CASE TRANSLATION: GERMANY

CASE CITATION:
5 October 2004, XI ZR 210/03, published BGHZ 160, 308-321[1]

NAME AND LEVEL OF COURT:
Bundesgerichtshof (BGH) (Federal Court of Justice)

Electronic signature (PIN); ATM; card holder; theft of card; subsequently used by thief; liability

Savings Bank liability for abuse of an ec-card[2]

Prima facie evidence of the negligent storage of an ec-card and PIN by the cardholder and the invalidation of the evidence

1. If, after the theft of an ec-card, the card is used with the correct personal identification number (PIN) at an automated teller machine (ATM), in principle the prima facie evidence demonstrates that the cardholder must have noted the PIN on the card or stored the PIN together with the card, if other causes of fraud can be disregarded as the result of the experience of life.

2. The possibility that unknown third parties can obtain a personal identification number (PIN) by eavesdropping may in principle only be considered if the ec-card was stolen in a close chronological sequence to the use of the PIN by the cardholder at an ATM or a point-of-sale (PoS) terminal.

Tenor

The revision against the judgment of the 5th Civil Chamber of the District Court (Landgericht) of Duisburg, 8 May 2003 is rejected, and will be at the expense of the plaintiff.

Facts of the case

1 The plaintiff demands the reimbursement of funds debited by the defendant savings bank from the plaintiff's current account after withdrawals at ATMs.

2 The plaintiff held a current account with the defendant. In November 1999 the defendant issued an ec-card and a personal identification number (PIN) to the plaintiff. The defendant's general terms and conditions regarding the use of the ec-card contained inter alia the following clauses:

3 'For damages, which occur before the loss is reported; the account holder is liable if the damages are the result of the account holder's violation of the duty of care and the duty of co-operation.

...

4 Damages which occurred before the loss is reported and which have to be accepted by the account holder will be borne by the savings bank provided that the cardholder did not violate his duty of care and his duty of co-operation with gross negligence.

5 Gross negligence of the cardholder is present, in particular, if

6 - the personal identification number is noted on the ec-card or is stored together with the ec-card (e.g., the original letter which contains the PIN),

7 - the personal identification number was communicated to another person and the abuse was caused thereby ...'

8

[1] *http://www.bundesgerichtshof.de >> Entscheidungen >> 05.10.2004.*
[2] *A eurocheque card is a cash card.*

9 The ec-card of the plaintiff was successfully used at the ATMs of two other savings banks by entering the correct PIN. On 23 September 2000 at 17:30, two amounts of 500 DM were withdrawn on two separate occasions, and in the morning of the following day, the sum of 1,000 DM was withdrawn. On 25 September 2000 the plaintiff initiated the blocking of her ec-card. The defendant charged the plaintiff's current account with the amounts withdrawn from the ATMs.

10 The plaintiff claims that on 23 September 2000, between 15.00 and 17.00, during a city festival, her purse which contained her ec-card was stolen. The plaintiff claims that the PIN was noted nowhere, but it was saved in the form of a telephone number on her mobile telephone. The mobile telephone was not stolen. The plaintiff claims that the thief must have decrypted the personal identification number or must have exploited a lack in the defendant's security system for the secrecy of the bank's cryptographic key.

11 The Local Court (Amtsgericht) decided in favour of plaintiff's demand of reimbursement of the amount of 2,000 DM plus interest, and the District Court (Landgericht) rejected the plaintiff's demand. With the revision admitted by the court of appeal, the plaintiff seeks for the reinstatement of the District Court's judgment.

Findings

12 The revision is without cause.

I.

13 The District Court based its decision in essence on the following:

14 The complaint is without cause. The plaintiff's current account was rightly charged with 2,000 DM because of the plaintiff's violation of the contract regarding the current account. The plaintiff is liable for damages to this amount. The prima facie evidence that the plaintiff violated the duty of care regarding the storage of the ec-card or the secrecy of the personal identification number in a grossly negligent way is in favour of the defendant. In particular it has to be taken into consideration that the plaintiff may have noted the personal identification number on the ec-card or that the plaintiff may have stored this number together with the ec-card. Other than because of the plaintiff's grossly negligent behaviour, the three withdrawals at an ATM without any failure when the PIN was entered by an unauthorised third party (the thief or an accomplice) may not be explained according to life experience.

15 The PIN and the 128-BIT-key to the PIN-system of the ec-card issued to the plaintiff by the defendants in November 1999 could not be decrypted on 23 September 2000. According to the authorized expert's report it is mathematically impossible to generate the PIN of an individual card by means of information present on the card without prior knowledge of the bank's cryptographic key. Even with maximum financial effort it would be impossible to design a computer that allows the calculation of the bank's cryptographic key. Other theoretic possibilities considered by the authorized expert regarding the explanation how a delinquent could have obtained the plaintiff's PIN if the plaintiff did not behave in a grossly negligent way would not exclude a prima facie evidence to the plaintiff's detriment nor weaken the evidence. All theoretic possibilities could not be considered as seriously neither in general nor in the specific case. The former applies to 'insider attacks', i.e. for attacks by employees of the bank against the bank's cryptographic key, for attacks against the software used for the authorization of transactions in the bank's data procession centre or unintended leaks of the software allowing a withdrawal without correct PIN or providing insiders the opportunity for an attack. According to the explanations of the expert, there is no evidence that such possibilities have been discovered and exploited for such criminal acts. Finally, in this case there was no evidence that the plaintiff's PIN was obtained by a third party.

II.

16 These observations withstand a legal review.

17 The plaintiff is not entitled to claim pursuant to Section 667, 675, Para 1, f Civil Code Section 676 or

Section 700, Para 1, 607 BGB the reimbursement of the amount of 2,000 DM withdrawn by an unauthorized third party from the defendant. The defendant lawfully debited the plaintiff's account with the amount of 2,000 DM originated by the cash withdrawals on 23 and 24 September 2000 at ATMs.

18 1. [...] The defendant has not proved that the withdrawals of money were made by the plaintiff or by a third party with the plaintiff's consent. Rather, the District Court reached the conclusion that the cash withdrawals were made by an unauthorized third party, namely the thief, or an accomplice with the help of the original ec-card. This is not disputed by the defence pleadings.

19 2. However the defendant is entitled to claim for damages from the plaintiff, because of a default in performance of contract. The defendant could charge the damages to the plaintiff's current account (see BGHZ 84, 371, 376) and debit the current account. The plaintiff is liable for the damage resulting from the misuse of the ec-card because the damage was caused by the plaintiff's grossly negligent violation of the duty of care and the duty of co-operation. As a result, the District Court correctly accepted the prima facie evidence that the plaintiff violated the duty to keep the PIN secret by noting the PIN on the ec-card or storing the PIN together with the ec-card.

20 a) Noting the personal identification number on the ec-card or storing it together with the ec-card constitutes grossly negligent behaviour of the cardholder, which is also pointed out in Section A. III. 2.4 of the general conditions for the use of ec-cards. The evaluation of this behaviour as grossly negligent takes into account that this behaviour undermines the special protection offered by the PIN which is required in addition to the ec-card because an unauthorised third party which obtained the ec-card and PIN could withdraw money without further ado (BGHZ 145, 337, 340 et seq.).

21 b) The District Court concluded rightfully that the prima facie evidence indicates that the plaintiff has noted the personal identification number on the ec-card or stored it together with the ec-card. The plaintiff has not invalidated this prima facie evidence. [...]

26 (2) So far the Senate has left open whether in cases in which cash was withdrawn at ATMs using the correct personal identification number to withdraw money, the prima facie evidence indicates that either the cardholder as the legitimate account holder himself has carried out the withdrawal or that a third party could have obtained the PIN after the theft of an ec-card because it was stored together with it (BGHZ 145, 337, 342). Only the latter comes into consideration as it remains an undisputed finding of the District Court. In the case-law of the courts of first instance and in the literature, a respective prima facie evidence is overwhelmingly approved to the detriment of the account holder (OLG Frankfurt - 8. Zivilsenat - WM 2002, 2101, 2102 f.; OLG Stuttgart WM 2003, 125, 126 f.; LG Hannover WM 1998, 1123 f.; LG Stuttgart WM 1999, 1934 f.; LG Frankfurt am Main WM 1999, 1930, 1932 f.; LG Darmstadt WM 2000, 911, 913 f.; LG Köln WM 2001, 852, 853; LG Berlin - 52. Zivilkammer - WM 2003, 128, 129; AG Diepholz WM 1995, 1919, 1920; AG Hannover WM 1997, 1207, 1208 f.; AG Wuppertal WM 1997, 1209; AG Charlottenburg WM 1997, 2082; AG Dinslaken WM 1998, 1126; AG Osnabrück WM 1998, 1127, 1128; AG Frankfurt am Main NJW 1998, 687 f. und BKR 2003, 514, 516; AG Flensburg VuR 2000, 131 f.; AG Hohenschönhausen WM 2002, 1057, 1058 f.; AG Regensburg WM 2002, 2105, 2106 f.; AG Nürnberg WM 2003, 531, 532 f.; AG Charlottenburg WM 2003, 1174, 1175; Werner WM 1997, 1516; Aepfelbach/Cimiotti WM 1998, 1218; Gößmann WM 1998, 1264, 1269; Palandt/Sprau, BGB 63. Aufl. § 676 h Rdn. 13; Musielak/Foerste, ZPO 3. Aufl. § 286 Rdn. 26), von einem erheblichen Teil aber verneint (OLG Hamm WM 1997, 1203, 1206 f.; OLG Frankfurt - 7. Zivilsenat - WM 2001, 1898; OLG Frankfurt - 24. Zivilsenat – WM 2002, 1055, 1056 f.; LG Berlin - 51. Zivilkammer - WM 1999, 1920; LG Dortmund CR 1999, 556, 557; LG Mönchengladbach VuR 2001, 17, 18; LG Osnabrück WM 2003, 1951, 1953; AG Buchen VuR 1998, 42 f.; AG Hamburg VuR 1999, 88, 89f.; AG Berlin-Mitte VuR 1999, 201, 202 f. und EWiR 2003, 891; AG Frankfurt am Main WM 1999, 1922, 1924 ff.; AG München NJW-RR 2001, 1056, 1057; AG Dortmund BKR 2003, 912, 913; AG Essen BKR 2003,

514; Pausch CR 1997, 174; Strube WM 1998, 1210, 1212 ff.; Zöller/Greger, ZPO 24. Aufl. vor § 284 Rdn 31). The vast majority of these decisions and sources refer to the old procedure for the generation and verification of the personal identification numbers with the help of a private 56 bit bank key or pool key. This old procedure was replaced in 1997 and therefore these decisions and sources have only a reduced validity for the evaluation of the security of the procedure after 1997. [...]

27 (3) The District Court and the Senate agree that in the present case the prima facie evidence argues for the grossly negligent behaviour of the cardholder concerning the secrecy of her personal identification number.

28 (a) Contrary to the plaintiff's opinion, the principles of the prima facie evidence are not inapplicable for the reason alone that there are several theoretical and practical possibilities for a third party to obtain the personal identification number. The District Court has rightly come to the conclusion that the withdrawal with the original ec-card and the correct PIN by an unauthorised third party cannot be explained other than with the grossly negligent behaviour of the plaintiff. Other reasons might be possible in theory but after an evaluation they have to be considered as beyond the experience of life.

29 (b) Against the application of the principles of the prima facie evidence the plaintiff can not mention that there is no empirical proof that the personal identification number is noted on the ec-card or stored together with the card. [...]

30 (c) The District Court – taking into account the authorized expert's advice – has reached the conclusion that even with the greatest financial effort it is mathematically impossible to generate the PIN of an individual card by means of information present on the card without prior knowledge of the 128 bit cryptographic key used by the bank. This complies with written information of the Federal Office for information security (Bundesamt für die Sicherheit in der Informationstechnik – BSI) towards the German savings banks and clearing house association (Deutscher Sparkassen und Giroverband – DSGV) dated 27 November 2001 regarding the new PIN-procedure introduced by the association. [...]

31 (d) The rules on the prima facie evidence are not inapplicable because it would be assumed that two different causes could have caused the damage, both of them typical courses of action but the plaintiff would only be liable in one case. [...] Eavesdropping of the PIN for instance by means of optical or technical devices or by manipulation of the ATM or by the attentive observation of the PIN input at a Point-of-Sale (PoS) terminal or an ATM without sufficient visual protection would be quite conceivable. [...]

32 The plaintiff does not argue such a case. The contrary was argued by the plaintiff, claiming that she did not withdraw money with the ec-card the day the card was stolen. [...]

33 (e) Without an error of law, the District Court does not attach importance to the 'insider attacks', i.e. attacks by employees of the bank to spy out the bank's cryptographic key, attacks against the software used for the authorization of transactions in the bank's data procession centre or unintended leaks of this software, attacks that would be a probability opposed to the prima facie evidence which is to the detriment of the account holder. [...]

35 (g) The plaintiff wrongly argues that the application of the principles of the prima facie evidence by the jurisdiction would result in cases of similar type in a reversal of burden of proof and would provoke a liability regardless of negligence or fault that is similar to a guarantee because the bank customer does not have the ability to reveal security leaks of the system. According to settled case-law of the Federal Court of Justice (Bundesgerichtshof - BGH) this prima facie evidence does not lead to a reversal of the burden of proof (BGHZ 100, 31, 34 with further references). The bank has to adduce full evidence that the cardholder has effected an withdrawal in person or their gross negligence made possible the abuse of the ec-card by an unauthorized third party, if the cardholder shakes the basis of the prima facie evidence with a detailed description and if applicable with proof of the

possibility of an atypical course of action. [...]

III.

37 The revision of the plaintiff was rejected as unfounded.

Commentary

A savings bank can debit the funds withdrawn by the card holder (or a third party authorized by the card holder) from the card holder's current account. Such reimbursement of expenses is based upon Section 676h of the German Civil Code (Bürgerliches Gesetzbuch – BGB). Section 676h BGB provides that:

> Das Kreditinstitut kann Aufwendungsersatz für die Verwendung von Zahlungskarten oder von deren Daten nur verlangen, wenn diese nicht von einem Dritten missbräuchlich verwendet wurden. Wenn der Zahlungskarte nicht ein Girovertrag, sondern ein anderer Geschäftsbesorgungsvertrag zugrunde liegt, gilt Satz 1 für den Kartenaussteller entsprechend.
>
> The banking institution may only demand reimbursement of expenses for use of payment cards or of their data if the latter have not been abused by a third party. If the payment card is not based on a current account contract but another contract for the management of the affairs of another, sentence 1 applies with the necessary modifications to the issuer of the card.[3]

In the event of an unauthorized withdrawal with the aid of an ec-card, the banking institution can take into consideration a claim for damages. The grossly negligent behaviour of the card holder regarding the storage of the PIN or the ec-card or both may result in the card holder's liability towards the banking institution. But in such a case, the banking institution has to prove the card holder's breach of the general terms and conditions regarding the use of the ec-card. The new 128-BIT-key system leads to a significant higher security and makes it very improbable that the PIN can be generated. Therefore the prima facie evidence (prima facie evidence is a similar concept to a presumption in English law) that the PIN and ec-card were stored together or that the PIN was noted on the ec-card is conceivable. In its general terms and conditions the savings, the bank enumerated a number of cases (they were not exhaustive) in which the card holder's behaviour is considered to be grossly negligent, and the BGH considers these provisions are valid.

For the future, it has to be discussed how the prima facie evidence, which is formulated to the card holder's detriment, can be challenged in individual cases. In practice it will be difficult for a card holder to demonstrate that the PIN was not noted on or stored together with the ec-card. The former will be impossible if the card was stolen and cannot be shown. The court's confidence in the security of the encryption system together with the validity of the general terms and condition's non-exhaustive list of what constituted grossly negligent behaviour resulted in a disadvantageous result for the consumer in this case.

Dr. Eßer is a member of the editorial board

Further commentary on the German Federal Court of Justice Judgement of October 5, 2004, Case XI ZR 210/03

By **Dr. Thomas Kritter**

Headnotes of the decision

1. If cash is withdrawn from an ATM shortly after theft of an ec-card by using the stolen card and the correct PIN, a *prima facie* presumption applies that the card holder had noted the PIN on the card or stored the PIN together with the card.

2. A sniffer attack on the PIN by a third person as an alternative reason in principle only can be considered if the ec-card has been stolen shortly after the PIN had been entered into an ATM or PoS terminal by the cardholder.

Facts of the case

The plaintiff had a current account with the defendant, a German savings bank. The bank had issued an EC-Card with a personal identification number (PIN). According

[3] *This provision serves to implement Article 8 of Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts OJ L144, 04/06/1997 P. 0019 - 0027.*

to the banks general terms and conditions, in case of loss of the card, a card holder was in principle liable for damages incurred before a notice of loss to the bank if he or she had negligently infringed their duties of care. However, the bank was prepared to indemnify the card holder provided he had not infringed his duty of care and was not grossly negligent. The general terms and conditions stipulated that a case of gross negligence was present in particular if the PIN was noted on the card or has been stored together with the card.

On two consecutive days two amounts of DM 500 and one amount of DM 1,000 were withdrawn before the card was blocked on the third day. The card holder claimed the card had been stolen at a local festival. She alleged that she had neither written the PIN onto the card nor stored the PIN together with the card. She claimed that the thief must have deciphered the PIN or must have taken advantage of defects in the security mechanisms in place to keep the bank's institutional key secret. The amount withdrawn was debited to the account. The card holder sued the bank for payment of DM 2,000.00.

Background of the decision

Since the end of the 1990s, there have been a considerable number of cases brought before the first and second instance courts where card holders had sued their banks for reimbursement of damages they allegedly suffered from misuse of their stolen cards.

The final instance judgement concerned an EC-card. The PIN of the card was protected by a Triple-DES 128-Bit-Encryption. The case belongs to a group of cases where it was argued that criminals must have been able to decipher the PIN, as the plaintiffs alleged they had adhered to their duties of care so that it was impossible for a thief to get knowledge of the PIN. The banks in such cases argued that it was impossible to decipher the 128-Bit-Encryption by a brute force attack at that point in time (around 2000).

In this situation, the majority of lower instance courts applied a *prima facie* presumption that (i) either the card holder had withdrawn the money or (ii) that a third person, after theft of the card, was able to obtain knowledge of the PIN because it had been kept together with the card. Contrary to these decisions, a substantial number of courts refused to apply such a *prima facie* presumption. It should, however, be noted that a number of these cases concerned the older DES-56-Bit-Encryption (which is deemed to be vulnerable to brute force attacks since the end of the 1990s).

Due to the relatively small amounts of money usually involved, cases usually started at (lowest) district court level (Amtsgericht with jurisdiction for claims until an amount of 5,000.00 Euro) with the possibility to appeal to the regional court (Landgericht) on facts and on law, with the possibility for a further appeal only on questions of law to the Federal Court of Justice (Bundesgerichtshof). Only a small number of cases started at regional court level (claims above an amount of 5,000.00 Euro) with the possibility to appeal on facts and on law to the Higher Regional Court of Appeals (Oberlandesgericht) with possibility of a further appeal only on questions of law to the Federal Court of Justice (Bundesgerichtshof).

Ruling

The Federal Court of Justice upheld the view of the majority of German Courts that the banks in cases of misuse of ec- and creditcards (using a 128-Bit-Encryption) can rely on a *prima facie* presumption.

The Court held that if cash is withdrawn from an ATM shortly after the theft of an ec-card by using the stolen card and the correct PIN, a *prima facie* presumption applies that the card holder had noted the PIN on the card or stored the PIN together with the card. It further held that a sniffer attack on the PIN by a third person as an alternative reason in principle only can be considered if the ec-card has been stolen shortly after the PIN had been entered into an ATM or PoS terminal by the cardholder.

According to the case law of the Federal Court of Justice, a *prima facie* presumption can only be applied where a fact to be proven is a typical occurrence in the normal course of events, taking into account all the undisputable and established circumstances of the individual case. If a *prima facie* presumption does establish causation, the opposing party can challenge the presumption on the basis of facts which cast serious doubt on whether a typical occurrence is involved.

The Federal Court of Justice as the final court of appeal, had to rely on the findings of fact of the Regional Court (Landgericht) as second instance court in this case. The regional court, having considered an expert opinion, came to the conclusion that even with substantial financial efforts it would be mathematically impossible to calculate the PIN on individual cards using the data stored on the cards without having deciphered the banks 128-Bit encrypted institutional

key. Deciphering the bank's institutional key by a 'brute-force-attack' was regarded as impossible by the expert heard by the regional court with regard to the Triple-DES-128-Bit-Key at stake. Due to the fact that the Federal Court of Justice only decides on questions of an appeal in law, the court was restricted to examine whether the lower court did appreciate all the evidence without any contradiction. The Federal Court of Justice did not find such mistakes in the appreciation of evidence of the lower court.

The Federal Court of Justice further upheld the lower court's view that the mere theoretical possibility of an insider attacks by persons concerned with the security infrastructure in the banking sector is not sufficient to deny a *prima facie* presumption.

Thus, a *prima facie* presumption applies, which leaves the banks' customers with the possibility to show that the banking system is not necessarily secure. In this regard, the court held that even though the burden for challenging the prima facie presumption lies with the customer, the bank might be obliged under the rules of secondary burden to substantiate facts to provide information on its security systems, taking into account the interests of the bank to keep the detailed infrastructure secret.

Reaction

The judgement was criticised in particular from consumer organisations. It was argued that the lower court had relied on an insufficient expert opinion, which to a great extent was based on assumptions as the bank had failed to provide the court's expert with sufficient facts as to the structure of PIN authentication system.

The judgement of the Federal Court of Justice was contested in a recent case before the Higher Regional Court of Appeal of Frankfurt. The plaintiff there, a consumer organisation representing several cases, argued that recent research had shown the 128-Bit-Key was not safe. The trial concerned cases of card misuse between December 1999 and February 2003. The Higher Regional Court of Appeal of Frankfurt appointed a court expert from the German Federal Office for Information Security. Heaving heard the expert, the Higher Regional Court of Appeal of Frankfurt shared the view of the Federal Court of Justice, that for the time period in question the Triple-DES-128-Bit encryption must be regarded as safe. The court held that it seemed practically impossible that criminals were able to decipher a PIN of an ec-card by a brute force attack. The court further referred to the fact that no case of an insider attack has become known in public an thus applied a *prima facie* presumption which the plaintiff was not able to challenge (judgement of January 31, 2008, Case 23 U 28/05).

Conclusion

With its 2004 judgement, the Federal Court of Justice decided a long drawn-out dispute between the lower instance courts about the application of a prima facie presumption in cases of ec- and credit card misuse, and the assumption about the security of the PIN system. The general discussion about security of the PIN and the ec- and credit card system will certainly continue, as the ruling of the Federal Court of Justice is based on certain mathematical-technical assumptions which might be contested in the future.

Dr. Thomas Kritter, LL.M. (University of London), Rechtsanwalt, is specially accredited for banking and capital markets law by the Bar Association for the District of the Court of Appeal of Karlsruhe. He is also a member of the working group on banking law of the German Lawyers Association.

http://www.kleiner-law.com

