ARTICLE:

UNAUTHORIZED USE OF BANK CARDS WITH OR WITHOUT THE PIN: A LOST CASE FOR THE CUSTOMER?

By **Maryke Silalahi Nuth**

In 2004,[1] the Trondheim District court in Norway declared a card holder had acted with gross negligence based on the fact the unauthorised payment transactions on the card holder's bank card were conducted in a relatively short time period after the card was stolen. While pointing out that the security system had previously had been considered 'unbreakable' and had, over time, proved to be breakable, the court decided that the PIN of the stolen payment card could not be broken in the short time demonstrated in this case. It is suggested that the Norwegian District court's ruling is wrongly decided, since it did not take into account the speed of change in technology, including the continuous advancement of intervention technologies. The paper also questions the court practice in Norway, which seems to lean towards the bank rather than the customer in cases of misuse of payment cards with or without using the PIN. A similar case from 2012 will be discussed to support this argument.

Summary of the facts

The misuse of a card can happen either because the card is copied or stolen.[2] Case Number 04-016794TVI-TRON dated 24 September 2004 concerns a bank card issued to Bernt Petter Jørgensen that was misused after being stolen. The card was called a Cresco Card issued by the Norwegian bank, DnB NOR Bank ASA.

A number of cards were stolen at around 15.00 to 15.20 on 4 August 2001. Four withdrawals were debited on the card in dispute totalling Nok. 9,628, each in the sum of Nok. 2,407 and respectively happened at 16:13, 16:14, 16:15 and 16:19. Jørgensen's other cards were blocked at around 16:10 by LOfavør StopService, an organisation with the authorization to block many bank cards simultaneously after the customer makes a telephone call to alert the bank to the loss of a card. LOfavør StopService is only allowed to block bank cards that are reported to LOfavør StopService, which did not occur in relation to the stolen Cresco Card. Jørgensen nonetheless argued that the person receiving his call in LOfavør StopService asked the Cresco Card to be blocked, but it did not happen. The Cresco Card was finally blocked on 7 August 2001 when the bank received the blocking request.

The Norwegian Complaints Board for Consumers in Banking, Finance and Mutual Fund matters (Bankklagenemnda 'Complaints Board')[3] was first to examine the case. By a majority (3 to 5), the Complaints Board considered the Cresco Card was misued because of Jørgensen's gross negligence. It was noted that the withdrawals happened only a short time after the Cresco Card was stolen, and furthermore, all the withdrawals were made by using correct PIN on the first try. Based on these facts, the majority of the members of the Complaints Board presumed it was most likely that the PIN of the Cresco Card was kept in the same wallet together with the stolen cards. The minority members of the Complaints Board considered that the case was too

1 *Case Number 04-016794TVI-TRON dated 24 September 2004. A translation of the case is published on pp 117-123.*

2 *Susanne Kartstoft, Elektronisk betaling i forbrugerforhold -ansvars- og bevisproblemer- retlige overvejelser ved brug på interntettet, TemaNord 1998:590, First Report (Copenhagen: Nordisk Miniterrad, 1998), p. 119.*

3 *The Norwegian Complaints Board for Consumers in Banking, Finance and Mutual Fund matters is an independent body with official financing. It has a permanent secretariat. In the first instance, the Board always seeks to find amicable solution between the parties. In the event the dispute cannot be resolved, the matter will be referred for formal consideration by the Board. All rulings issued by the Board can be appealed in a court of law.*

poorly argued and therefore should be dismissed.

Jørgensen later argued before the Trondheim District court that the code to his Cresco Card was kept in a safe in his house and not kept together with the stolen cards. He also argued that efforts to block his cards were started immediately, as demonstrated by his telephone call to LOfavør StopService, and the blocking of his other bank cards before the misuse of his Cresco Card took place. The bank should be held responsible for the transactions that were conducted after the blocking of his other cards, according to Jørgensen.

The bank argued that Jørgensen reported the theft late. The withdrawals from the Cresco Card happened with the correct PIN on the first try. This fact, according to the bank, suggested that the PIN had been kept together with the misused Cresco Card.

The legal issues

Some legal issues of the case and implications on the legal practice are discussed below.

Burden of proof

Both Jørgensen and the bank rejected the claim that they had the burden of proving that Jørgensen had acted with gross negligence in relation to the misuse of the Cresco Card. The court decided that the bank had the burden of proving that Jørgensen had acted with gross negligence. This is line with a basic principle under the Norwegian civil procedural law which generally places the burden of proof on the person who has brought the case to the court or the plaintiff.[4]

Level of security

One main concern in the use of payment cards is the level of system security protecting the cards from any misuse by unauthorized parties.[5] The court considered that Jørgensen had acted with gross negligence, while at the same time the court also doubted whether the PIN of the Cresco Card was capable of being broken in the short period of time between the theft and the misuse of the card. The court seemed to be reluctant to make an express statement as to whether the Cresco Card had a lower or the same security level with cards otherwise found in the market at that time. The actual level of system security in Cresco Card was not proven before the court. In addition, some expert witnesses testified that the PIN under the earlier double-DES system could be broken. However, the same experts also provided different opinions with respect to how long it takes to break a PIN in that particular system.

From expert witness testimony, it appeared that the highest level of security for a bank card is the triple-DES system, because the code under this system is believed to be unbreakable. The court noted that another system, the double-DES system, can be broken in terms of minutes, seconds or hours. Before the triple-DES system was introduced, the double-DES system was considered as unbreakable. The court did not expressly declare which of these systems was in use in the Cresco Card. However, the court expressed doubts that there was an opportunity to 'break' the card's code in the short time span between the stealing of the card to its misuse. By doing so, the court was implying that the code in the Cresco Card was not protected by an unbreakable security system, the triple-DES security system, and accordingly was breakable. Given the system under which a code can be broken is the double-DES security system, then it can be submitted that the court perhaps considered, albeit impliedly, that the Cresco Card was protected by double-DES security system.

From the foregoing, it is clear that the court had knowledge that the level of security of the PIN in the Cresco Card was lower than the best available technology in the market at that time. That the court did not address the adequacy of security system provided in Cresco Card is worthy of criticism, especially given the vast amount of work on this topic by the team at the University of Cambridge Computer Laboratory.[6] Using a security system that can be broken poses risk to banks as well as customers. The risk of the unauthorised use of stolen cards is logically higher using the double-DES system than in the 'unbreakable' tripple-DES system. Jørgensen could have argued that even if the Cresco Card fell into the hands of a thief, the card would not have been misused if the bank had used the highest level of security in the card. If this argument is capable of succeeding, then arguably the bank should share responsibility together with customer in case of the misuse of a card, even if the misuse was made possible by the customer's gross negligence.

4 *Jo Hov, Rettergang (Oslo: Papinian, 2010), pp. 1148-1149.*

5 *Dr Charles Wild, Neil MacEwan, Stuart Weinstein and Neal Geach, Electronic and Mobile Commerce Law (Hatfield: University of Hertfordshire Press, 2011), p. 30.*

6 *For instance, see: http://www.cl.cam.ac.uk/research/security/publications/; Professor Ross Anderson - http://www.cl.cam.ac.uk/~rja14/; Dr Steven J. Murdoch - http://www.cl.cam.ac.uk/~sjm217/; Light Blue Touchpaper - http://www.lightbluetouchpaper.org/.*

Liability for misuse

Jørgersen was considered to have acted with gross negligence since he, as presumed by the bank and endorsed by the court, must have kept the PIN together with the stolen Cresco Card. Jørgersen stated from the beginning the PIN to his Cresco Card was kept in a safe in his house, and was not near the Cresco Card. Setting aside for later the discussion on whether the card and the PIN were indeed kept together, it is interesting to note that the Norwegian legal practice has long considered the keeping of a PIN together with the associated card as gross negligence, even if the card and the code have been securely kept.[7] It is not considered gross negligence if the code is kept nearby the card in a secured place. However, the code must be in a well-disguised to make it unreadable to others.[8]

A customer may not be declared to have acted with gross negligence when keeping the PIN and the card nearby each other if two conditions are fulfilled. First, the card holder must have disguised the code. A card holder's creativity in disguising the code can be a decisive element in determining whether he has acted with gross negligence. Second, it is also required that both the card and the disguised code are kept in a secure place. Limiting access to both can be achieved, for example, by placing the card and the disguised code in a locked container in a car, locked cabinet in an office or school, or a safe in a house.

From the foregoing, it is suggested that a customer will be considered as having acted with gross negligence if the customer keeps the PIN and the card together in an unsecured place (where it is possible for other persons to have access to the card) and the code is not well disguised. In other words, two security features are expected to be in place. First, the access to the physical card and code must be secured. Second, the code must be in a disguised form that makes it difficult for others to know the actual code.

Evidence

The general rule cited by the court in the case was Ot. Prp. (1998-99) Number 41, which stipulates that a court should not assume that a customer acts with gross negligence unless there is specific evidence of this. The legal reasoning centers around the fact that if a PIN is known to an unauthorised party, it is not a sufficient ground to assume that customer has acted with gross negligence. Relating the requirement of specific evidence to the security features mentioned previously, it is suggested that to declare a customer as having acted with gross negligence, the court must have evidence that (i) access to the physical card and code is not limited to the customer, and (ii) the code that is kept together with the card is in a badly disguised form, making it possible for others to know the code.

Despite the foregoing, the court inferred that it was most likely that the code had been kept by Jørgensen together with the card in a badly disguised form that made it possible for others to know the code – in other words, he was not telling the truth. The bank did not submit any evidence as to whether the code, which was allegedly kept together with the card, was disguised or if the code was disguised, whether it was disguised badly. The court did not go into specific discussion on the code's form of representation. The problem is that the court's declaration that Jørgensen had acted grossly negligencely was not supported by the evidence required by the law.

The reasoning on which the court grounded its jugdment that Jørgensen had acted grossly negligently is not clear. As previously discussed, the court was of the opinion that the level of security provided in the Cresco Card was not the highest, and further implied that the code may have been broken if the time period between its stealing and misuse was longer than actually happened. Expert witness testimony seemed to lend support to this opinion. So it was clear that the court did not doubt that the PIN in the Cresco Card was breakable.

In the absence of specific evidence that (i) Jørgensen had indeed kept the PIN together with his Cresco Card and (ii) the code that was allegedly kept together with the card was not disguised or badly disguised, it is questionable why the court considered that Jørgensen was not telling the truth. Indeed the court noted that the experts had different opinions on how long the code in double-DES security system can be broken ranging between seconds, minutes or hours. However, the misuse happened in more or less one hour after the card was stolen, which is within the time frame mentioned by the experts. Therefore, there

7 *For example: Bankklagenemnda 95352/96010, BKN 91459/93041, BKN 92306/94030 and BKN 95073/95070. See also Susanne Kartstoft, Elektronisk betaling i forbrugerforhold -ansvars- og bevisproblemer- retlige overvejelser ved brug på interntettet, TemaNord 1998:590, First Report (Copenhagen: Nordisk Miniterrad, 1998), p. 130. For a general discussion, see Stephen Mason, ' Debit cards, ATMs and negligence of the bank and customer' , Butterworths Journal of International Banking and Financial Law (March 2012): 163-173, which includes case law from a number of jurisdictions.*

8 *See: BKN 96094/96042, BKN 93399/95024 and BKN 96177/96043. See also: Susanne Kartstoft, Elektronisk betaling i forbrugerforhold -ansvars- og bevisproblemer- retlige overvejelser ved brug på interntettet, TemaNord 1998:590, First Report (Copenhagen: Nordisk Miniterrad, 1998), pp. 130-131.*

was a possibility, however small, that the code of the Cresco Card was broken in the short time period between the theft and misuse of the card. Furthermore, the court also did not explore the possibility that the thiefs might either (a) have obtained the correct PIN easily, or (b) have used an intervention technology device that made withdrawals possible without the correct PIN, since the authorization terminal can be led to believe that the correct PIN was entered.[9]

Even if it is to be argued that the court was of the opinion that the security provided in the card is the unbreakable triple-DES system, the court should have been more thorough and elaborate in its reasoning. The court noted itself that a system security that was considered unbreakable before, the double-DES system, turned out to be breakable after all. This was made possible by the development of intervention technology. Given the continuously rising speed of developments in technology, the court should have shown awareness of the possibility that a technology, no matter how good it is, may be broken by tomorrow's technology. Intervention technology that facilitates crime is mostly developed by persons with bad intentions, who keep a low profile, and therefore it is not possible to be fully sure if the latest developments in intervention technology have out-run the highest level of technology the banks implement have at any given time.[10] The nuance was not captured in the court judgment in the case.

Customer protection

Presumably, the court did not want to declare the code in the Cresco Card was broken because there was no evidence to that effect, and the bank had argued that the code in the Cresco Card was of high security level. Here the court had acted with prudence.

Unfortunately, court prudence did not seem to be implemented when examining Jørgensen's conduct. It was clear that the bank did not have any evidence of Jørgensen keeping the code together with the Cresco Card, and Jørgensen had argued that code of the Cresco Card was locked in a safe in his house. Despite this evidence, the court declared Jørgensen had acted with gross negligence. It was as if the court had considered the mere fact that the Cresco Card had been used with the alledgedly correct PIN was sufficient evidence of the grossly negligent conduct of the customer.

From the foregoing it can be submitted that the court had leaned towards banks instead of the customer. In itself this tendency is worthy of criticism. Customers have limited resources to prove that they had not acted grossly negligently. Customers also have no say on which type of security system that is used by the bank. On the contrary, banks can easily allocate resources to investigate or prove matters. Banks also decide the level of security to be used in payment cards. By leaning towards the bank rather than customers in doubtful circumstances such as in this case, the court protected the resourceful rather than the weaker party. Such an approach is against the basic principle of consumer protection law that provides and encourages protection of parties with weaker bargaining position.

The tendency of the Norwegian courts to lean towards banks was also shown in the recent and much discussed Øiestad case.[11] The facts of the case are as follows: Paal Øiestad was in Rome in September 2008 on holiday, together with his partner and son. A credit card from MasterCard owned by the family was stolen and the card was charged with over Nok 50,000 before it was cancelled. The Øiestad family had three cards with the same code and they used the cards every day. Øiestad insisted that they had not written down the code anywhere, because they had committed the code to memory. The bank, DnB NOR Bank ASA, argued before the Complaints Board and the District Court that the customer had acted with gross negligence by allegedly keeping the PIN together with the stolen and misused bank card. This meant that a thief could misuse the card. As background reasoning, the bank referred to the fact of the timing between the last use of card by the customer and that the misuse of the card occurred within one day. The bank won the case before the Complaints Board and District Court. Øiestad appealed the case.

While waiting for the examination by the appeal court, Øiestad received a letter from DnB NOR dated 12 June 2012.[12] Under the letter, the bank offered an apology for having accused Øiestad and his family of gross negligence by keeping the PIN together with the card. The letter mentioned that the bank just recently had been informed

9 *For a description of this intervention technology, see Dr. Stephen J. Murdoch, 'Chip and PIN is broken', ISSE GI-Sicherheit 2010, available at http://www.cl.cam.ac.uk/~sjm217/talks/isse10chipandpin.pdf.*

10 *Maryke Silalahi Nuth, 'Taking advantages of new technologies: For and against crime', Computer Law and Security Report 24(5) (2008), 437- 446.*

11 *Svein Erik Furulund, 'Blir ikke trodd av DnB NOR', Aftenposten, 1 February 2010, available at http://www.aftenposten.no/okonomi/innland/Blir-ikke-trodd-av-DnB-NOR-5317185.html; see also: Ida De Rosa, 'Kortsvindel sak kan få følger for mange', Aftenposten, 27 June 2012, available at http://www.aftenposten.no/okonomi/Kortsvindelsak-kan-fa-folger-for-mange-6915861.html; Karina Jørgensen, 'Helomvendig fra Storbank', NRK, 27 June 2012, available at http://www.nrk.no/helse-forbruk-og-livsstil/1.8222700.*

12 *A translation of the letter is included in the annex to this article, and a scanned copy of the original letter is available at http://www.forbrukerrådet.no/_attachment/1130286/binary/8413.*

by their sub service supplier that transactions on the Øiestad family MasterCard in Rome in 2008 had been conducted without using any PIN, as had been argued by the Øiestad family from the beginning. The Øiestad family and the bank agreed to settle the case amicably. The bank agreed to pay for all the costs incurred by the Øiestad family (including legal fees and court fees) and the Øiestad family received compensation from the bank.

The issue on how the unauthorized use of the Øiestad family's card could be used without using the PIN is not discussed here. It should be noted that the bank in the Øiestad case happens to be the same bank behind the issuance of Jørgensen's Cresco Card. The arguments submitted by the bank in the Øiestad case seem to be similar to those in Jørgensen's case. The implication of this case on the Norwegian court practice has yet to be seen.

It took three years before the Øiestad family was notified by the bank that the transactions on Øiestad's misused card was conducted without using any PIN. The bank, as in the Jørgensen case, did not submit any evidence that Øiestad had kept the PIN together with the stolen card. Notwithstanding, the Complaints Board and court found that Øiestad had acted with gross negligence. Again, the court, as in Jørgensen case, leaned towards the bank, because the court was willing to declare Øiestad had acted with gross negligence without specific evidence, and the court instead put much emphasis on the fact that the stealing and misuse of the card took place within a day.

Both the Jørgensen case and the Øiestad case show that the task to ascertain fully whether a customer has acted grossly negligently is certainly not an easy one. In both cases, the banks failed to submit specific evidence that their customers had acted with gross negligence. For customers as the party with lesser resources, it is even more difficult to prove that they had not acted grossly negligently. In examining cases of misuse of cards, the court should have at least required the bank to put forward data and information logs of the unauthorized payment transactions showing whether PIN was indeed used. Based on the case circumstance and examination in both the Jørgensen case and the Øiestad case, it is suggested that the respective courts should not have so readily accepted such poor quality evidence from the banks.

Applicable rules and its developments

The legal basis used by the court to set the liability in the Jørgensen case was section 35 paragraph 2 of Lov om finansavtaler og finansoppdrag [Finansavtaleloven] 25.6.1999 No. 46 (Act on Financial Contracts and Financial Assignments)[13] ('Financial Contracts Act') as applicable in 2004. Under this Act, an account holder is liable for up to kr 8,000 for loss caused by the misuse of his or her card if (i) the misuse is made possible by the grossly negligent behaviour of the card holder, or (ii) the account holder failed to notify the loss to the card issuer as soon as possible or within the reasonable time after the loss should have been discovered.

Since 2004, the Financial Contracts Act has been amended twice by way of Law Number 81 dated 19 juni 2009 nr. 81 as enforced on 1 November 2009 ('Amended Act of 2009') and Law Number 42 dated 18 nov 2011 nr. 42 as enforced on 1 January 2012 ('Amended Act of 2011'). These amendments were conducted to implement the Payment Services Directive[14] in Norway.[15]

The prevailing general rules relating for responsibilities relating to use of payment instrument are provided under section 34 of Amended Act of 2009 as follows:

1. A customer who has the right to use a payment instrument shall use it in accordance with the conditions of the issuance and use of the payment instrument, and shall take all reasonable precautions to protect the personal security system associated with the payment instrument as soon as the instrument is received. In addition, the customer shall without undue delay inform the institution or the party the institution has nominate, if the customer becomes aware of the loss, theft or misappropriation of the payment instrument, or unauthorized use (section 34 paragraph 1).

2. The institution issuing a payment instrument shall, without any consequence on customer's duty provided on point 1 above, ensure the personal security system

13 *Law Number 46 dated 25 June 1999.*

14 *Directive No. 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC (Text with EEA relevance) OJ L319, 5.12.2007, p. 1–36.*

15 *Online banking services and the need for amendments to the Financial Contracts Act to implement the Payment Services Directive in Norway, see: Banklovkommisjonen (Banking Law Commission), Norges offentlige utredninger 2008:21 (Oslo: Departementenes servicesenter Informasjonsforvaltning, 2008), pp: 7-10.*

associated with the payment instrument is not accessible to anyone other than the customer who is entitled to use the payment instrument. In addition, the institution shall ensure that the customer at any time may make notification referred to in point 1 above or request that any blocking of the payment instrument be repealed. The institution shall also ensure that the customer, within 18 months from date of such notification, may provide written evidence to have made such a notification, and shall also prevent any use of a payment instrument after the said notification has been made (section 34 paragraph 2).

3. The institution bears the risk of sending a payment instrument to the customer and personal security system associated with the instrument (section 34 paragraph 4).

As can be noted from the above, in the case of stolen cards, section 34 of Amended Act of 2009 provides clarity as to the card holder's obligations to report the conditions that pose a risk of misuse arises that is, at the moment the card holder actually obtains knowledge that the card is stolen.[16]

Furthermore, section 34 of the Amended Act of 2009 provides an obligation on the bank to ensure the personal security system associated with the payment instrument is not accessible to anyone other than the customer who is entitled to use the payment instrument. It is submitted here that this section can be used as a legal basis to require banks to put in place a high level security system that can ensure that no unauthorized use of a payment instrument can be conducted. This is certainly a welcome development to correct the practice of using low level security systems in payment card protection.

Another article of relevance to the topic of this paper is section 35 of the Financial Contracts Act. This section was the subject of an amendment both in the Amendment Act of 2009 and the Amendment Act of 2011. The section is applicable to both debit and credit cards and contains provisions relating to the misuse of account and payment instruments as follows:

1. The institution shall generally be considered responsible for all losses due to unauthorized payment transactions unless otherwise provided by this section. A payment transaction is unauthorized if the customer has not consented to the transaction (section 35 paragraph 1).

2. The customer shall be liable for up to Nok. 1,200 for loss by an unauthorized payment transactions due to the use of a lost or stolen payment instrument if the personal security procedure is used, or due to misappropriation of a payment instrument if the customer has failed to protect the personal security system and the bpersonal security system is used (section 35 paragraph 2).

3. The customer shall be liable for the entire loss on unauthorized payment transactions if the loss is due to negligence by the customer or the customer has failed to meet one or more of its obligations under section 34 paragraph 1. If the payment transaction has occurred with the use of an electronic payment instrument, the customer shall only be liable up to Nok 12,000. If the loss is because the customer has willfully failed to fulfill their obligations under section 34 paragraph 1, the customer shall bear the entire loss. The same applies if the loss is due to the customer having acted fraudulently (section 35 paragraph 3).

4. Unless the customer has acted fraudulently, the customer shall not be liable for losses resulting from the use of lost, stolen or unauthorized payment instruments that take place after the customer has notified the institution that pose serious use of misuse of payment card – for example that a payment instrument is lost or a code or other security procedure may have become available to unauthorized persons. The customer is not liable for any loss as mentioned if the institution has not ensured that the customer can make such notification (section 35 paragraph 4).

5. If the customer denies having authorized a payment, the use of a payment instrument is not in itself to be regarded as sufficient evidence that the customer has agreed to the transaction, or that the customer has acted fraudulently or willfully or grossly negligently failed to fulfill one or more of its obligations under section 34 paragraph 1. The institution shall have to prove that the transaction was authenticated, properly registered and recorded and not affected by technical failure or other error (section 35 paragraph 5).

The above-mentioned amendments to section 35 of Financial Contract Act offer much clarity in relation to the distribution of liability in cases of the misuse of payment cards. More protection to customers is

16 See also BKN 2011-028 and BKN 2011-039.

provided by way of the express stipulation that the use of a payment instrument in itself cannot be regarded as sufficient evidence that the customer has acted fraudulently or willfully or grossly negligently, which in the Jørgensen case seems to be the situation. In addition, the section also sets a clear placement of burden of proof by stipulating that the institution or bank shall be the party responsible to prove that the transaction was authenticated, properly registered and recorded and not affected by technical failure or other error. This is in line with the principle of consumer protection providing protection to the weaker party such as bank customers.

Concluding remarks

The Norwegian legal practice has for some time shown a tendency to lean towards banks in cases of misuse of payment cards. Customers have been declared by courts to have acted with gross negligence, even though no specific evidence to that effect was submitted before the court. The Jørgensen case is an example of such an experience. The development of legal rules in Norway since 2004 have been helpful in providing clarification on some issues relating to the distribution of liability in the case of misuse of payment cards, while at the same time promoting better customer protection. The recent development in the Øiestad case brings hope of a change in the Norwegian legal practice that each bank and their customers shall be placed in their respective rightful position.

Maryke Silalahi Nuth is a Post-doctoral Research Fellow at the Norwegian Center for Computers and Law, Institute of Private Law, Faculty of Law, University of Oslo. Her main research areas include on-line contracting, electronic payment systems, IT-related crime, privacy, security and data protection.

http://www.jus.uio.no

Annex

Pål-Gunnar Øiestad
Arnes vei 3
0488 Oslo

Our ref: OP KBT Kontotjenester Elektronisk kanal/ PSvOSLO, 13

Date: June 2012

Stolen MasterCard

I refer to our telephone conversation on Monday 12 June and the meeting that you and Supreme Court barrister Arne Meltvedt had with our attorney Trond A. Lie regarding the abovementioned matter.

The bank was recently informed by our sub service supplier that the PIN code was not used with your stolen Master Card in Rome 2008. You were right in your claim, and that is now confirmed.

We can only strongly regret that you and your family have lived with these accusations for over three years, and there are no grounds for claiming that you have been negligent.

Again, we can only apologize.

With warm regards
For DNB Bank ASA

Petter Sverreng
Seksjonsleder

- DNB Bank ASA

Postadresse: NO-0021 Oslo
Tif: 04800
Foretaksregisteret:
www.dnb.no

Besøksadresse: LØRENFARET 1 A, OSLO
Faks: NO 984 851 006 MVA