Science of Law Journal (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/law.2023.021007
ISSN 2616-2296 Vol. 2 Num. 10

Allocation of Liability for Bank Card Theft

Ren Xiaonan

Department of Law, China University of Political Science and Law, Beijing, China
rxncupl@163.com

Keywords: Bank card theft, Liability allocation

Abstract: The Supreme Court issued a new judicial interpretation on bank card theft in May 2021, which determined the no-fault liability of banks in the phenomenon of bank card theft. However, although the interpretation is based on the position of protecting financial consumers, it does not take into account the type of cardholder, the difference between counterfeit card theft and cyber theft. Through differentiate between Small-value electronic fund transfers and large-value electronic fund transfers, cyber theft, a new mechanism for allocating responsibility should be constructed for cyber-skimming of bank card unit accounts: if the bank's payment instructions have passed the security procedures, the cardholder bears the presumption of liability for fault, thus providing banks with an outlet for exemption from liability.

1. Introduction

In recent years, with the rapid development of the digital payment, criminals bank card online theft in a variety of ways and means, the phenomenon of bank card online theft is endless, and a large number of civil lawsuits between cardholders and card issuers have emerged. According to the data of the hunting platform, the number of online frauds occurred in 2019 was 15,505, with a per capita loss of 24,549 yuan, of which the per capita loss of financial fraud, especially credit card fraud, was as high as 4,492 yuan.[1]

Bank card skimming, i.e., unauthorized transactions of bank cards, refers to the reduction of funds or increase of overdraft amount in bank card accounts not due to one's own intention[2]. Specifically, it can be categorized into three types of cases: offline theft of counterfeit cards, offline theft of real cards, and theft. Bank card cyber-skimming occurs through cyber means, i.e. through others stealing and using the cardholder's bank card cyber-transaction identification information and transaction verification information.

The issue of liability allocation for bank card theft mainly centers around the cardholder, the thief and the card issuer. The cardholder should first assume full and final responsibility, and return the entire amount of money stolen based on the legal relationship of infringement. However, in real life, since it is difficult to identify or find the swipers in criminal cases, they can only be transferred to the card issuing bank or the cardholder to bear the risk, so that the card issuing bank or the cardholder can bear the risk by themselves, therefore, this paper only discusses the risk distribution and liability rules between the cardholder and the card issuing bank.

2. Current Legislation and Ruling of Bank Card Skimming Transactions

The latest Bank Card Interpretation, E-Commerce Law and legal provisions related to large-value electronic fund transfers need to be analyzed first; then the sample cases are described in general and analyzed in typical cases to reveal the current legislative and judicial status of bank card cyber-skimming transactions and to find out where they need to be improved.

2.1. Current legislation

For small electronic payments, the relevant legislation is the Bank Card Interpretation and the Electronic Commerce Act.

Online transactions can be carried out through three ways: online banking, payment account-based third-party payment institutions or payment gateway-based third-party payment institutions. Brush theft in the payment account mode refers to the brusher stealing the change in the third-party payment institution, and the parties involved are the third-party payment institution and the customer, not directly involving the card-issuing bank, and the relevant disputes are subject to the E-Commerce Law; whereas in the online banking mode, the brusher steals the amount in the bank card directly, which not only applies to the Interpretation of Bank Cards, but also peculiarly involves the third-party payment institution and other subjects, and applies to the E-Commerce Law.

Article 7 of the Bank Card Interpretation stipulates that card theft should follow the lines of liability for breach of contract, based on articles 577, 591 to 593 of the Civil Code. This article specifies the bank's no-fault liability and the cardholder's liability for negligence and derogation. The Supreme Court held that the reasons are[3]: (1) The act of bank card theft is not an authorized act of the cardholder. (2) The application of no-fault liability in bank card contract disputes is based on the principle of reciprocity of risk and benefit, encouraging card issuers to provide more secure products and services, and protecting the interests of non-defaulting parties to enhance the sense of contract compliance. (3) The provisions relating to fault apply, and if the cardholder fails to fulfill his obligation to keep the password authentication code properly, he will have to share the loss.

At the same time, if the transaction of a sale contract on an online platform is carried out through bank card theft, the content of the E-Commerce Law is also involved. In this regard, Article 57(2) of the E-Commerce Law stipulates the rule of liability sharing, which is that the bank bears no-fault liability, and the cardholder should share the loss if he is at fault.

As for the allocation of responsibility for fraudulent use of large electronic funds, there are legal gaps in China's legislation. The Law of the People's Bank of China and the Law of Commercial Banks only regulate traditional banking business; the Measures for Payment and Settlement mainly target small payment methods such as bills and credit cards; the Measures for the Administration of Electronic Banking Business, and Measures for the Administration of Bank Card Business still mainly regulate the transfer of small electronic funds; with June 2005, China's legislation still exist a legal loophole.

At present, only Article 45 of the Electronic Payment Guidelines (No. 1)(hereinafter referred to as the "Guidelines"), which specifies that banks must authenticate the source of a payment order but also does not explicitly stipulate whether the bank should share in the loss, has provided for loss sharing in the case of a large-value electronic fund transfer.

2.2. Rulings Studies

The author used "credit card", "online" and "theft" as the search keywords on pkulaw, and a total of 18 cases were selected as the research sample for analysis.

2.2.1. Mindset and norms of adjudication

Analysis of cases can be concluded, the bank is liable on the basis of two kinds: one is the bank should bear the liability for breach of contract, because the bank and the customer entered into a credit card contract between the bank, the bank violated the attached obligations, and therefore be liable, such as Pingliang Intermediate People's Court of Gansu Province, the civil end of the judgment No. 983, the People's Court of Mackerel District of Yingkou City, Liaoning Province, the people's court of the civil beginning of the judgment No. 3333, and so on; the other is that the bank should Tort liability, because the bank violated the customer's property rights, and its premise is that the bank has fault, such as Kunming City, Yunnan Province Intermediate People's Court civil final judgment No. 9140. Next, the author will start from these two bases, analyze the court decision there are differences and consensus:

(1) Theory of liability for breach of contract

First, there are different causes of such disputes, including debit card disputes, credit card disputes and savings (deposit) contract disputes[4]. However, the legal relationship between the bank and the customer is not complex, and the two enter into a comprehensive framework contract, which cannot be generalized in terms of a famous contract. This mixed relationship includes the custodial relationship, investment relationship, payment and settlement relationship (i.e., the trust contract relationship), the bank card contract relationship, and so on.

Secondly, the principles of attribution are different, with the idea of fault liability and no-fault liability. In some cases, the cardholder relied on the Commercial Bank Law and the Guidelines to prove that the bank had failed to fulfill the corresponding obligations of confidentiality and notification, and then demanded that the bank bear the liability for breach of contract under Article 509 of the Civil Code. In some cases, the court relied on Article 7 of the Bank Card Interpretation as the basis for its decision, requiring the bank to assume no-fault liability for breach of contract and the cardholder to share the loss according to fault.

(2) Theory of Tortious Liability

Torts are categorized into general and special torts, and the corresponding principles of attribution are the principle of fault liability, the principle of no-fault liability and the principle of fair liability[5]. Here the author does not discuss whether the thief infringes on the customer's claim to the money or ownership, because both can be attributed to the infringement of the customer's property rights, so the tort relationship between the bank and the customer clearly belongs to the general tort.

2.2.2. Definition of cardholder and issuer obligations

In addition to the differences in the basis for the decisions in the line of reasoning, there is also confusion in the courts' definition of the obligations of the cardholder and the card issuer.

Regarding the cardholder's obligation to keep the password properly, there are cases that clicking on the Trojan horse program violates the obligation; there are cases that informing the password to others violates the obligation, such as Pingliang Intermediate People's Court of Gansu Province, (2021) Gan 08 Civil Final No. 983 Judgment, the password set by the cardholder has the uniqueness and secrecy, which is known only to the cardholder, who has the obligation to keep it in strict confidence and keep it properly; therefore, repeatedly handing the debit card to others for business cannot exclude the possibility of password leakage. Lending a debit card for business purposes doesn't eliminate the risk of password exposure. It's assumed that Gao didn't properly safeguard the debit card's password, and thus should be held accountable for any breach.

However, the context in which the password was shared should also be considered. For instance, as per the judgment of the Beijing Municipal No. 2 Intermediate People's Court (2021) Beijing 02

Civil Final 13808, if a cardholder, due to deteriorating eyesight in old age, shared the bank card password with his son to seek assistance in using the card, such a scenario aligns with practical reasoning. Based on the limited rationality and level of attention of natural persons, the cardholder should not be blamed for the absolute obligation of distinguishing the identity information and bank card verification information stolen by criminals through fraudulent means, nor should the cardholder be blamed for maintaining a high degree of vigilance to the bank's SMS notification and verification prompts at all times.

3. Reconstruction of the allocation of liability for bank card skimming transactions

There are many differences between counterfeit card skimming and cyber skimming, the biggest of which is the presence or absence of a physical card. According to the risk allocation mechanism, the risk of transactions should be shared by the cardholder and the card issuer[6]. Therefore the Bankcard Interpretation's unified approach to regulate them based on the position of protecting financial consumers is open to question. By understanding the extra-territorial laws, it is possible to construct a new system of responsibility allocation: the bank and the cardholder agree on the security procedures, and if the bank proves that its payment instructions are in accordance with the security procedures and the cardholder can't prove that he/she is at fault, the bank shall be held liable.

3.1. Differentiation of cardholder types

In terms of legislation, the relevant provisions on credit card cyber theft are reflected in the Bank Card Interpretation and the E-Commerce Law, both of which stipulate the no-fault liability of banks based on the position of protecting financial consumers. However, there are so far no clear provisions in the relevant laws or interpretations on large-value electronic fund transfers.

On the judicial front, while the majority of credit card cybersquatting cases involve individual cardholders, there are also some cases in which a company's bankcard unit account has been swiped. Confusion has also arisen over the application of laws relating to large-value electronic payments, such as the Guidelines, in the context of cybersquatting of bank cards against individuals.

There are significant differences between small-value EFT and large-value EFT in terms of the value orientation, basic principles and main content of the legislation, which should therefore be categorized in terms of legislation. The small-value EFT system is an electronic funds transfer system for individual consumers, which mainly regulates the relationship between bank customers and banks. Large-value EFT systems are EFT systems for brokers and commercial banks in markets such as commodities, and are primarily concerned with the relationship between corporations and banks. The primary purpose of regulating small-value electronic fund transfers (EFT) is to protect consumers, given that the cardholder often has less power compared to the bank. On the other hand, the regulation of EFTs prioritizes equity. It's presumed that companies, possessing professional investment expertise, can comprehend and mitigate the risks associated with substantial fund transactions. Hence, responsibilities should be allocated equitably.

3.2. Distinguishing between counterfeit card fraud and cyber fraud

According to Professors Kuter and Rubin, the loss-sharing mechanism for unauthorized transactions is based on the principles of loss spreading, loss reduction and loss determination[7]. Therefore, they believe that according to the principle of loss dispersion, the bank is the main body to bear the risk; according to the principle of loss reduction, the cardholder is the main body to bear the risk. Therefore, in order to balance the interests of the cardholder and the card issuer, the

cardholder should bear a certain limit of liability, and the rest of the liability should be borne by the bank. The criterion of "a certain limit of liability" is the median value of the amount of cash withdrawn by the cardholder from the bank each time. Because the amount is too small will not promote the cardholder to improve the level of self-caution, the amount is too large for the cardholder. Therefore, from the principles of loss spreading and loss reduction, this paper will explain that counterfeit card theft and theft should be different risk allocation mechanisms.

3.2.1. The principle of loss spreading: the bank assumes the risk

According to the principle of risk diversification, whoever is most likely to spread the risk bears the risk. In the case of bank card theft, the bank can transfer the risk to the cardholder by charging a fee, while the cardholder cannot spread the risk. Therefore the risk should be borne by the bank. However, at the same time, this makes it more expensive for the cardholder to hold a credit card, which is also inherently unfavorable to the cardholder.

3.2.2. The principle of diminution of loss: the cardholder bears the risk

Counterfeit card skimming may occur because banks do not provide a secure and confidential environment for their customers in the vicinity of ATMs, or because they do not have high levels of anti-forgery identification technology. Therefore, in such cases, banks are in a position, have the opportunity and have the ability to prevent the crime by improving their systems and transaction environments. For example, scholars believe that replacing magnetic stripe cards with chip cards can better reduce the risk of skimming[8]. Although the cost is higher, banks do have the ability to prevent it.

In the case of online theft, since the password is the only passport to the transaction, the reason for the occurrence is that most cardholders casually inform others of their passwords or click on the fraudulent links and programs created by the thief to disclose their passwords, so that the thief can conduct transactions by entering the correct account passwords in online banking. Therefore, the risks associated with online payments cannot be prevented simply by banks identifying the risks and improving their technology, because no matter how banks improve their technology, they can only ensure that their own systems do not have problems, and they cannot recognize whether or not the screen in front of the cell phone is actually the cardholder himself or herself. It is also necessary for the cardholder to raise awareness of the need to prevent such risks, "who can minimize the risk who bears the risk", so the cardholder should bear the risk.

3.3. Allocation of responsibility for cyber theft from bank card unit accounts

If the trial of a bank card theft transaction is conducted along the lines of the bank's no-fault principle, the bank, even if it has complied with all reasonable security procedures, will have to bear no-fault liability first, then do its utmost to prove whether the cardholder has disclosed the password, and finally, with a high probability, bear the entire loss. First, this exposes banks to greater risk while spreading the risk to cardholders by charging service fees and other means, forcing many customers not to choose large-value e-payments, but low cost was originally the advantage of large-value e-payments.[9] Second, many cardholders in addition to vulnerable individuals and companies, companies are not the financial consumers we want to protect but also this explanation is protected, which will make the company to reduce the duty of care for large-value transactions. It is therefore necessary to seek a new mechanism for sharing responsibility in order to strike a balance between the interests of banks and cardholders.

The new liability allocation mechanism holds that the cardholder and the bank should first agree on a security procedure and that the cardholder should be held liable if a payment instruction passes

through the security procedure, unless the cardholder can prove that he or she is not at fault.

The new liability regime also has the following advantages: firstly, the law allows the customer to set the scope of payment at the same time as entering into a security procedure agreement with the bank. For example, in a specific agreement, the bank is willing to share the risk with the customer in order not to lose an important customer[10]. Second, higher security verification obligations can be imposed on banks. The security verification obligations agreed by the bank in the security procedure agreement will definitely be fulfilled by the bank proactively to prevent risks[11].

3.3.1. Banks are the ultimate risk takers

Bank card theft cases are not only ordinary civil law cases, but also financial cases. The biggest difference between financial law and other laws lies in the allocation of risk, the core function of commercial banks and other financial institutions is to manage risk, and higher risk is accompanied by higher expected returns. Therefore, the essence of the assumption of responsibility that we are discussing is in fact the sharing of risk, and it is the one who shares the risk when the thief is unable to determine or recover the compensation, because the risk-bearer can still recover the compensation from the thief, and it is the thief who is the final bearer of the responsibility. The ultimate bearer of liability is the skimmer. Therefore, between the bank and the cardholder, if neither the bank nor the cardholder is at fault, the bank must be the ultimate bearer of risk.

3.3.2. Payment instructions that comply with security procedures are at the cardholder's risk

According to the principle of "credit and performance" of the Payment and Settlement Act. Payment and settlement is based on the fundamental principle of credit. In order to implement the settlement principle of "keeping credit", the bank must fulfill the obligations of the trustee, i.e., it should take all kinds of effective measures to strictly implement the payment and settlement system to ensure that the payment and settlement work is carried out normally. Any party should consciously maintain the order of payment and settlement, or will bear all the consequences arising therefrom. At the same time, the cardholder should also abide by the credit, to maintain social credibility. Once the economic contract is established, it has legal effect and both parties must abide by it.

If a payment instruction issued in the name of the cardholder complies with a pre-agreed security procedure such as a password verification code, it constitutes an apparent agent. According to Article 172 of the Civil Code and Article 28 of the Interpretation of the Supreme People's Court on Several Issues Concerning the Application of the General Provisions Part of the Civil Code of the People's Republic of China (Legal Interpretation [2022] No. 6), the payment instruction and the consequences take effect between the cardholder and the issuing bank, the bank as a bona fide counterparty is exempted from liability, and it is up to the cardholder to recover from the person who stole the money.

3.3.3. Presumptive liability for fault of the cardholder

The cardholder's contractual obligation is mainly the obligation to keep the code properly. Some scholars believe that for the proper storage of the password cardholders are only responsible for intent and gross negligence, and should be exempted from liability for general negligence and specific minor negligence. Such as the "Electronic Commerce Law" legislators believe that Article 57, paragraph 2 of the second sentence of the "user fault caused by unauthorized payment" should be interpreted as "the user due to intentional and gross negligence caused by unauthorized payment"[12]. However, some scholars believe that as long as the user is at fault, it should bear full responsibility. For example, according to Li Jianxing, if a user inputs information such as ID

number without noticing the abnormal situation of the link, or if a user receives an unidentified text message and opens the text message link, which leads to the acquisition of personal identification information, etc., as long as it is the user's general negligence that directly causes the theft of brushes, it should be considered that the user is at fault[13].

It is clear that the legislators of the E-Commerce Law have raised the standard of cardholder fault in order to maximize the protection of consumer interests. However, it should be noted that the unauthorized transactions in the E-Commerce Law are generally small transactions for which banks are capable of bearing the risk, while bank card theft is a large-value electronic payment. As can be seen by drawing on the relevant U.S. law, in large-value electronic payments, there can be no bias in favor of the cardholder, and therefore the cardholder needs to bear the full presumption of liability for fault. He or she needs to prove that he or she has no possibility of leakage, otherwise he or she is presumed to be at fault.

3.4. Specific explanation of "security procedures"

In order to make the Security Procedures Rule applicable in our country, two of the conditions need to be further explained, i.e. the security procedures have "commercial reasonableness", "accept in faith", and "acceptance in faith by the bank".

The UCC considers the "commercial reasonableness" of a security procedure to be determined by a combination of the cardholder's expressed wishes to the bank, the bank's knowledge of the type and frequency of the cardholder's payment instructions, the alternative security procedures offered to the cardholder, and the practices of other banks in similar circumstances. At the same time a security program must be "commercially reasonable" if (1) the cardholder declines the bank's offer of a security program after it has been provided and chooses another program (2) the cardholder undertakes in writing to be bound by the agreement with respect to any payment instructions. At the same time, "good faith" means subjective honesty and objective compliance with reasonable commercial standards of fair dealing.

In the case studies above, the courts have found inconsistencies in the obligations of banks, such as whether the bank has a statutory obligation to notify a single transaction or to notify an unusual transaction. However, under the security program, the bank and the customer can agree in advance on a variety of similar security program items, stipulating a variety of authentication methods, such as stipulating "password + verification code + single transaction notification" or "password + verification code + single transaction receiving" and so on. By agreeing on a variety of security procedures to specify the obligations of the bank, it can be well avoided in practice, the obligation to identify the phenomenon of confusion.

4. Conclusions

Compared with counterfeit card fraud, the bank's obligation to recognize counterfeit cards and ensure a secure offline transaction environment disappears, and the bank's attributability is greatly reduced, making it unreasonable for the bank to assume no-fault liability. At the same time, many of the risks associated with online transactions cannot be overcome by banks through improved technology, and the level of care and attention of cardholders must be increased at the same time. Focusing only on the "protection of cardholders" will inevitably lead to overkill, resulting in an unbalanced distribution of risk and loss between cardholders and banks.

Based on the above differences, this paper reconstructs the allocation of responsibility for theft transactions of bank card unit accounts. The bank first proves that it has fulfilled the security procedures; then the cardholder bears the presumption of fault; the bank bears the ultimate risk when both parties are not at fault; and both parties share the loss when they are at fault.

References

[1] The net hunting platform is a joint police-citizen fraud reporting platform formed by the Beijing Municipal Public Security Bureau's security team and the 360 Internet Security Center. Hunting Platform: "2019 Fraud Trend Research Report," released January 9, 2020, https://110.360.cn/index/newsInfo?id=141.

[2] Article 15, paragraph 2, of the Bank Card Interpretation.

[3] "Head of the Second Civil Court of the Supreme Court Answers Reporters' Questions on the Bank Card Regulations." See BYU Law, https://www.pkulaw.com/news/c5fdb2778a72ef8dbdfb.html. Last accessed March 15, 2022

[4] See Decision of the Supreme People's Court on Amending the Provisions on the Causes of Civil Cases (Law [2020] No. 346).

[5] Wang Liming, Research on Tort Liability Law (Previous Volume), People's University of China Press, 2015 edition, pp. 200-201.

[6] Dai Xinyue, Zhang Junkan, and Xu Xiaoxi, "A Typological Study on the Determination and Allocation of Liability in Bank Card Stealing Disputes--Taking 152 Judgments as the Object of Study," in Law Application, No. 3, 2017, p. 54.

[7] Robert D. Cooter & Edward L. Rubin, "A Theory of Loss Allocation for Consumer Payments", Texas Law Review, 1987, p. 90.

[8] Lin Dabiao. "The division of responsibility for encountering cloned cards varies from case to case," People's Court Daily, October 18, 2012, p. 3.

[9] Liu Ying, Li Lisha: "The Law of Large Electronic Funds Transfers under the Perspective of Interest", in Hebei Law, No. 6, 2008, pp. 53-55.

[10] Hu Chao, "Allocation of Fraud Losses in Large Electronic Payment Systems--Related Rules and Implications of Title 4A of the U.S. Uniform Commercial Code," in Journal of Chihuahua College, Vol. 4, No. 4, 2014, p. 48.

[11] Su Pan, "The Construction of the Loss Allocation Mechanism for Bank Card Disputes over Swiping--Centering on Security Procedures," in Law Application, No. 18, 2019, p. 63.

[12] E-Commerce Law Drafting Group, Interpretation of the Provisions of the E-Commerce Law of the People's Republic of China, Law Press, 2018 edition, p. 185.

[13] Li Jianxing, "Rules for Sharing Responsibility for Unauthorized Payments on the Internet", in Legal Science, No. 4, 2020, p. 92.