SUPREME COURT'S
JUDGMENT

Case no.

delivered in Stockholm on 21 June 2022

T 4623-21

PARTIES

Appellant

MT

Counsel: Attorney MN

Respondent

Länsförsäkringar Bank Aktiebolag, company registration no. 516401-9878
106 50 Stockholm

Counsel: Attorney EF

Counsel: Attorney SA

THE MATTER

Claim

RULING APPEALED

Judgment of the Svea Court of Appeal of 2021-06-23 in case T 8893-20

THE SUPREME COURT
Riddarhustorget 8

Postal address
Box 2066
103 12 Stockholm

Telephone 08-561 666 00
Fax
E-mail: hogsta.domstolen@dom.se
www.hogstadomstolen.se

Office hours
08:00–12:00
13:15–16:00

JUDGMENT

The Supreme Court modifies the judgment of the court of appeal in respect of the substantive matter and orders Länsförsäkringar Bank Aktiebolag to pay MT SEK 385,000 and interest in accordance with Section 6 of the Interest Act from and including 5 November 2019.

The Supreme Court modifies the judgment of the court of appeal also on the question of costs of litigation and releases MT from the obligation to compensate Länsförsäkringar's costs of litigation in the district court and the court of appeal, and orders Länsförsäkringar to compensate MT for his costs of litigation:

– in the district court in the amount of SEK 112,500, of which SEK 87,280 relates to counsel fees, and interest in accordance with Section 6 of the Interest Act from and including 3 July 2020; and

– in the court of appeal in the amount of SEK 24,500, of which SEK 19,600 relates to counsel fees, and interest in accordance with Section 6 of the Interest Act from and including 23 June 2021.

Länsförsäkringar shall compensate MT for his costs of litigation in the Supreme Court in the amount of SEK 27,125, of which SEK 21,700 relates to counsel fees, and interest in accordance with Section 6 of the Interest Act from and including the day of the Supreme Court's judgment.

CLAIMS IN THE SUPREME COURT

MT has claimed that the Supreme Court shall order Länsförsäkringar Bank Aktiebolag to pay him SEK 385,000 and interest.

Furthermore, MT has claimed that the Supreme Court shall release him from the obligation to pay Länsförsäkringar's costs of litigation in the district court and the court of appeal and award him compensation for costs of litigation incurred there.

Länsförsäkringar has opposed modification of the judgment of the court of appeal.

The parties have claimed compensation for their costs of litigation in the Supreme Court.

REASONS FOR THE JUDGMENT

What is at issue in the case

1. The general rule is that an account holder of a bank or of another payment service provider is not liable for a transaction that has been carried out without the consent of the account holder or another person who is authorised to use the account (unauthorised transaction). By virtue of the fact that withdrawals, transfers from accounts and other transactions are currently often carried out by the use of the account holder of their own authorisation codes for authentication purposes, the main rule has been subject to significant exceptions.

2. The issue in the case is whether a consumer who has acted with gross negligence by disclosing their authorisation codes should also be deemed to have acted particularly reprehensibly and therefore shall be liable for the entire amount in relation to the bank (see Chapter 5 (a), Section 3 of the Payment Services Act (2010:751)).

Background

3. MT was a bank customer of Länsförsäkringar and Skandinaviska Enskilda Banken (SEB). In August 2018, he received a call from a fraudster who stated that he was calling from SEB's security division.

4. The fraudster stated that MT had not responded to a letter from SEB in which the bank required written consent for the bank's handling of personal data in accordance with the General Data Protection Regulation (GDPR) and that MT was therefore obliged to visit a bank branch in order to consent to the bank's processing of personal data. In the event he failed to do so by the following day, he would be struck off as a customer of the bank. When MT inquired why he could not provide his consent by e-mail, the fraudster replied that the bank had determined that written consent was necessary for security reasons. MT stated that he could not make it to the bank branch on time and asked whether the problem could be solved in some other manner. He was then urged to log in to SEB with his mobile BankID in order to approve the processing of personal data. When logging on, MT was presented with the text "I am identifying myself at: Länsförsäkringar". When MT asked about this, the fraudster explained that the text was a result of the fact that MT's BankID had been issued by Länsförsäkringar.

5. After the terms and conditions regarding the GDPR had been accepted, the fraudster claimed that MT had an old BankID and that he needed to go to a bank branch to renew it. MT asked if he could renew it in some other manner, to which the reply was that he could, in such case, use his bank security token. Since MT would not have access to the bank security token until he returned home, they scheduled a telephone meeting for later that evening. The fraudster also asked about MT's roots, and told him that his parents also came from Iran. They continued the conversation in Persian.

6. During the conversation that evening, MT followed the fraudster's instructions and entered numbers into the bank security token and also provided the response codes generated by the bank security token. It thereby became possible for the fraudster to order a new BankID in MT's name and, *inter alia*, transfer a total of SEK 397,000 from his account at Länsförsäkringar.

The case in the district court and court of appeal

7. MT, who conceded that he had acted with gross negligence, claimed that Länsförsäkringar was to be ordered to pay him SEK 385,000 and interest, equal to the amount transferred with a deduction of SEK 12,000. MT essentially alleged that he, however, had not acted particularly reprehensibly.

8. The district court granted MT's claim. The court of appeal, on the other hand, dismissed the plaintiff's claim on the merits.

Liability for unauthorised transactions

9. The Swedish rules regarding liability for unauthorised transactions are based on the First and Second Payment Services Directives.[1] The provisions of the First Payment Services Directive (PSD1) which concerned liability for unauthorised transactions and related issues were originally implemented in the Act on Unauthorised Transactions with Payment Instruments (2010:738). In conjunction with the implementation of the Second Payment Services Directive (PSD2) in 2018, the act was repealed and the rules regarding

[1] See Directive 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 and Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No. 1093/2010, and repealing Directive 2007/64/EC.

unauthorised transactions were instead incorporated in Chapter 5 (a) of the Payment Services Act.

10. A payment service user, e.g. an account holder, is obliged to protect personalised security credentials linked to a payment instrument and otherwise comply with the terms and conditions which, according to the agreement with the payment service provider, are applicable to the use of the payment instrument (see Chapter 5, Section 6 of the Payment Services Act).

11. The term *payment instrument* is defined as an account card or other personal instrument or a personal routine which, according to contract, is used to initiate a payment order. The definition encompasses, for example, credit cards, BankID, and bank security tokens. *Personalised security credential*, which is defined as a personally adapted feature provided by the payment service provider to the payment service user for the purposes of authentication, means, for example, a personal code. (See Chapter 1, Section 4.)

12. Chapter 5 (a) regulates the liability relationship between a payment service provider and an account holder when an unauthorised transaction has occurred from an account holder's account. *Unauthorised transaction* means, according to the regime, a transaction which is carried out without the consent of the account holder or another person who, according to the account agreement, is authorised to use the account (see Chapter 1, Section 4).

13. In the event an unauthorised transaction has been carried out, the main rule is that the account holder's payment service provider is to restore the account to the position it would have had had the transaction not been carried out (see Chapter 5 (a), Section 1). In the event the unauthorised transaction could have been carried out as a consequence of the fact that the account holder did not protect the account holder's personalised security credentials in the manner required in accordance with Chapter 5, Section 6, the account

holder is liable for the amount, but not to exceed SEK 400 (see Chapter 5 (a), Section 2).

14. When an unauthorised transaction has been able to be carried out as a consequence of the fact that the account holder, due to gross negligence, has disregarded an obligation in accordance with Chapter 5, Section 6, the starting point is that the account holder is liable for the entire amount. The liability, however, is limited to not more than SEK 12,000 where the account holder is a consumer. In the event the consumer has acted particularly reprehensibly, however, he or she is liable for the entire amount (see Chapter 5 (a), Section 3.)

15. When an amount has been paid as a consequence of an unauthorised transaction, the starting point is thus that the consumer is not liable for any part. Depending on the manner in which the consumer has acted, liability on the part of the consumer increases, in which context the liability:

- is limited to not more than SEK 400 where the consumer has not protected the consumer's personalised security credentials;
- is limited to not more than SEK 12,000 where the consumer has acted with gross negligence; and
- is unlimited where the consumer has acted particularly reprehensibly.

16. The regime is based, *inter alia*, on the notion that there is a socio-economic and crime-prevention interest in reducing the handling of cash for the benefit of card use and internet payments. Accordingly, there is a benefit in an account holder being able to use payment instruments without risking economic losses which are too onerous. The desire to encourage the use of various types of payment instruments has given rise to a regime according to which the parties, to a certain extent, share the risk of unauthorised

transactions. This means, *inter alia*, that the economic liability is to be sufficiently onerous that the account holder attempts as far as possible to comply with the terms and conditions applicable to the use of the payment instrument. This has resulted in a balance according to which the account holder is responsible for not more than SEK 12,000 for grossly negligent acts and is fully liable only in conjunction with particularly reprehensible behaviour. (See Government Bill 2009/10:122, p. 16 ff.)

More specifically regarding liability in conjunction with particularly reprehensible acts

17. The regime in Chapter 5 (a), Sections 2 and 3 of the Payment Services Act implement the provisions of Article 74 of the PSD2. It follows from the directive that the account holder shall bear all losses relating to any unauthorised payment transactions if they were incurred by the account holder acting fraudulently or using the payment instrument with intent or gross negligence in contravention of the terms and conditions for the issuance and use of the payment instrument or by failing to take all reasonable measures to protect their personalised security credentials. Where the account holder has neither acted fraudulently nor intentionally failed to fulfil its obligations, Member States may reduce the liability taking into account, in particular, the nature of the personalised security credentials and the specific circumstances under which the payment instrument was lost, stolen or misappropriated.

18. It is thus apparent from Article 74 that consumers at all times have unlimited liability in terms of amount when the loss has been caused by the consumer acting fraudulently or when the consumer intentionally disregards the requirements for handling of the security credentials. On the other hand, the liability may be limited when the loss has been caused by action which is deemed to be grossly negligent.

19. By virtue of the regime in Chapter 5 (a), Sections 2 and 3 of the Payment Services Act, Sweden has exercised the possibility to limit the liability in cases of gross negligence when the account holder is a consumer.

20. In a comparable manner, Denmark and Norway have limited the amount of the consumer's liability in conjunction with the consumer's negligent acts (see Section 100 of the Norwegian Payments Act, law no. 652 of 08/06/2017 and Sections 4-30 of the Financial Agreements Act, law 2020-12-18-146). As far as Denmark is concerned, furthermore, unlimited liability applies in respect of losses when the account holder has intentionally provided the account holder's personalised security credentials to the person who has carried out the unauthorised transaction under such circumstances that the account holder was aware or should have been aware that there was a risk of misappropriation. In a similar manner, it follows from the Norwegian regime that the account holder is liable for the entire amount of the loss where the account holder has intentionally violated the account holder's obligations in such a manner that the account holder must have understood that the violation could entail a proximate danger of misappropriation of the payment instrument.

21. As regards unlimited liability, Sweden requires, as mentioned, that the consumer has acted particularly reprehensibly (see Chapter 5 (a), Section 3). The expression does not appear either in the PSD1 or PSD2. Nor is there any comparable requirement in Danish or Norwegian law.

22. The question is thus what action is to be deemed particularly reprehensible. In order to be able to determine how serious the consumer's action must be in order to reach the level of the requirement, there is cause to first determine what, according to the regime, is meant by a *grossly negligent act*. In this context, it may be natural to seek guidance in the provisions of civil legislation in which the same term is used. The term *gross negligence*,

however, may not be ascribed a uniform meaning in all areas in which it is used (see the "*Mariefred's School*", case NJA 1992, p. 130).

23. Certain guidance for the interpretation, on the other hand, is obtained from both the regime of the directive as well as the preparatory works for the Payment Services Act. According to the recitals of the PSD2, what is negligent may be evaluated according to national law. However, gross negligence according to the directive should be more than mere negligence and cover conduct exhibiting a significant degree of carelessness. For example, mention is made of keeping the security credentials used for authorisation of a payment transaction beside the payment instrument in a format that is open and easily detectable by third parties. (See Recital 72 of the PSD2.)

24. The preparatory works state that gross negligence in the sense referred to Chapter 5 (a), Section 3, must involve a marked deviation from the standard of care in which the account holder has been reckless to such a degree that he or she is not excused; minor cases of sloppiness or temporary absent-mindedness thus do not constitute a grossly careless act (see Government Bill 2009/10:122, p. 27 ff.). The preparatory works provide a number of examples of cases of gross negligence. These involve the use of account cards and are thus of limited guidance as regards other payment instruments.

25. It is apparent from the very wording alone of the regime that, in order for the consumer's action to be deemed to be particularly reprehensible, something more than an act which is grossly negligent is necessary. The act must thus be more serious than a marked deviation from normal care. This comports well with the fact that, according to the preparatory works, it is particularly the case where the action constitutes a qualified form of gross carelessness that is intended. The preparatory works state that the regime is to cover cases in which the consumer has acted so reprehensibly in relation to the

payment service provider that it would be appalling if the provider needed to bear liability for any part of the amount. Thus, according to the preparatory works, this involves cases in which the consumer, by virtue of the consumer's actions, may be deemed to have been indifferent to the risk of unauthorised transactions. (*Cf.* Government Bill 2009/10:122, pp. 17 f. and 27 ff.)

26. It follows from the above that the consumer is responsible for the entire amount when the consumer has acted fraudulently (see Article 74 of the directive). The same should apply when the consumer has intentionally provided personalised security credentials, e.g. log-on information for a BankID or codes to a bank security token, to an unauthorised person and was then aware or had cause to suspect that there was a significant or proximate risk that his or her actions would give rise to a loss (compare Article 74 and the regime in Danish and Norwegian law).[2]

27. In addition to these cases, it may be deemed to be particularly reprehensible when the consumer – even if he or she does not intentionally provide the personalised security credentials to an unauthorised person – was indifferent to the risk of unauthorised transactions. A particularly reprehensible act thus exists where the consumer was aware, i.e. actually understood, that there was a risk of an unauthorised transaction but nonetheless acted in such a manner as constitutes a breach of Chapter 5, Section 6 (see paragraph 10). With this assessment, the person to whom he or she understood that the personal authorisation credential was being provided is of particular importance.

---

[2] *Cf.* Marte Eidsand Kjørven *et al.*, *BankID-opplysninger på avveie - om vilkårene for aktivering av forsettsansvaret etter finansavtaleloven § 35 og ny finansavtalelov § 4-30 (4),* Lov og Rett, 2021, p. 335 ff., Marte Eidsand Kjørven, *Who Pays When Things Go Wrong? Online Financial Fraud and Consumer Protection in Scandinavia and Europe*, European Business Law Review 2020, p. 77 ff. and Susanne Karstoft, *Misbrug af NemID til optagelse af lån*, UfR 2019 B p. 339 ff.

28. The determination of whether a consumer has acted particularly reprehensibly shall, in principle, be made objectively, i.e. on the basis of the manner in which a comparable consumer would typically have acted in the same situation. In the determination in the assessment of any liability when the consumer, in conjunction with fraud, has not protected his or her personalised security credentials linked to the payment instrument, there is reason to ascribe particular weight to certain factors. Amongst these are the setting and situation in which the consumer found him or herself and his or her possibility to defend against an unauthorised transaction. The consumer's age and experience may be significant. Consideration should also be given to how cunning the fraud has been and what the consumer understood or should have understood regarding the information provided to the fraudster and the possible consequences of providing it. (*Cf.* Government Bill 2009/10:122, p. 27 ff.)

29. It is the payment services supplier who bears the burden of proof that the consumer has acted particularly reprehensibly (*cf.* Government Bill 2009/10:122, p. 28).

The assessment in this case

30. It is common ground that MT, through gross carelessness, disregarded the obligation to protect the codes for his mobile BankID and the response codes generated by his bank security token and that this gave rise to the unauthorised transactions.

31. The General Data Protection Regulation, GDPR, entered into force at the end of May 2018 and was an event which to a great extent gave rise to contacts between companies and consumers in the course of that year. The question about which MT was contacted in August 2018 pertained to the alleged requirement of written consent for the bank's GDPR processing which

could not be provided by e-mail. It is apparent that MT, in conjunction with the first conversation, was under the impression that urgent measures needed to be taken by him in order for him not to lose the possibility to use his account and he was stressed thereby.

32. It is apparent from the investigation, furthermore, that MT perceived the fraudster to be a calm and professional bank official who provided explanations which MT understood to be reasonable in response to the questions posed by him. This applied, for example, to the question as to why the processing of personal data was to be approved in a certain way and why, during the first log-on by means of the BankID, he was presented with information that MT identified himself at Länsförsäkringar despite the fact that the fraudster said he was calling from SEB.

33. The fraudster further succeeded in building up MT's trust during the first telephone conversation. He also persuaded MT, after first having encouraged him to visit a bank branch, to himself propose the solutions which provided the fraudster with the possibility, in the course of the second conversation and by means of the codes from the bank security token, to create a new BankID and carry out the unauthorised transactions.

34. Accordingly, it is apparent from the investigation that MT was exposed to a cunning deception. However, he demonstrated significant negligence in that, during the second conversation, he provided the codes from his bank security token. Nevertheless, it has not been evinced that he intentionally provided the codes to an unauthorised person in conjunction with both of the conversations. Nor may it be deemed evinced that MT acted as he did with an understanding that there was a risk of the unauthorised transactions which were carried out. Thus, it has not been a question of such action as is required for a consumer to be deemed to have acted particularly reprehensibly.

35. Accordingly, MT's action will be granted. The claimed amount and the manner of calculating the interest has been stipulated.

Costs of litigation

36. With this outcome, MT shall be released from the obligation to pay Länsförsäkringar's costs of litigation in the district court and the court of appeal.

37. Länsförsäkringar shall compensate MT for his costs of litigation in the district court, court of appeal and the Supreme Court. The costs for expenditures in the district court are stipulated. The costs are otherwise reasonable.

Justices of the Supreme Court Kerstin Calissendorff, Johnny Herre (reporting Justice), Stefan Johansson, Cecilia Renfors and Johan Danelius participated in the ruling.
Judge referee: Margareta Sandén