, it was held by the Local Court in Hamburg that keeping the EC card in the hip pocket of a pair of trousers (without carrying the secret number) was not regarded a grossly negligent violation of the duty to care.[15] 'Saving the EC components separately'[16] means keeping them in different boxes, pieces of furniture and locked drawers,[17] or in different pockets of items of clothing.[18]

The Local Court in Kassel has determined that it is extremely careless behaviour to keep a note of the PIN in an address book together with the ATM card.[19] Such behaviour is in conflict with the strict duty of secrecy stipulated in the conditions for the use of the Maestro Card, in accordance with the prevailing case law. This method of concealing the PIN is well-known by criminals.[20] However, in the opinion of Professor Udo Reifner, such behaviour cannot be considered unreasonable. It is usual for a person to make a permanent record of the PIN for the purposes of an aid to memory. Further, he also approves the transmission of the PIN to persons of trust.[21]

Nevertheless, if the card holder fails to notice the loss of an ATM card by taking money out or placing money, account statements, and the ATM card carelessly into the pocket of a coat or jacket, such behaviour is considered as grossly negligent, in accordance with a decision by the District Court at Halle.[22]

The requirement of isolating the card in a safe is out of touch with everyday life. On the one hand, the card holder acts grossly negligently if he is absent for three or four hours while leaving the card and the PIN on the

[11] *In contrast, concerning to the duty of secrecy, the card holder only has to afford a reasonable, i.e. conventional duty of care (in German: 'zumutbar', what can be expected of an average card holder). Full particulars are discussed by Stefan Werner in Thorwald Hellner and Stephan Steuer (editors), Bankrecht und Bankpraxis, (2008) Rz 6/1463.*

[12] *Although informing others of the PIN seems to be practiced in particular between family members, nevertheless the prevailing opinion is strictly against any transfer of the PIN, for which see Franz Häuser and Lutz Haertlein, E. Bankkartenverfahren, in Münchener Kommentar zum HGB, 2nd edition, (beck on-line 2009) Rn E 33 and following; likewise Ernst Heymann, Norbert Horn, and Peter Balzer, Handelsgesetzbuch (Commercial Code), 2nd edition, (2005) section 372 annex; Adolf Baumbach, Wolfgang Hefermehl, and Matthias Casper, Wechselgesetz, Scheckgesetz, Recht der kartengestützten Zahlungen, 23rd edition (2008) Rn 36; Wolfgang Gößmann, Aspekte der ec-Karten-Nutzung, WM (1998) 1264, 1269; Viola Russenschuck, Die Auszahlung von Bargeld an Automaten nach deutschem Zivilrecht (2002) 75 and following; for dissenting views, see Christian Hofmann, Schadensverteilung bei Missbrauch der ec-Karte, WM (2005) 441, 444 and Professor Dr. Udo Reifner, Die Haftung des Kontoinhabers bei Missbrauch seiner Bankomatkarte durch Dritte, BB 1912, 1918.*

[13] *Stefan Werner, Verantwortlichkeit bei missbräuchlicher Verwendung der ec-Karte unter Eingabe der richtigen PIN, BKR (2004) 50.*

[14] *Wolfgang Gößmann, Aspekte der ec-Karten-Nutzung, WM (1998) 1264, 1269.*

[15] *Local Court Hamburg, VuR (1999) 88.*

[16] *BGH WM (2000) 2421, 2422.*

[17] *Wolfgang Gößmann, Aspekte der ec-Karten-Nutzung, WM (1998) 1269, referring to District Court Essen, WM (1988) 493 and District Court Hanau, ZIP (1995) 559.*

[18] *Wolfgang Gößmann, Aspekte der ec-Karten-Nutzung, WM (1998) 1269, referring to Local Court Hannover WM (1996) 2013.*

[19] *Local Court Kassel, I D 5. b – 1. 95 WuB, Pfeiffer.*

[20] *Local Court Kassel, WM (1994) 2110; see Stefan Werner in: Thorwald Hellner and Stephan Steuer (editors), Bankrecht und Bankpraxis, (2008) Rz 6/1470; Horst Ahlers, Die neuen Bedingungen für ec-Karten, WM (1995) 601, 607; dissenting Hartmut Strube, Haftungsrisiken der ec-Karte, WM (1998) 1210 and following.*

[21] *Professor Dr. Udo Reifner, Die Haftung des Kontoinhabers bei Missbrauch seiner Bankomatkarte durch Dritte, BB (1989) 1912 and following.*

[22] *District Court Halle, WM (2001) 1298.*

In order to provide for the safety of the maestro system, the credit services sector promotes the physical shielding of the front of ATMs, as well as a nationwide development of video control at each ATM.

desk in his flat,[23] or if he keeps both components in a folder.[24] However, the card holder is entitled to physically carry the card as well as the PIN. On the other hand, the PIN must not be written down on the card or otherwise stored together, to avoid a thief obtaining the PIN if the card is stolen.

In what is known at the 'Hospital case', the court made high demands on the safe keeping of the card and PIN. It was determined that keeping the card with the PIN (camouflaged as a four-digit telephone number) was a grossly negligent contributory cause that allowed a third party to obtain unauthorized access to the account. The card holder was not exculpated by putting both components (card and code) into a solid strong box in a locked sick room. It is a matter of fact that a hospital is considered an unsafe location where the theft of such items cannot be excluded.[25]

The cumulative effect of judicial pronouncements indicates that it is necessary to keep the components (card and PIN) strictly separated, even in private rooms. According to a recent judgement of the Federal Court of Justice of Germany (Bundesgerichtshof, BGH), the customer does not act grossly negligent if they keep the card and PIN in different rooms of a flat, and, as a result, unauthorized, abusive withdrawals follow.[26] Within the domestic arrangements of a family home, it is not necessary to take measures against theft between family members where the relationships between family members are in good order, and if the card issuer does not request special protective measures to be put in place caused by any specific circumstances the family might find themselves in. Examples where the card issuer might consider that there are special circumstances that require additional consideration for security are flat-sharing communities or residential homes where family members are not present.

In a recent judgment of the Higher Regional Court of Düsseldorf, it is considered to be grossly negligent if a purse containing the card is placed in a shopping trolley in a department store.[27]

Observing the PIN by third parties

It is possible to differentiate between active and passive observation of the PIN.[28] The most common method is passive observation, such as looking over someone's shoulder, especially at ATMs in busy places or at POS terminals in supermarkets. Criminals will go to the length of renting flats across from ATMs for this purpose. Thus, they take possession of different PINs by using binoculars, telephoto lens, mini-spy-cameras, or by transmitting the PIN to an external personal computer where the ATM has been manipulated by the criminal to obtain the PIN when the PIN is entered into the ATM.

In order to provide for the safety of the maestro system, the credit services sector promotes the physical shielding of the front of ATMs, as well as a nationwide development of video control at each ATM.[29] On the other hand, the card holder is obliged to take reasonable precautions. If the card holder takes cash out of the bank account at ATMs, or makes payments at POS terminals, they have to stay away from the next customer, protect the number pad, and such like.[30]

It is possible to fabricate a clone of the card and take cash out of the victim's bank account at an ATM in a foreign country if a criminal obtains sufficient information from the card and knows the correct PIN.

[23] *District Court Frankfurt 1. December 1992, 2/13 ol 98/92.*
[24] *Higher Regional Court of Nürnberg WM (1989) 405; Stefan Werner in Thorwald Hellner and Stephan Steuer (Ed), Bankrecht und Bankpraxis, (2008) Rz 6/1470.*
[25] *District Court Bonn, NJW-RR (2000) 1415.*
[26] *Federal Court of Justice of Germany, NJW (2001) 286.*
[27] *Higher Regional Court of Düsseldorf, BKR (2008) 41.*
[28] *Professor Dr. Manfred Pausch, Risiken im automatisierten Verkehr mit Magnetstreifen, VuR (1997) 121, 124; Professor Dr. Manfred Pausch, Die Sicherheit von Magnetstreifenkarten im automatisierten Zahlungsverkehr, CR (1997) 174.*
[29] *Various authors demand an obligation of the banks to provide an area-wide video control of ATMs, see Professor Manfred Pausch, Risiken im automatisierten Verkehr mit Magnetstreifen, VuR 1997, 121 (123); Stefan Werner in Thorwald Hellner and Stephan Steuer (Ed), Bankrecht und Bankpraxis, (2008) Rz &/1481.*
[30] *Professor Dr. Manfred Pausch, Risiken im automatisierten Verkehr mit Magnetstreifen, VuR (1997) 124; Werner Schindler, Die neuen PIN-Nummern der ec-Karten, NJW-CoR (1998) 223, 226; Stefan Werner in Thorwald Hellner and Stephan Steuer (Ed), Bankrecht und Bankpraxis, (2008) Rz 6/1469.*

The information, but not the PIN, can be obtained from the magnetic stripe on the reverse of the card. From 1982 on in Germany, detectors for an anti-fraud feature known as the Moduliertes Merkmal (MM code) began to be installed in ATMs, in order to provide protection from cloned cards.[31] The MM code consists of two components, one stored on the magnetic stripe, and one hidden within the material of the card. The MM code is verified by the ATM with a cryptographic operation that is performed to check that the component of the MM code on the magnetic stripe corresponds to the one hidden on the card. The correct hidden component of the MM code cannot be calculated from the information recorded on the magnetic stripe alone. It is also necessary to have a cryptographic key, which is stored in the MM code detection unit. ATMs in Germany include a special MM detection unit and sensor to read and verify the MM code, although cash machine manufacturers are not permitted to obtain access to or service the unit.

The prevailing case law indicates that it is considered as grossly negligent behaviour where the customer fails to realize the loss of the card by taking money out, then putting the money, account statements, and card into a coat pocket. The same consequences apply where the customer does not protect the number pad.[32] Generally, the card holder has to take reasonable care. The mere fact that the offender knew about the PIN is not sufficient to prove the card holder's breach of his duty to care.[33] In other reported cases, the chance of observing a different secret number is mentioned, but was excluded in the case under consideration.[34] On one occasion, the District Court in Berlin formally criticized the lack of safety screening devices. In this case, the criminals had detected the secret number and thereupon pursued the card holder through Berlin. In the view of the court, the card holder is not at fault if she does not pay attention to people around during the time it takes to make the withdrawal.[35]

To this end, Dr. Tilman Hoppe proposes the following: 'First of all, the banks as well as the participants of the POS system are requested to redesign the conditions in such a way that is not possible to spy out the PIN. Especially, the screen of the key pad at POS terminals in trade seems inadequate in case of large crowds. It should be taken into consideration whether the identification of the customer is carried out as it is the case with the POZ system.'[36] Hoppe draws the conclusion that the bank is obliged to prove that the respective ATM is not protected at best. Measures of improving the shield of the number pad are required, especially in superstores.[37]

It is debatable whether Hoppe's proposal is acceptable: 'to deliberate about whether in trade the identification of the customer should take place as it is the case with the POZ system.'[38] This comment is in conflict with a long experience in providing for the security for withdrawals at ATMs in comparison with those of the eurocheque system. With good cause, the eurocheque as well as the (former) POZ system were suspended (in 2001, respectively in 2007), because it was easy to forge the manuscript signature but impossible to detect whether the correct secret number, if used, was used by the card holder, and not an unauthorized third party. The PIN system is arguably much more secure than payment instruments using the signature to authorize the customer, because of the cryptographic controls in place.[39] Since 2006, the credit services sector has refused to accept the risks of forgery in connection with the POZ system based on the manuscript signature of the customer.[40]

In 2003, the Local Court in Dortmund reached the conclusion that there is no empirical deduction providing that the card holder must have caused unauthorized withdrawals from an ATM in a grossly negligent way, where they retained the card with the PIN, or noted the PIN on the card where it was stolen from a rucksack.[41] In contrast to the view of the Higher

[31] *Manfred Lochter and Werner Schindler, Missbrauch von PIN-gestützten Transaktionen mit ec- und Kreditkarten aus Gutachtersicht, MMR (2006) 292, 294. Concerning the risk of forging bank cards in Austria, see Gerwin Haybäck, Haftungsfragen bei Totalfälschung der ec-Karte, wbl (1999) 56.*

[32] *District Court Halle, WM (2001) 1298.*

[33] *Local Court Buchen VuR (1998) 42. The risk of observing the PIN is not mentioned in the following: District Court Hannover, WM (1998) 1223; Local Court Dinslaken, WM (1998) 1126; Local Court Osnabrück, WM (1998) 1227; Local Court Charlottenburg, WM (1998) 1224.*

[34] *Local Court Wildeshausen, WM (1998) 1128; District Court Bonn, WM (1995) 575; Local Court Frankfurt, CR (1998) 723.*

[35] *District Court Berlin, ZBB (1999) 85.*

[36] *In German, Dr. Tilman Hoppe, Anscheinsbeweis bei Ausspähen der PIN, ZBB (1999) 88 (93) proposes: 'Zunächst sind die Banken wie auch die Teilnehmer am POS-Verfahren im Handel gehalten, die Bedingungen bei der Eingabe so zu gestalten, dass ein Ausspähen nicht möglich ist. Besonders der Sichtschutz der Eingabetastaturen im Handel erscheint im Falle unübersichtlichen Gedränges allzu dürftig. Es wäre dringend zu überlegen, ob im Handel die Legitimation des Kunden nicht ausschließlich durch Unterschrift geschehen sollte, wie bisher schon im sogenannten POZ-Verfahren.'*

[37] *Dr. Tilman Hoppe, Anscheinsbeweis bei Ausspähen der PIN, ZBB (1999) 88 (93).*

[38] *POZ system means point of sale without guarantee of payment by using EC card plus a manuscript signature (without a PIN); Dr. Tilman Hoppe, Anscheinsbeweis bei Ausspähen der PIN, ZBB (1999) 93, referring to Ulrich Häde, Die Zahlung mit Kredit- und Scheckkarten, ZBB (1994) 33, 41.*

[39] *Gerwin Haybäck, Risikohaftung bei missbräuchlichen Bankomatbehebungen: Ein österreichisch-deutscher Rechtsvergleich, (2008) II.D.3, p 96 and following; to EC liability Gerwin Haybäck, ÖBA (1997) 256 and following.*

[40] *Stating that the former POZ system was 'highly susceptibel (in German: "anfällig") to misuse': Wolfgang Gößmann, § 68: ec-Kassen und POS-System (Point-of-Sale). GeldKarte, in: Herbert Schimansky, Hermann J. Bunte, and Hans-Jürgen Lwowski, Bankrechts-Handbuch, Bd 1, 3rd edition (2007) marginal number 12, 13.*

[41] *Local Court Dortmund, BKR (2003) 912.*

Regional Court of Frankfurt,[42] most of the cases show that obtaining the secret number is not to be considered as absurd and only a theoretical possibility.

According to a recent decision of the Austrian Supreme Court (OGH), the card holder is not liable for withdrawals caused by unauthorized third parties where he keeps the card and PIN safe. In this case, the card holder took out 90 Euro from an ATM. When doing so, he not aware that he was being observed by an unknown person. The card holder protected the key pad against observation from behind with the upper part of his body. After the withdrawal, the customer put the money and the card into a wallet, and the wallet into the main pocket of his rucksack, which he then placed on his back. He was followed by the thief, who stole the card in the underground. When the card holder noticed the theft, he initiated the block of the card. However, 310 Euro (the original 90 Euro plus a further withdrawal of 310 Euro meant the maximum of 400 Euro maximum was reached because that was the maximum for any withdrawal a day) were withdrawn by an unauthorized third person. The Austrian Supreme Court (OGH) decided that the card holder did not breach his duty of care. It was determined that he was not obliged to take additional measures against criminals, such as protecting the key pad with the second hand or shielding it from lateral observation. In contrast to the court of appeal, who considered it as negligent behaviour because of the fact that the card holder had worn the rucksack on his back and had therefore lost the sight of the zip, the Austrian Supreme Court stated in this case that the safekeeping of the card enclosed in the main pocket of the card holder's rucksack was performed according to his duty to care. As a consequence, the bank lost the appeal.

As a result, the court drew the conclusion that it is sufficient to put a purse into a closed rucksack that is worn on the back, and to protect the number pad with the upper part of the body, even if the purse and card disappear from the customer's sight.[43]

Guessing or calculating the PIN

At the time of implementation of the ATM PIN system, it was only considered an academic question whether unauthorized third parties were able to find out the PIN, because of the marginal probability of 0,03 per cent.[44] It is generally accepted that the Data Encryption Standard (DES), which was applied until the end of 1997, was considered cryptographically secure.[45] Randomizing the code using conventional means was considered impossible. In 1992, the Higher Regional Court of Berlin considered the PIN code secure, in reference to statements of the Federal Office for Security and Information Technology. Regarding the guessing or randomizing the PIN code at that time, the Federal Office acted on the assumption of 72 quadrillion alternatives.[46]

However, this judgment was overturned by the rapid development of the semiconductor technology. In 1994, experienced criminals would have required 1900 years to find out a PIN. Three years later, they would only have needed 96 days, shortly after only 19 days, since 1999 no more than 24 hours.[47] Thereafter, a decision of the Higher Regional Court of Hamm initiated a serious discussion as well as major doubts about the cryptographic safety of DES used until the end of 1997. In this now famous case, the court refused to grant a prima facie evidence in favour of the bank. It was possible that the criminal could have decoded the PIN by using the data recorded on the ATM card. As a consequence, the customer won the case.[48]

As a result, the cryptographic system was updated and replaced by the Triple Data Encryption Algorithm (TDEA). New, regionally generated PINs have been distributed, and an on-line network has been established.[49] Thus, the credit services sector improved the safety of the system against external attacks. Nevertheless, several judgments in favour of the card

[42] *Higher Regional Court of Frankfurt, WM (2002) 2101.*

[43] *The 'Rucksack' decision of 2 February 2007, in: ÖBA 2007/1424 (OGH). Consenting Georg Graf, Wer haftet beim Bankomatkartenmissbrauch? Anmerkungen zu einem aktuellen OGH-Urteil sowie den Auswirkungen des Transparenzgebotes auf die Auslegung von AGB, ÖBA (2007) 531 and following.*

[44] *The Higher Regional Court of Berlin (German: Kammergericht), case: WM (1992) 729, relied on a statement from the Federal Office for Security and Information Technology (Bundesamt für Sicherheit in der Informationstechnik) for this figure of the margin of probability.*

[45] *Concerning the safety of the PIN cp. Manfred Lochter and Werner Schindler, Missbrauch von PIN-gestützten Transaktionen mit ec- und Kreditkarten aus Gutachtersicht, MMR (2006) 292 and following. Referring to the former DES PIN system, see the US study at http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf: A DES key consists of 64 binary digits (0s or 1s) of which 56 bits are randomly generated and used directly by the algorithm.*

[46] *Federal Office for Security and Information Technology (Bundesamt für Sicherheit in der Informationstechnik). For the judgment mentioned above, see Higher Regional Court of Berlin, WM (1992) 729.*

[47] *The detailed report of 19 January 1999 is available at: http://www.heise.de/tp/deutsch/inhalte/te/1771/1.html.*

[48] *Higher Regional Court of Hamm, NJW (1997) 1711 and following. To the safety of the former PIN system, sceptically Professor Dr. Werner Schindler, Ec-Karten: Wie sicher ist die PIN-Nummer?, NJW-CoR (1997) 284; Hans-Jürgen Stenger, Zur Kritik an der Annahme einer Errechenbarkeit einer PIN, CoR (1997) 363 and following.*

[49] *Hartmut Strube, Haftungsrisiken der ec-Karte, WM 1210 (1998). In respect of the question of the safety of the PIN, see Johannes Köndgen, Die Entwicklung des privaten Bankrechts in den Jahren 1999-2003, NJW (2004) 1288.*

holder were delivered.[50] For example, the Local Court at Duisburg reached the conclusion that PIN codes could be decoded by ordinary card readers. Even the RSA-155-Code (512-bit numbers in the code have about 155 decimals) used in internet transactions (SSL protocol) was cracked. Although it is admitted that some withdrawals at ATMs are performed by using stolen payment cards, this does not necessarily imply grossly negligent behaviour on the part of the customer.[51]

On the other hand, there are still decisions in favour of the prima facie evidence of ATM withdrawals that either the card holder has withdrawn the money, or he has not kept the secret number safe.[52] The Higher Regional Court of Hamm mentioned several methods of manipulation, such as card reader, frequency of certain number combinations, switching off the 'faulty operation counting function' in the card by technical manipulation,[53] and others. However, in Germany, off-line systems have not been in use since 1997.[54] From that time on, the prima facie evidence could not be countered by the possibility that criminals discovered the PIN.[55] The Federal Court of Justice of Germany felt confident that the security architecture of the Triple Data Encryption Algorithm (TDEA) system practiced since 1997 is safe. For this reason, the court has imposed significant demands on the customer whenever the latter has attempted to counter the prima facie evidence in favour of the bank.[56]

Prima facie evidence in favour of the bank – a controversial issue

In contrast to other payment instruments, such as the cheque, specific problems of evidence arise from the ATM PIN system, because of the anonymous communication process. If it is impossible to find out who executed the withdrawal at issue, it is necessary to begin the investigation with what is meant by a legally performed electronic payment process. If the bank was legally obliged to furnish full proof, it would result in insoluble difficulties.

The prevailing judicial opinion is that the prima facie evidence is granted in favour of the bank. This is proper evidence which is equated to formal evidence. The prima facie evidence comes into action in case of formal and typical events. According to experience, the circumstances of the case must either indicate only one cause or one definite process.[57] Exercising prima facie evidence is based on the assertion that the decoding of the PIN is impossible at short notice. The prima facie evidence rests upon the mutable experience of life, as well as technological progress.

Therefore, the use of the EC (ATM) card in connection with the PIN establishes the ground for prima facie evidence that either the card holder himself withdrew the respective amount at the ATM, or enabled the unauthorized withdrawal by grossly negligent behaviour.[58] Regarding unauthorized transactions caused by third parties, the customer is required to report abnormal events described in a plausible, precise, and substantial manner, should he intend to counter the prima facie evidence. In accordance with the provisions of section 670 of the German Civil Code, only where the customer succeeds in reporting such evidence in substance, will a claim for disbursement not be granted to the bank:[59]

§ 670 Ersatz von Aufwendungen

Macht der Beauftragte zum Zwecke der Ausführung des Auftrags Aufwendungen, die er den Umständen nach für erforderlich halten darf, so ist der Auftraggeber zum Ersatz verpflichtet.

Section 670

Reimbursement of expenses

If the mandatory, for the purpose of performing the

[50] *Local Court Hamburg, VuR (1999) 88; Local Court Frankfurt, WM (1999) 1922; Higher Regional Court of Stuttgart, NJW-RR (2002) 1274.*

[51] *Local Court Duisburg, JurPC Web-Dok (1999) 197, Abs 1 – 15; cracking the RSA-155-Code, see http://igw.tuwien.ac.at/fit/2001/fit05/sicherheit/der_rsa_algorithmus.html.*

[52] *District Court Stuttgart, WM (1999) 1934; Local Court Dinslaken, WM (1998) 1126, referring to: Local Court Hannover, WM (1997) 1207; Local Court Wuppertal, WM (1997) 1209, against Higher Regional Court of Hamm, NJW (1997) 1711. Likewise the side proceeding of this case, see District Court Darmstadt VuR (2000) 357; Rolf Aepfelbach and Gerd Cimiotti, Zur Sicherheit des ec-Kartensystems, WM (1998) 1218 and following.*

[53] *The Federal Office for Security and Information Technology considered the possibility of switching off the 'faulty operation counting function' in the card by technical manipulation as an 'annoying issue', for which see Werner Schindler, Die neuen PIN-Nummern der ec-Karten, NJW-CoR (1998) 223, 224.*

[54] *Stefan Werner, Anscheinsbeweis und Sicherheit des ec-PIN-Systems im Lichte der neuen Rechtsprechung, WM (1997) 1516.*

[55] *Local Court Frankfurt, NJW (1998) 687; Local Court Osnabrück, WM (1998) 1127.*

[56] *Federal Court of Justice of Germany, NJW (2004) 3623; expressively confirmed two years later, Federal Court of Justice of Germany, NJW (2007) 593.*

[57] *Federal Court of Justice of Germany, NJW (1996) 1828; (1997) 528. Taking of evidence in the view of the experts, cp. Manfred Lochter and Werner Schindler, Missbrauch von PIN-gestützten Transaktionen mit ec- und Kreditkarten aus Gutachtersicht, MMR (2006) 297.*

[58] *District Court Köln, WM (1995) 976; Local Court Diepholz, WM (1995) 1919; Local Court Schöneberg, WM (1997) 55; Local Court Hannover, WM (1997) 64; Local Court Frankfurt, WM (1995) 880; Local Court Wuppertal, WM (1997) 1209; Local Court Hannover, WM (1997) 1207; Local Court Charlottenburg, WM (1997) 2082; Stefan Werner, Beweislastverteilung und Haftungsrisiken im elektronischen Zahlungsverkehr, MMR (1998) 232 and following; Wolfgang Gößmann, Aspekte der ec-Karten-Nutzung, WM (1998) 1269.*

[59] *Dr. Tilman Hoppe, Anscheinsbeweis bei Ausspähen der PIN, ZBB (1999) 89; BGH NJW (1979) 1964; BGH WM (1979) 417.*

mandate, incurs expenses that he may consider to be necessary in the circumstances, then the mandator is obliged to make reimbursement.

This may be the case if the card holder has demonstrably not been at the place of the events (that is, at the physical location of the unauthorized withdrawal at the ATM or POS terminal) at the time in question; if the ATM card was lost before the withdrawal; if a video recording suggests another conclusion, or if fingerprints on the retracted card are not those of the customer, or a manipulated faulty operation counter are detectable.[60]

Further, the ATM journal is of importance. The case law indicates that the correct documentation of a single payment by the ATM journal tape is considered as prima facie evidence that the ATM has paid out money in the amount of the documented sum.[61] In case an ATM does not dispense money at all or dispenses out too little, this may be a fault that is documented by the ATM journal. Time, place, sum, denomination, and data input are documented exactly, although it is possible but rather difficult to destroy the data of the ATM journal. The authenticity of a card is checked by the modulated feature (MM-Modul) in the ATM corresponding with the chip on the card. The module on the card is read by the bank, and data is exchanged between the card and the bank, and if this data is accepted by the bank, it provides sufficient evidence to the satisfaction of the bank to infer that the customer's card is physically in the ATM. This evidence is considered to be prima facie evidence that the customer's card was inserted in the ATM, and acts to demonstrate that a third person cannot have inserted a duplicate EC card in the terminal.

Given such evidence, it is for the customer to verify why atypical events are to be taken into consideration.[62] The jurisprudence concerning the prima facie evidence makes clear that, regarding electronic means of payment, there is a close connection of prima facie evidence and system security.[63] If prima facie evidence is to be accepted lawfully, it is necessary to assume the security of the system is functioning correctly.

The customer cannot merely carry out his duty to report the theft of a card and any subsequent misuse as a matter of fact. He is also required to make clear what the abnormal events are, and to described them.[64] As mentioned above, the Higher Regional Court of Hamm did not grant a prima facie evidence to the bank in 1997.[65] The court did not exclude the possibility that an unauthorized third person could have been able to find out the PIN by guessing or calculating it. This judgment is now in the minority, because it acts on the assumption that only the card holder knew the correct PIN, and the use of the correct PIN was not sufficient to prove the card holder's breach of his duty of care.[66]

Position of the Federal Court of Justice (BGH) and subsequent case law

Thereafter, the Federal Court of Justice of Germany decided a case in favour of the bank, in which a third person having stolen the payment card took 1000 Euro out of the ATM.[67] Considering the application of the 128 bit Triple Data Encryption Algorithm (TDEA) in 1997, the prima facie evidence suggested the fact that the thief noticed the PIN only because the card holder was negligent by keeping the secret number together with the ATM card. It was concluded that the claimant must have violated her duty of care by having recorded the PIN on the card or stored the latter together with the PIN. The Federal Court of Justice of Germany refused the alternative explanation of decoding the PIN, because this would be mathematically impossible. Although at the time of this case, there was no evidence put forward to indicate the code had been cracked. In the view of the court, purely theoretical possibilities to find out the PIN are not sufficiently suitable to disable the prima facie evidence. The result means there is no reason to obtain evidence regarding the system security. Obtaining the PIN by observation is only considered as a 'different' cause where the card is stolen in close connection with the respective ATM, at the same time the PIN was entered. In this instance, the card holder was not able to substantiate such circumstances.

In the view of Stefan Werner, the Federal Court of

[60] *Michael Bucher, Die Risikoverteilung bei der Benutzung elektronischer kartengesteuerter Zahlungssysteme, (Verlag P. Lang, 1992), 302.*

[61] *Herbert Schimansky, Hermann-Josef Bunte and Hans-Jürgen Lwowski, Bankrechts-Handbuch, (3rd edition, Verlag C. H. Beck München, 2007), 13-14.*

[62] *Gerwin Hayböck, Risikohaftung bei missbräuchlichen Bankomatbehebungen: Ein österreichisch-deutscher Rechtsvergleich, (2008) 156 and following.*

[63] *Stefan Werner, Beweislastverteilung und Haftungsrisiken im elektronischen Zahlungsverkehr, MMR (1998) 234 and following.*

[64] *Local Court Schöneberg, WM 66 (1997); Local Court Hannover, WM 64 (1997); Local Court Wuppertal, WM 1209 (1997); District Court Hannover, WM 1123 (1998); District Court Bonn, NJW-RR 815 (1995). In general Wolfgang Gößmann, Aspekte der ec-Karten-Nutzung, WM (1998) 1270.*

[65] *OLG Hamm, NJW (1997) 1711.*

[66] *Local Court Buchen, VuR (1998) 98; similiar District Court Frankfurt, VuR (1997) 423; District Court Frankfurt, VuR (1998) 162; District Court Dortmund, CR (1999) 556. Against it, the bank won the case, because the customer did not succeed in demonstrating the practical alternative of guessing or randomizing the PIN, Local Court Flensburg, VuR (2000) 131. Likewise: District Court Köln, WM (2001) 852.*

[67] *Federal Court of Justice of Germany, NJW (2004) 3623; consenting Jan Christian Eggers and Andreas Goerth, Die Haftung des Bankkunden für unbefugte Abhebungen mittels ec-Karte und PIN – BGH, NJW (2004) 3623; BGH JuS (2005) 492.*

The correlation between the theft of the card and the unauthorized withdrawals as mentioned by the Federal Court of Justice is somewhat ambiguous.

Justice stated that, at least if a card and PIN are used promptly at an ATM, the prima facie evidence argues for the fact that the card holder has noted the PIN on the card or stored it with the card. Certainly, this argument only applies if different causes regarding the misuse can be excluded, according to the experience of life.[68] This judgement was criticized by Christian Hofmann inasmuch as it has 'discharged the bank from responsibility although the bank is able to battle against failure of the payment system.'[69] Rightly, the Institute of Financial Services (Hamburg) emphasized the significant problems for the customer to counter the prima facie evidence under the prevailing circumstances.[70]

The correlation between the theft of the card and the unauthorized withdrawals as mentioned by the Federal Court of Justice is somewhat ambiguous. The prima facie evidence is granted to the bank at the expense of the card holder where the PIN is entered and at the first attempt at withdrawal succeeds within one hour after the theft of the card. This time is short, hence the explanation that the thief was able to decode the PIN by using technical instruments is excluded.[71]

The Federal Court of Justice of Germany confirmed the prevailing case law in a class action[72] initiated by a consumer advice centre.[73] In this case, a number of consumer claims of card holders were transferred to the Consumer Advice Centre of Nordrhein-Westfalen. By transferring the minor claims of 19 participants, a total of 13,500 Euro was claimed, due to cards being used by unauthorized third parties. The Federal Court of Justice decided that the Advice Centre of Nordrhein-Westfalen was a rightful claimant. In the interests of the consumer as well as for the public benefit, the judicial assignment for collection was considered to be necessary because it produces a more effective enforcement than any individual action. This is the case if there are circumstances preventing a person with the right to initiate an action, for example in the case of disproportionately high costs of the proceedings, or a high risk of litigation, or of practical problems of law enforcement.[74]

In this decision, the Federal Court of Justice confirmed the previous case law concerning the distribution of the burden of proof in case of misuse of stolen EC cards. The alternative of observing the PIN by a third party as a 'different' cause that only comes into question if the EC card was stolen and where it can be shown that it coincided with entering the PIN by the card holder at an ATM or POS terminal. The court convincingly emphasized the limits of the prima facie evidence. It is not possible for a customer to challenge a bank effectively until the safety standard of the electronic payment system is no longer granted to be authentic or genuine.

Conclusion

The distribution of risks between the EC card holder and the bank in case of unauthorized withdrawals at ATMs or POS terminals caused by third parties is closely connected with the safety standard of the electronic payment system. Despite the prevailing assertions of the safety of the system, courts always have to question if the current system grants a sufficient safety standard in order to apply the prima facie evidence in favour of the bank.

[68] *Stefan Werner, Verantwortlichkeit bei missbräuchlicher Verwendung der ec-Karte unter Eingabe der richtigen PIN, BKR (2004) 504 and following. Critically: Hartmut Strube, Verantwortlichkeit bei missbräuchlicher Verwendung der ec-Karte unter Eingabe der richtigen persönlichen Geheimzahl, BKR (2004) 497, 501 and following: ' The technical dispute concerning the PIN system, also a legal issue, will go on.' ,In Der technische Disput über das PIN-System, nicht eben ein urjuristisches Thema, wird also weitergehen' : BKR (2004) 501.*

[69] *Christian Hofmann, Schadensverteilung bei Missbrauch der ec-Karte, WM (2005) 441, 449 'den aus der Verantwortung entlassen hat, der Sicherheitslücken des Systems bekämpfen kann.'*

[70] *Institute of Financial Services (Hamburg) (Institut für Finanzdienstleistungen) (Hamburg), VuR (1998) 256.*

[71] *Local Court München, BKR (2005) 39.*

[72] *For that purpose, on 27 November 2008, the European Commission issued a Green Paper ' On Consumer Collective Redress' , Brussels, 27.11.2008 COM (2008) 794 final; Georg E. Kodek, Sammelklagen für Verbraucher: Ein neues Grünbuch der EU, ecolex (2009) 185.*

[73] *Consumer Advice Centre of Nordrhein-Westfalen (Verbraucherzentrale Nordrhein-Westfalen).*

[74] *Federal Court of Justice of Germany: NJW (2007) 593, 595 et seq. Likewise: Higher Regional Court of Frankfurt, Keine Anhaltspunkte für Sicherheitsmängel des PIN-Verschlüsselungssystems, MMR (2008) 473; Higher Regional Court of Karlsruhe 06. 05. 2008 - 2 O 16/07, BeckRS 15410 (2008).*

Further improvements to the security architecture of ATMs and POS terminals should be achieved. This refers, for example, to an effective shielding of the number pads, video control, increased program code and internet safety. The traditional magnet strips have to be replaced by highly effective computer chips. It is time for a world-wide improvement and the introduction of a secondary form of authentication, such as a biometric measurement of the fingerprint or other biometric measurements, such as user authorization with an iris scan.[75] For this purpose, several appropriate projects, such as 'FairPay', are provided by the German Research Centre for Artificial Intelligence.[76] To this end, banks, software developers as well as university departments dealing with the internet and safety technology, should work together.[77]

The costs may be high – but safety, particularly in the electronic age, is worth its price, especially if it ameliorates the anguish and suffering that people have to go through when money is taken from their bank account with authority.

Gerwin Haybäck, Dr. phil., Dr. iur, Assistant Professor at the Department of Business Law, University of Salzburg, Austria, is an author of several publications in the field of civil (consumer) law, commercial law, and intellectual property law. In April 2009 he won the Leopold Kunschak Scientific Award.

gerwin.haybaeck@sbg.ac.at
http://www.uni-salzburg.at/HWR/haybaeck.gerwin

[75] *Guiseppe Parziale and Reingard Riener-Hofer, Biometrie: Begriff und Diskussionsstand, juridikum (2004) 79; this study was influenced by the USA entry and visa requirements imposed by after 11 September 2001.*

[76] *German Research Centre for Artificial Intelligence (Deutsches Forschungszentrum für Künstliche Intelligenz) at http://www.dfki.de/web/forschung/projekte?pid=103.*

[77] *Manfred Leber, Fair Pay – Sicherheit im elektronischen Zahlungsverkehr, CR (2000) 492.*

