CASE TRANSLATION: NORWAY

CASE CITATION:
Journal number 04-016794TVI-TRON

NAME AND LEVEL OF COURT:
Trondheim District Court

DATE OF DECISION:
24 September 2004

DECISION RENDERED BY:
Assistant Judge Leif O. Østerbø

CASE TYPE:
General Civil

PLAINTIFF:
Bernt Petter Jørgensen

LAWYER FOR THE PLAINTIFF:
Philip Niklas Jahn Hayes

DEFENDANT:
DnB NOR Bank ASA by the Chairman of the Board

LAWYER FOR THE DEFENDANT:
Kristine Edvarda Richardsen

Bank card; theft of card; unauthorized use; PIN; electronic signature; burden of proof; liability; gross negligence

Judgment

Case background:

The holder of a bank card, Bernt Petter Jørgensen, had two shoulder bags stolen on Saturday 4 August 2001. The theft took place between the hours of 15:00 and 15:20 pm while Jørgensen was loading his luggage into a rental car after arriving at Alicante Airport in Spain. The shoulder bags contained, amongst other things, a wallet containing several credit cards. In addition to the credit cards, two mobile telephones, airline tickets, keys, and cash were also stolen.

Jørgensen was robbed of six cards, and his wife was robbed of four such cards. Two of the cards were used without authority. This case concerns a particular card, a Cresco Card (hereinafter 'the card'). The second card was issued by Nordea (Kreditkassen). Regarding the misuse of the second card, the issue has been settled with the bank, the bank having accepted Jørgensen's explanation.

The loss of the card at issue was detected immediately. However, the parties disagree about who was responsible for failing to bar the card from being used until Tuesday 7 August 2001. There were a total of four debits on the Cresco card, with a total amount of kr 9,628. The debits were made on Saturday 4 August 2001 at 16:13, 16:14, 16:15 and 16:19 including debits of kr 2,407. Prior to these charges, the card was last used at Torp airport in Sandefjord where withdrawals occurred in connection with the flight to Spain.

The Board of Bank Complaints for Consumers in Banking (Bankklagendmnda) considered the case on 20 June 2002. The majority, consisting of three of the five members, stated, amongst other things, that they:

> '[Board of Bank Complaints] Find that the case should be considered on its merits and refer to the rationale of the earlier cases, BKN 2001-017 and 2001-052 BKN. It appears from the information in the present case that the payment card was used with a PIN code, and the correct code, according to the information, was entered on the first try, just shortly after the card holder's wallet was stolen, containing the respective card. The card holder himself made withdrawals with the card, the last time at Torp airport in Sandefjord, before the theft took place. The majority found that the unauthorized user of the card did not discover the code when the card holder withdrew the funds. Following a review of events as stated, the board's majority finds that it is most likely that the code, possibly in a poorly disguised form, was stolen along with the card from the card holder's wallet. This is contrary to the card holder's recollection. The misappropriation is considered to be possible because of the gross negligence of the card holder, and the bank can hold the card holder responsible for kr 8,000 of the unauthorized withdrawal amount, for which see the

> Law of Financial Contracts § 35 (2) point a and the current account policies section 5a. The majority point out that it cannot be assumed that the abuse took place after the card was reported lost. Thus, BBS was contacted by the complainant's assistant at 13.28 on the day of the loss. The Bank Board of Complaints (hereinafter "Board") also refers to the card holder's verification he has obtained from LOfavør StopService that his LOfavør MasterCard was blocked at 16.10 on the day of the loss, before the misuse started. The card holder has stated that his assistant in Norway requested that the relevant payment card be blocked, which it was not. As the case appears, the relevant payment card was not reported to LOfavør StopService, which under the terms of the agreement was an essential requirement. Reporting the card as stolen was necessary for the center to block the card in the matter in dispute.'

In accordance with the majority's view, the case was decided with the following conclusion:

> "The bank can hold the card holder liable for kr 8,000 for misuse of his credit card."

The two members representing the minority of the board would dismiss the case because they believed there was insufficient information for the case to be heard on its merits.

Jørgensen filed a complaint at the Trondheim District Court on 13 May 2004, and the defendant's response was received on 7 June 2004. Thereafter, Jørgensen filed pleadings on 25 June, 5, 20 and 25 August, and 20 and 21 September 2004. The defendant filed response pleadings on 7 June, 16 July 15 and 21 September 2004. The Trondheim District Court heard the case under the rules for simplified proceedings set out in the Civil Procedure Act § 322.

Pursuant to the Civil Procedure Act, § 322a third sentence, Jørgensen requested an oral proceeding. This was held in Trondheim court on 22 September 2004. In addition to the plaintiff, a total of 7 witnesses provided testimony.

The plaintiff has essentially argued as follows:

Jørgensen did not keep the PIN with the card. The codes were written down, and were in his safe at his residence. Jørgensen maintains that he has no trouble remembering the codes, which he had memorized. From Jørgensen's point of view, his actions are not blameworthy.

Several similar episodes have been featured in the media, and one must take as a fact that PIN codes can be broken by the use of advanced computer equipment. It also appears that there have been a number of such cases brought before the Board (Bankklagendmnda) and the courts. It appears unreasonable that so many people are certain that they have kept their card and code in such a way that others will easily be able to acquire it.

It is difficult for card holders to substantiate that they have not kept the card and code together, and the banks have not used any resources to prevent the abuse of cards when stolen.

DnB NOR Bank ASA has the burden of proof, and it should be the bank's risk that it is not known how the thieves made the withdrawals.

Jørgensen believes that there is such doubt about the events that it cannot be assumed that he has acted with gross negligence.

In addition, it is submitted that Jørgensen gave notice of the loss in time. Efforts to get transactions blocked started immediately and he declared that his EuroCard and LOfavør MasterCard were locked at 4:10 on the day of the loss. That the bank failed to block the card in a timely manner, must be the responsibility of DnB NOR Bank ASA. The plaintiff has submitted the following claims for relief:

1. Cresco is ordered to pay kr 8,000 to Bernt Petter Jørgensen with the addition of the general penalty, including 12% interest before 1 January 2004, and 9.25% interest after 1 January 2004, from 1 September 2001 until payment is made.

2. Bernt Petter Jørgensen is awarded legal costs with additional penalty interest from the judgment until fulfillment of the payment.

The defendant makes the following argument:

DnB NOR Bank ASA (hereinafter called the bank) believes it is the claimant that has the burden of proof, thus requiring Jørgensen, who claims that he has not been grossly negligent, to substantiate this claim. Further, the bank believes that it has substantiated that the card holder was substantially grossly negligence. The bank maintains that the card holder did not report the theft in a timely manner. It appears that the message to block the account was first registered on Tuesday 7 August 2001.

The thief used the correct PIN. This suggests that Jørgensen, the card owner, kept the code with the card. When the misuse of the card occurred, the card holder's PIN was correctly entered on the first try. The complainant has thus been grossly negligent.

Copying the magnetic stripe is a known problem for the bank and both software and technical devices for such copies can be purchased in specialty shops. However, the copy has the same PIN code as the original. It is not possible to 'crack' the PIN on the card given to Jørgensen.

It is unlikely that someone who travelled on the same flight from Torp to Alicante would observe that Jørgensen entered the code at the outlet at Torp. There are no other likely causes of the abuse, other than the card holder kept the code with the card.

The defendant has submitted the following plea:

1. DnB NOR Bank ASA is acquitted.

2. DnB NOR Bank ASA is awarded costs plus the general judgment will accrue from the fulfillment of payment.

The court notes:

The claim was made against Cresco Kredittkort AS. The statement was later corrected to DnB Nor Bank ASA. Regarding the court's competence, it is noted that it is not the correct geographical venue for the case. DnB NOR Bank ASA has been notified that the writ names the incorrect defendant. However, no objections were filed either against the defendant when the entity was changed, or the court's competence. The court considers that the party designation in this particular case can be corrected. It is referred to the structural changes that have taken place on the defendant's side, see the Civil Procedure Act § 97. DnB NOR Bank ASA have also explicitly agreed that they are the appropriate defendant in the case.

Furthermore, the parties met for negotiations without any objections against the court's (geographical) competence. The court sees itself competent to decide the case, see Civil Procedure Act § 92.

The parties have devoted some attention to the question regarding who has the burden of proving that Jørgensen acted with gross negligence. The court will first consider this question.

The court refers to the general rules of the burden of proof, and refers specifically to Ot. Prp. (1998-99) no. 41 on page 44 which states:

> 'It should be stressed that even without a rule of a statutory burden of proof, a tribunal or a court cannot assume that the customer has acted with gross negligence unless there is specific evidence of this. That the PIN code has been used and the customer has no explanation on how the code became known to the unauthorized persons, cannot be sufficient to assume that the customer acted with gross negligence and impose responsibility.'

The court also believes it will be in error to require the card holder to prove that he did not act with gross negligence. The court believes that the bank has the burden of proving that Jørgensen acted with gross negligence in connection with unauthorized uses that have been made with his bank card.

The Court then turns to the more substantive issues.

The Law of Financial Contracts § 35, second paragraph provides as follows:

> The account holder is liable for up to kr 8,000 for losses caused by the unauthorized use of payment cards if
>
> a) the account holder or a person the credit card has been given to by gross negligence has made the abuse possible, or
>
> b) the abuse is made possible because the account holder or a person the credit card has been given to has failed to notify the institution as soon as possible after discovering the loss of the credit card or within reasonable time after this should have been discovered.

The provision is written so that the bank is entitled to charge the account holder up to kr 8,000 for losses caused by unlawful use of his credit card, if the abuse is made possible by gross negligence of the account holder, or if the account holder has failed to notify the bank as soon as possible after learning the payment card has been lost.

First, the court will consider Jørgensen's claim that he notified the bank within a reasonable time of the stolen

card, see the Law of Financial Contracts § 35, second paragraph, letter b. On this point, the court takes the same position as the board (Bankklagenemnda).

The court believes that Jørgensen did not notify the bank of the loss in time, showing that the stolen card was not enrolled in the blocking scheme under LOfavør StopService. The court cannot see any failure of the bank in this context and finds that it cannot be determined that Jørgensen was informed that the card was included in the Lofavør Stop Service arrangement, or that he had reasonable grounds to believe it.

The court finds that BBS was notified of the first block at 18:28 on the day of the loss, after the unauthorized use of the card took place. The other cards were locked at 16:10. The court notes that this assessment is not required for a finding of gross negligence. The court further refers to the board's review, provided above, which this court endorses.

The court then turns to the question of whether the conditions for gross negligence, as required in the Law of Financial Contracts § 35, second paragraph letter a, have been fulfilled.

By Supreme Court judgment in Rt 2004 page 499, premise 32, is quoted:

> 'The Supreme Court's judgment rendered in Rt-1989-1318, stated that gross negligence must represent a substantial departure from the usual prudent course of action, and that it must be about a performance which is highly blameworthy, for which he is substantially more to blame than under the question of ordinary negligence. The case referenced considered liability insurance. I refer you on to Rt-1995-486 where it was referred to the judgment of 1989. Also in the legislative history of the provision in the Financial Contracts § 35, NOU 1994:19 page 144, it is stated that a substantial departure from the usual prudent course of action for any act or failure to qualify for gross negligence. I put this as a basis for further discussion …'

The court assesses Jørgensen's actions.

The court has considered a number of possible events. The court is of the opinion that it appears very unlikely that Jørgensen actively took part in the misuse of the card. The bank does not dispute this point. The court does not believe or find evidence that Jørgensen gave the code to others and that they in turn obtained access to the account in question. The bank is in agreement on this point.

The court also notes that someone entering the correct code on his or her first attempt, by pure guesswork, is also highly unlikely.

Another possibility that has been promoted is that prior to departure, someone saw Jørgensen enter his PIN when withdrawing funds at Torp airport in Sandefjord and this passenger, also on the flight to Spain, committed the theft and subsequent unauthorized use. The court believes that this appears to be a highly unlikely sequence of events, particularly in light of the fact that one of the other cards subject to unauthorized use was not in use at Torp airport.

It remains for the two other possible events, and it is these events that the parties have devoted the most attention. One option is that Jørgensen kept the code with the card in such form that it was possible for others to acquire the code. The second of the remaining options is that someone managed to 'break' the PIN on the card and then make withdraws. It is hard to imagine any other realistic sequence of events.

For the court, the question of whether a PIN code can be cracked was at the heart of the matter, and we now consider this.

The court understands that the PIN is not stored in the card. The card has a verification value. When the code is entered at the terminal, a complicated process is started, and there is a (de) cryption/cryptographic calculation in the interaction between the outlet terminal and a remote central computer that is connected on-line. The result of this process is that the code is either approved or denied, but other possibilities exist.

Central to the security system appears to the court to be what is called the DES system. This algorithm is a system for encryption of 'keys' used in several areas. This is related to the process that is achieved to demonstrate whether the key code is correct or not.

It appears uncertain whether the current board used the double or triple DES system. Double DES has a substantially lower level of security than triple DES. The

uncertainty associated with the card's security is related to the issue date. In this respect, the security of the card seems to be crucial.

The parties agree that the card was issued between 1 and 15 February 2000. At that time, the bank upgraded the systems without knowing whether the stolen card had been upgraded or not. The witness Haugstad explained to the court that all cards of the type Jørgensen was in possession of, which had an expiration date of the fourth month of 2001, should have been equipped with triple-DES. The misused card, expiring in February 2002, would have been equipped with triple-DES. As the court understands it, and based on Sundby's testimony, the upgrade process and the security could be different depending on which part of the card is in question, and there are other uncertainties associated with the current card's security. It is also unclear how the upgrade process took place. The court finds, therefore, with some doubt it must assume that the worst of these systems (double DES) was in place on Jørgensen's stolen Cresco card.

At significant points, there is no correlation between the statements that the expert witnesses have given. The witness Arnesen argues that it is generally known that the double-DES system has known vulnerabilities and PINs that are associated with this system can be 'cracked' within seconds or minutes. This can also be accomplished by relatively unprofessional people. Supporting this point is a judgment from a German court, and also testimony from an individual claiming to have 'broken' a PIN in 1998 (see German sentence of Amtsretten in Darmstadt, dated 24 February 1989). In the instant case, the court does not find any reason to put evidentiary weight on the latter two evidentiary offerings. The witness Tønnesen also believes that PINs can be 'broken' so that cards can be used within a very short time frame.

Arnesen believes that the triple-DES system, which is in use today in practice, will not be broken even with a very long time period and a high level of data capacity. She is not aware that anyone has managed to 'break' the code in the triple DES system.

The witness Sundby believes that PINs on cards with the double (simple) DES system, which are now replaced by the triple DES, could be broken in less than a day, provided that the person breaking the card had significant computing power available to them. Also testifying, Haugstad believe that if it is possible to 'crack' a PIN under the former security level. However, Haugstad maintains that this would take a very long time, longer than the time in question in the present case.

The experts also disagree about whether the effort to 'crack' the code needs to be done after receipt of the actual card or not. The witness Arnesen believes much of the work can be done in advance and that it then will only take seconds or minutes to 'crack' the code after obtaining a card. The witness Sundby says work cannot commence until the card is obtained.

The court finds the circumstances are such that it can be assumed that it is most likely that a person has to have the card in their possession before the work begins, and thus that it necessarily takes a fair amount of time between when a card is obtained by a thief to the point that a PIN can be found. Anything else would, among other things, mean that there would be 'copying machines' for 'buckling' of PINs that anyone with such a motive could use if they had another card in their possession. The court reasons that the work must have been performed after having obtained the card, regardless of whether it involves simple, double or triple DES. However, the court considers it unrealistic, that within a practical time frame (i.e. the card's two year validity period), the triple DES can be broken.

The court is of the opinion that it is probable that it will take a relatively long time to 'break' a PIN that has the double DES system, and that in any case it would take more than an hour or two.

It is assumed that the standard security systems that are used are effective. However, according to Jørgensen, no cases have been documented that demonstrate the implementation of the systems are secure.

The court refers in this respect to the fact that banks are subject to supervision and operate a comprehensive internal control work, and the witness Haugstad's explanation that both the standards and the practical implementation are revised thoroughly and regularly. In that regard, Haugestad explained that the systems are subject to annual audits. The Banks Control Center (BSK), in addition to the major international card companies,

conducts such audits.

The court does not find that there is reason to accept that the banks' security systems are in doubt. Although the implementation of a system necessarily involves opportunities for errors, the court cannot see that this involves significant practical risk for customers with cards.

The Financial Supervisory Authority issued a statement dated 20 August 2002 stating that they cannot see that there is any doubt regarding the bank's note of 3 December 1993 that PIN codes cannot be 'broken'. The statements contained are not new, but they have not been withdrawn or replaced by new statements. The view thus appears to be in force. However, the court does not know, as the plaintiff has pointed out, the background material for these statements.

The court believes, however, contrary to the plaintiff's claims, that it has, on occasion, to express that the bank has not done a complete evaluation or does not have sufficient expertise in this area. The court has been provided with a letter from the Oslo Police District to the Complaints Board dated 11 June 2003 where it is expressed that they are of the opinion that PINs cannot be 'broken'.

However, considering all of the expert witnesses, expressing that PINs subject to the double-DES system (no longer in use today) can be broken, provided that the party has sufficient time and computing power. The statements from the Financial Supervisory Authority, the Central Bank and the Oslo police will probably be understood with these reservations.

Banks are further subject to the supervision of the Commission and self-control, including the Banks' Standardization Office, and international card security requirements.

The court believes that, contrary to the arguments of the plaintiff, that the time factor is relevant. The misuse of the card took place about one hour after the cards were stolen. The authorization log shows, together with response codes, the correct PIN was used in the first attempt (response code 00 and not 55), and that this applies to all four outlets in question. This provides concrete evidence of the alternate sequence of events that the code was readily available and that it therefore must have been kept with the card, or in disguised form so it was natural for others to be able to connect the card and code in a short time.

On the last attempt to withdraw the funds, the transaction was rejected because the amount available in the account was exceeded (response code 61 in the authorization log). The court does not find that there is reason to question the accuracy of the information in the authorization log, as the plaintiff argues.

It must seem obvious that any system of this type will have risk factors relating to safety. There will always be a theoretical possibility that a PIN can be 'broken'. The court finds in the present case it is likely that the code on the card cannot be 'broken' within the time period available in the instant case.

As a result, there is only one possible alternative option available.

The court concludes that there is no other explanation that can be considered a reasonable explanation under the circumstances, other than that the PIN was stored with the card. The court finds that the standard of proof is met by DnB NOR Bank ASA as required in the legislative history discussed above and upon which the court has based its assessment.

The court finds that it is probable, based on specific indications, that Jørgensen kept the code with the card, and that this made it possible for unauthorized access to take place a very shortly after the card was stolen. There are circumstances that the case law falls under the term of gross negligence. For the record, it is emphasized that there are no such circumstances in our case as provided in Rt 2004 page 499.

The fact that Jørgensen was very familiar with the regulations for the storage of cards and codes, including card rules, is not disputed. The court chooses not to consider this issue further.

Costs:

DnB NOR Bank ASA prevails in full. The main rule in this situation is that Jørgensen be required to pay all legal costs, for which see the Civil Procedure Act § 172 first paragraph.

The court, however, finds reason to apply the exception in the Civil Procedure Act § 172, second paragraph. This is because there is actual doubt regarding the specific course of events.

Although the court found it likely that there was gross negligence based on the plaintiff's actions, there is also reasonable doubt in relation to the opportunity to 'breaking' the PIN of the card if it is assumed that the card had a lower security level than is currently being used. It appears in this respect from a number of witness statements that suggest that the PINs used in this earlier system could be 'broken'. The testimony, however, differs markedly among others in terms of how long it would take to 'crack' a PIN with the card security protections used in 2001.

The court believes that the requirements of the Civil Procedure Act § 172, second paragraph are met by 'the matter was so questionable, that there was good reason' for taking legal action.

The court is of the opinion that Jørgensen should not be required to pay DnB NOR Bank ASA's legal costs. The parties shall bear their own costs.

Rendition:

1. The court finds for DnB NOR Bank ASA.

2. The parties shall bear their own costs.

***

The court adjourned

Leif O. Østerbø Judge

The verdict can be appealed to the High Court. The appeal must be declared directly to the district court within one month after the sentence has been served. If the appeal concerns a capital value below 50,000 kroner, it cannot be brought without the consent of the Court of Appeal. Application for consent in such cases must be submitted simultaneously with the appeal statement.

Simultaneously with the appeal statement, the appellant must pay the appeal fee, which is 24 times the court fee. If the trial has lasted more than a day, it incurs an additional fee. If the appeal fee is not paid within the appeal deadline, the appeal is deemed as not filed.

The declaration of appeal must be signed or co-signed by an attorney. The appellant may also contact the court office will appeal the declaration written and signed there.

With thanks to Kevin McGillivray, Gro Caroline Sjølie and Svein Yngvar Willassen for revising the initial translation of this judgment.