DUE DILIGENCE OBLIGATIONS FOR PAYMENT SERVICE PROVIDERS

Findings of an analysis carried out by the Team Monitoring Financial Markets at the Federation of German Consumer Organisations (Verbraucherzentrale Bundesverband – vzbv)

10 October 2024

Legal information

Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.

Team Monitoring Financial Markets
MBFinanzmarkt@vzbv.de

Rudi-Dutschke-Straße 17
10969 Berlin

CONTENT

CONSUMER RELEVANCE

Attacks targeting bank accounts are increasing. Phishing messages, notifications claiming to be from family members in messenger apps, calls purporting to be from employees at a user's bank, and unusual SMS messages – consumers are targeted by scammers in numerous ways on a daily basis. The damages incurred are rising, and those afflicted are often forced to accept their losses. The German Consumer Associations often receive reports of how payment service providers accuse consumers of acting with gross negligence for supposedly not exercising proper due diligence. The payment service providers interpret due diligence obligations very broadly: do not click on links; do not share TANs with employees; always be aware of the latest security warnings on the bank's website; and never believe anyone who claims to really be calling from the number shown on a phone's display. The reasons given for supposed gross negligence are varied and seem to be used at will.

However, consumers who have fallen victim to scams repeatedly report that the scammers carried out strange activities using their accounts, such as increasing payment or overdraft limits and requesting unusual transfers; that the consumers had difficulty contacting their banks in order to stop transfers; or that the service providers themselves asked consumers to do the very same things that are supposedly prohibited. When service providers call on consumers to meet wide-ranging due diligence obligations, how do the providers themselves act when fraudulent activity occurs? Do the service providers fully meet their own due diligence obligations, and what exactly are these obligations?

SUMMARY

Amidst increasing cases of online banking fraud, payment service providers repeatedly claim that consumers do not comply with due diligence obligations. On this basis, they refuse requests for refunds or compensation. However, complaints that have reached the German Consumer Associations and independent research carried out by vzbv's Team Monitoring Financial Markets cast a critical light on the due diligence obligations that service providers themselves have to meet, and thus also on the question of contributory negligence on their part. The following report highlights six problem areas:

1. **Inconsistent behaviour:** Service providers do not behave in such a way that would make scams easy to recognise. In some instances they contradict their own warnings and include confusing passages in their general terms and conditions (GTC).
2. **Incomprehensible texts and processes:** Consumers find some of the texts and procedures used by payment service providers incomprehensible and confusing. Consumers are thus unable to properly grasp warnings, with the result that these warnings help payment service providers dodge liability with respect to consumers while failing to adequately prevent fraud.
3. **Difficulty making contact:** Consumer complaints often state that in urgent cases service providers are difficult or impossible to reach by phone.
4. **Inadequate analysis of transactions:** Complaints about fraud cases detail frequent, striking administrative changes to accounts, such as raising payment or overdraft limits, or unusual transactions including payments to recipients abroad. These processes and transactions are sometimes not blocked by the payment service providers nor do they lead to follow-up questions for the account holders.
5. **Inappropriate technological design:** Complaints suggest that banking systems are not sufficiently resilient when it comes to social engineering. This makes it too easy for consumers to fall victim to scams. There are also system configurations, for example in service providers' apps, that have only a limited impact, without consumers being sufficiently aware of this.
6. **Behaviour that is harmful to consumers:** Consumers claim that service provider's employees are not always able to help, and in some cases behave in a way that does not reflect the urgency of the problem, so that valuable time is wasted unnecessarily.

The current legal framework defines very few due diligence obligations for payment service providers, and those obligations that exist are often only vague. The only exceptions are the obligation to be contactable by phone at all times when it comes to cases of fraud, and the obligation to provide evidence that a payment procedure was authorised. In court proceedings, this often means that only the consumers have to defend themselves against the accusation of an infringement of due diligence obligations, while the service providers offset their obligations – for example, to restore the account balance within one bank working day in the case of fraud – against claims for compensation from the consumer. Service providers also repeatedly manage to evade their obligation to provide evidence of authorisation by a de facto reversing the legal dispute. They achieve this by putting themselves in a position where prima facie evidence is sufficient, so that they do not have to submit tangible evidence to the court.

1. PROBLEMS WITH RESPECT TO FINANCIAL SERVICES

Online banking is becoming ever more important. In 2023, 57 percent of the German population used online banking.[1] At the same time, scammers are increasingly targeting consumer accounts. According to the German Federal Criminal Police Office, fraud involving accounts and cards rose 45 percent from 2018 to 2023, when 90,000 cases were recorded.[2] Banks and other savings institutions thus warn about various forms of fraud in different places on their websites: as a warning on the homepage[3], on the online banking log-in page[4], in the website's service section[5], whenever users log in to the banking app[6], and as an educational component with various chapters in a dedicated section[7]. Consumers are often required to check websites and relevant security warnings in order to avoid potentially being accused of neglecting due diligence obligations if they are the victims of a scam.[8] If consumers miss the warnings, banks and savings institutions may refuse to reimburse them for any money lost.

But what due diligence obligations do banks themselves have to fulfil to make it more difficult for scammers to empty customer accounts? Why do scammers still seem to find it so easy, even though security measures have been heightened considerably in recent years, for example via strong customer authentication? Insights gained from consumer complaints[9], and independent analysis carried out by the Team Monitoring Financial Markets, suggest there are several issues. While by no means a comprehensive list, these issues include: inconsistent behaviour from employees of payment service providers; texts and processes used by payment service providers that are hard to understand; difficulty contacting service providers; and possibly inadequate transactions analysis and design of the technology used.

1.1 Inconsistent behaviour

Procedures and processes for safe online banking are defined in a very limited manner. A process excluded by one provider may well be used by another. Even a very common warning, such as not to enter multiple TANs in succession[10], as this might be a typical sign of a scam[11], is by no means a guaranteed indicator of such. For example,

---

[1] Eurostat: Individuals – internet activities, https://ec.europa.eu/eurostat/databrowser/view/ISOC_CI_AC_I__custom_5475301/bookmark/table?lang=en&bookmarkId=b96fab00-944e-4d02-94e7-b910bc79f103, 02/08/2024.

[2] Atzler, Elisabeth: Betrug mit Karten und Konten wächst, in: Handelsblatt 24/07/2024.

[3] https://tfbank.de/, 23/07/2024.

[4] https://meine.deutsche-bank.de/trxm/db/, 23/07/2024.

[5] https://www.haspa.de/de/home/service/sicherheit-im-internet.html?n=true&stref=sitemap, 23/07/2024.

[6] For example in the case of ING-DiBa.

[7] https://wissen.consorsbank.de/t5/Ihre-Sicherheit-im-Online/tkb-p/finanzcoach-sicherheit, 23/07/2024.

[8] Cf Verbraucherzentrale Bundesverband: Bank oder Betrüger? Erhebung zur Erkennbarkeit von Betrug im digitalen Zahlungsverkehr (English summary available), 2024, p. 5f, https://www.vzbv.de/sites/default/files/2024-05/24-05-09%20Bericht_vzbv_Betrugserkennung.pdf, 23/07/2024.

[9] The consumer complaints are based on descriptions of individual cases that reached the Consumer Associations' advisory centres. These are detailed descriptions of particularly notable issues from the consumer advisory centres, which have been qualitatively assessed. It is not possible to draw conclusions about the frequency of such cases that reach the advisory centres nor in the general population.

[10] See for example https://www.volksbank-buehl.de/banking-service/service/tipps-sicheres-online-banking.html, 23/07/2024.

[11] See Bundesamt für Sicherheit in der Informationstechnik: Was tun im Ernstfall?, https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Online-

some regulated account information services request up to three successive TANs as part of a standard procedure.[12] Despite statements to the contrary, some service providers also include links to online banking services in emails or send links to be clicked on via SMS. In light of this inconsistent behaviour, it is no surprise that consumers cannot always identify scams. Indeed, one survey showed that in the case of 38 percent of genuine service provider communications, consumers suspected a scam.[13]

1.2 Incomprehensible texts and processes

In addition to the lack of clearly defined processes, consumers complain that service providers' texts are incomprehensible or too ambiguous. For example, participants in the above-mentioned survey classified warning notifications intended to inform them about scammers hijacking their authentication tools as "confusing" or "incomprehensible". Consequently, the warning notifications failed to achieve their aim of making persons affected aware of fraudulent behaviour. Only 16 percent of those surveyed correctly understood the content of these warning notifications.[14] The approval texts in authentication tools are also sometimes confusing. For example, if consumers want to increase a transfer limit in their online banking or change an exemption order, the app of one direct bank indicated a request awaiting approval with the words "Online-Abschluss" (i.e. purchase product online), although in this instance no product had been signed up for.

In addition to the texts themselves, the various procedures are also not always clear or comprehensible. For example, respondents to the above-mentioned survey rated the processes described as "laborious", "complicated", "confusing", and "not straightforward". They criticised a "strange sequence" of steps and expressed uncertainty and feeling overwhelmed.[15]

1.3 Difficulty making contact

Consumer complaints from 2024 show that service providers are sometimes hard to reach in an emergency. One consumer complained that he was the victim of a phishing attack. He recognised it immediately and contacted his bank. He claims that it took 25 minutes until his account was blocked, a period in which the scammers managed to debit his account to the tune of 4,800 euros. Another consumer experienced the following:

> *Criminals managed to access my bank details, online banking, login data, and credit card information following a phishing attack. […] I spent almost the entire Saturday trying to contact the bank, and had to wait several hours in a queue until I finally had an employee on the line who was also able to block the virtual credit card. It took a total of more than six hours to reach someone using the bank's service hotline.*

Banking-Online-Shopping-und-mobil-bezahlen/Online-Banking/Was-tun-im-Ernstfall/was-tun-im-ernstfall_node.html, 23/07/2024.

[12] See Verbraucherzentrale Bundesverband: Übersicht zur Erhebung bei Kontoinformationsdiensten, 2022, p. 4, https://www.vzbv.de/sites/default/files/2022-06/2022-06-14%20KID_Ergebnispapier-final.pdf, 23/07/2024.

[13] Verbraucherzentrale Bundesverband (2024) (such as note 8), p. 16.

[14] Ibid., p. 14.

[15] Ibid., p.16f.

Another consumer reported needing three hours to contact an employee at another bank after discovering an unauthorised transfer.

When the Team Monitoring Financial Markets invited consumers to report their experiences of trying to reach payment service providers' customer service employees by phone, consumers offered extremely varied reasons as to why they couldn't contact their providers. These include being left on hold endlessly, the lack of an option to make contact by phone, or calls being cut off. Despite persistent further attempts to make contact, only 52 out of 178 consumers succeeded with a subsequent attempt. Eleven consumers claimed that they were unable to report an instance of unauthorised account access by phone.[16] A survey carried out last year showed that it is not always possible to contact neobanks and direct banks in an emergency, Of the ten neobanks assessed, four did not provide any contact number or only did so for a single issue.[17]

1.4 Inadequate analysis of transactions

Victims of fraud often report to the German Consumer Associations that perpetrators used their assets in ways that deviate sharply from the consumer's typical behaviour. For example, transfer limits were increased, payments of unusually high sums were made to various individuals in quick succession, credit limits were requested and immediately maxed out, assets transferred or altered, and several instant credit transfers were made although consumers had never previously carried out such transfers. The following examples from the advisory centres of the German Consumer Associations illustrate the issues:

- *A consumer's account was emptied online at the end of January. A third party had gained access to his online account. […] Soon afterwards, the account was empty. This involved four flights to foreign destinations and payments in Dubai (with a credit card from the bank that the perpetrator also organised for himself). Such transactions are not typical for the consumer and he did not carry them out using his usual end device.*
- *The consumer's account was hijacked using a phishing SMS, an overdraft was set up and maxed out to make several transfers.*
- *A consumer explains: I received a call with the number of my bank from someone claiming to be an employee. Apparently, a case of fraud had been identified. […] Ten real-time transfers of about 2,000 euros were then made from my deposit current account and my savings account to a Spanish account. In the afternoon I became suspicious, called the bank, was left on hold for an hour. Unknown persons had increased my transfer limit to foreign countries to 100,000 euros.*
- *A consumer received a notification claiming to be from "netflix" […] There were then several payments made from her credit card account in the currency AED (United Arab Emirates).*

[16] Verbraucherzentrale Bundesverband: Verzweifelte Anrufe. Wie Banken ihre Kunden am Telefon im Regen stehen lassen. Ergebnisse eines Verbraucheraufrufs, 2024, https://www.vzbv.de/pressemitteilungen/banken-lassen-kundinnen-mit-problemen-allein, 16/08/2024.

[17] Verbraucherzentrale Bundesverband: Im Notfall schwer erreichbar? Erhebung zu telefonischen Kontaktmöglichkeiten bei Neobanken und Direktbanken, 2023, https://www.vzbv.de/sites/default/files/2023-07/23-05-10_Ergebnispapier_ServicetelefoneNeobanken_final.pdf, 24/07/2024.

- *Criminals made a total of 43 instant credit transfer payments from the consumer's current accounts to a single recipient name in France. The total damage amounted to 43,000 euros.*
- *A consumer was contacted by someone claiming to be a bank employee […] Subsequently, almost 50 purchases were made using Apple Pay. The damage amounted to almost 10,000 euros.*
- *The consumer's credit card was misused. It was used in Italy, Morocco, and London all within one day.*
- *Someone claiming to be a bank employee asked the consumer whether she had made transactions in the last half hour – namely increasing the transfer limit to over 3,900 euros, a transfer of 2,300 euros, and three transfers of about 500 euros. As the consumer had been walking her dog during the previous half hour she answered no. The supposed employee had knowledge of the account, as he gave further details of transfers the consumer had previously made. […] The caller then claimed that the consumer now had to "cancel" the incorrect amounts. Requests for transfers were then sent to the consumer. The consumer's own name was given as recipient. The caller drew particular attention to this, explaining that the authorisation was necessary to transfer the money back.*
- *More than 4,000 euros (account/overdraft) were charged to a consumer's account using a debit card. […] When the consumer asked the bank why the card was not blocked following more than 20 rejected payment attempts, he received no response.*

1.5 Inadequate technological design

Other consumer complaints raise questions about the technological design of service provider systems and what image of consumers guides them. There are cases, for example, in which consumers are called from what appears to be the service provider's actual phone number in order to reverse supposedly fraudulent activity, and with just one wrong click in the app the access to entire accounts is transferred to criminals. Consumers are put in stressful situations by scammers, and it also cannot be assumed that everyone possesses extensive knowledge about payment terminology and processes. Scammers will presumably always be able to use a plausible story and communication skills to get some consumers to make that single click. However, vzbv is of the opinion that technological systems that are used by extremely different kinds of people are inadequately constructed if a single wrong click can trigger such severe consequences. Critical applications that are not aimed solely at experts should be designed in such a way that they are resilient against potential attacks.[18]

This is all the more important when scammers can hijack systems even without using social engineering techniques, as the following consumer complaints suggest:

- *Credit card misuse led to unauthorised access. The consumer received an activation SMS for Apple Pay, but did not react to it. Weeks later, fraud occurred in the form of product purchases in physical shops.*
- *A consumer had problems with online banking and technical problems with her TAN app in January 2024. She subsequently received an activation letter from*

[18] For more on this topic see Zimmermann, Verena; Renaud, Karen: Moving from a "human-as-problem" to a "human-as-solution" cybersecurity mindset, in: International Journal of Human-Computer Studies, 2019, p. 169–187.

the bank. However, she was still not able to re-register the TAN app. She received a total of nine activation letters. It turned out that approving the activation codes had installed security procedures for external third parties.

- *When the bank employee asked me whether I had received phishing emails or SMS, I answered with a clear no. I am so careful with bank data that even my own husband doesn't have my login details. The bank employee then noticed that the TAN app had been installed on a new Android phone in late May 2024. I remember that shortly before that I wanted to make a transfer. As usual, the bank's online banking system requested a TAN and, as usual, I opened the TAN app to approve the transaction. At that point I received an error notification directly from the app. The same thing happened when I tried again. I tried switching to SMS TAN, but again without success, as it wasn't activated. When I read that I would need a new activation letter to make this possible, I abandoned the process. Three days later I attempted a new transfer, and it worked. The next day my entire account had been emptied.*

Even when consumers seem to use technology correctly, it does not always lead to the intended results. This could be due to a malfunction or a construction issue. This might be the case, for example, if a credit card is blocked in an app only for future payments using that app, but is not necessarily blocked for transactions outside the app. Consumer complaints again illustrate such issues:

- *A consumer claims his credit card was misused in December 2023. He mentions that he blocked the credit card using the online banking app and ticked card misuse as the reason. […] He later spoke to a bank employee. The employee did not see online that the card was blocked, and thus himself requested that the card be blocked.*
- *A consumer has had a current account since 1990 and in February 2024 received one SMS message at night and another in the morning from the bank's credit card service that a credit card and a digital card with a payment limit of 1,000 euros had been activated. That same day the consumer requested that her account be blocked, as she had not requested any cards. However, both cards were used to debit the account, as they had not been blocked along with the account.*

1.6 Behaviour that is harmful to consumers

Consumers also report ongoing frustrating experiences after they have fallen victim to scammers. They do not always receive the support they are due after reporting scams to the relevant service providers. They are either left waiting, referred to various forms or processes, or simply refused help. The following cases illustrate the problem:

- *A consumer was the victim of credit card fraud. After seeing in her online banking system that 1,500 euros were due to be debited to her account, she immediately called the emergency service to stop the transaction. She was told that it could not be stopped, as she first had to wait until the account had been debited and could then object to the payment within a 30-day period. In addition, her account was blocked. Everything happened as she had been told. The account was debited and she wanted to lodge her complaint, but was informed that "for technical reasons it is not currently possible". She immediately phoned the bank and was told that her case was not an emergency and she should use the form provided.*

- *A consumer had concerns after falling for a phishing scam. He immediately called his bank to block his account. However, the bank told him to wait until the following day. Four days later, a transfer of over 5,000 euros that he had not authorised was made to the UK.*
- *A married couple were in South Africa and, under the pretext of a security check, were lured to an ATM that had clearly been manipulated. The machine kept their credit card. Within ten minutes the couple requested that the card be blocked. The next day it became clear that 200 euros had been withdrawn, which is the general maximum withdrawal limit at ATMs in South Africa. Several days later the account was debited for two additional sums amounting to 5,000 euros. The thieves were able to transfer money using the card even though it had been blocked for several days. There was no TAN, no email, and no questions as to whether the couple themselves has initiated these unusually high transfers in a foreign country.*
- *A consumer's credit card was misused. […] The bank refused to compensate the loss or to initiate a chargeback procedure with Mastercard. Allegedly, the consumer had authorised the payments using the app, but this was not the case.*

2. CURRENT LEGISLATION

The legislation on dealing with unauthorised payments have their origins in the provisions of the EU Payment Services Directive.[19] According to the legislation, payment service providers bear primary responsibility for the economic consequences of transactions that the users of payment services have not actually authorised.

According to Article 73 PSD 2 payment service providers have to refund unauthorised payment transactions quickly (see also § 675u German Civil Code, BGB). Even a transaction that is technically correct does not, as a rule, prove that victims of fraud neglected their obligations or either intentionally or through gross negligence violated conditions for the issuing and use of these payment instruments (Art. 72, § 675w BGB). If the transaction is due to the use of a stolen or lost payment instrument or other misuse of a payment instrument where the consumer was in a position to be aware of the loss, the affected account holder is liable for an initial amount of just 50 euros. Consumers are only obliged to compensate the full amount if the losses are due to intentional or grossly negligent infringement of their legal obligations[20] pursuant to § 675l (1) BGB or the conditions for the issuing and use of the payment instrument.

2.1 Vaguely defined obligations

The discussion on the obligation to prevent fraud focuses first of all on the users of payment services.[21] Only when these obligations are violated are payment service users liable. However, for non-specialists these obligations are not always as easy to understand as they may first seem.

---

[19] Currently, the second Payment Services Directive (EU) 2015/2366 applies; article standards in the following refer to this version of the directive, unless otherwise specified.

[20] The standards offer additional protection to those not guilty of fraud; explicit details are omitted here for the sake of simplicity.

[21] See, for example, MüKoBGB/Jungmann, 9th Edition 2023, BGB § 675l note 34, Beck Online. Comments are provided for detailed examples that do not, however, always allow for generalisations, cf. for example ibid. note 36.

Standards set out general requirements, and GTCs and conditions of use set out relevant examples. This also necessitates making formal exceptions to such clear provisions[22], for example because a clear prohibition on forwarding TANs outside the online banking system must not apply to account information and payment authorisation services as well as other services. [23] Consequently, conditions for consumers with respect to online banking are sometimes confusing, for example when, on the one hand, they state that "information that only the customer possesses (e.g. TANs) may not be passed on outside the online banking system either orally (e.g. by phone) or in text form (e.g. by email, messenger services)".[24] On the other hand, exceptions to these provisions under certain conditions are stated two paragraphs later. It is thus difficult to establish provisions as standards that always apply. It remains necessary to assess cases on an individual basis.[25]

In light of such inconsistent rules, it remains difficult for consumers to differentiate between genuine, non-fraudulent activities and actual fraud. Therefore, it cannot be generally assumed that entering several TANs in succession always constitutes grossly negligent behaviour on the part of the consumer.

2.2 De facto reversal of litigation

According to Article 73 of the Payment Services Directive, service providers are obliged to promptly refund unauthorised payments "*in any event*"[26]. Consequently, it is thus banks that have to prove users acted in a grossly negligent manner in order to hold them liable – if necessary as plaintiff in court. However, this is not the case in practice, as the highest courts have ruled that persons who are victims of unauthorised payments cannot demand that banks refund payments if the consumers themselves would subsequently have to pay the amount back in compensation for damages. What the German Federal Court of Justice (BGH) and the Higher Regional Court (OLG) Frankfurt am Main otherwise deem acting against the spirit of the law[27] raises the question of why a bank should be allowed to sometimes take several weeks to examine a case without, in the meantime, refunding the amount. If the assessment ultimately concludes that the consumer has not acted with gross negligence, then not refunding the consumer immediately would constitute a clear violation of § 675u BGB.

As a result of this reversal, the bank does not have to try to present convincing evidence of the grave accusation of gross negligence by the customer to the court and present at least prima facie evidence. Instead, it is the users of payment services who are repeatedly obliged to exercise their right to an immediate refund in the case of unauthorised payments pursuant to § 675u BGB in a legal proceeding that often takes

[22] For example, see Clause 7.1 (2) b of the online banking conditions, 182 410.000 D1 (version: Sep. 2022) v4.1 of the S-Management-Services – DSV Gruppe via Sparkasse Köln-Bonn

[23] According to Article 33 of the Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366, third-party service providers have the right to access interfaces intended for customers if their own means of access to the bank are disrupted. This means that they can take control of a user's data to access the bank.

[24] Quoted as an example from Clause 7.1 (2) b of the online banking conditions, 182 410.000 D1 (version: Sep. 2022) v4.1 of the S-Management-Services – DSV Gruppe via Sparkasse Köln-Bonn

[25] And such are the results. Maihold in: Ellenberger/Bunte BankR-HdB, § 33. Bankgeschäfte online, note 248, beck-online

[26] Excluding precisely defined suspicion of fraud

[27] Cf. BGH ruling of 17/11/2020 (Az.: XI ZR 294/19), note 25 and also OLG Frankfurt am Main ruling of 6/12/2023 – 3 U 3/23, note 46

considerable effort and time. This regularly puts payment service users in a worse position than intended by law.

2.3 Banks' obligations and the issue of contributory negligence

Pursuant to § 675v BGB, banks that violate their obligations may be excluded from seeking compensation from users whom they claim are guilty of gross negligence of their own obligations. The obligations applicable to payment service providers in this case are based on § 675m (1) (3) and (5) BGB and are addressed in § 675v (5) BGB[28]: Payment service users are not liable for gross negligence if it was not possible to contact the service provider. They are also not liable for subsequent payment transactions from the moment the initial security violation was reported.

It is particularly important that the wording of § 675v (5) BGB does not appear to offer protection from the consequences of gross negligence in the case of a service provider that does not ensure appropriate means of contact, as here the text is missing a reference to the correct paragraph 3. Some legal experts assume an editorial error.[29] Article 74 of the Payment Services Directive also excludes liability for gross negligence if the service provider does not provide appropriate means for notification at all times.

Pursuant to § 254 BGB, banks must ensure that harm remains minimal even when grossly negligent behaviour on the part of a customer has been identified. The additional obligations of payment service providers with respect to this duty to minimise harm are not specifically codified. Such obligations also include the adequate monitoring and reaction to patterns of attempted fraud in light of newly identified threats.[30]

In light of this, it is concerning when consumers report cases in which banks refuse to refund payments because it was not possible to block payment instruments either at all or in time or the consumers were made to wait. Reporting fraud, as opposed to the blocking of payment instruments, is the decisive factor when it comes to exemption from liability. The courts ought to reject banks' claims for compensation from consumers in such cases.

Another critical point is when banks, despite knowing the typical strategies used by scammers, fail to stop payments that match these patterns, for example when scammers set up a new payment instrument and then prepare and request payments to empty an account. In such cases the courts must, at the very least, reduce the amount of compensation and even refuse it if it is apparent that the bank has neglected its obligations in a significant way. To date, however, claims of contributory negligence have often been rejected because monitoring account transactions and evaluating the risk of payment processes has not been considered a payment service provider obligation.[31] In 2012, the BGH[32] also stipulated the need for "major cause for suspicion". The landmark ruling by the highest court falls short of both the risks and the technological developments.

---

[28] Another provision that excludes gross negligence on the part of payment service users, pursuant to paragraph 4, is the absence of effective customer authentication. However, this is defined as a formal requirement rather than as a violation of an obligation.

[29] See also Maihold in: Ellenberger/Bunte BankR-HdB, § 33. Bankgeschäfte online, note 400, beck-online

[30] See also Maihold in: Ellenberger/Bunte BankR-HdB, § 33. Bankgeschäfte online, note 380, beck-online

[31] Cf. BeckOK BGB/Schmalenbach, 70. Ed. 1/5/2024, BGB § 675v, note 19, beck-online

[32] BGH, ruling of 24/4/2012 − XI ZR 96/11, NJW 2012, 2422, 2425, note 32f. beck-online

CONCLUSION

Considering the overall picture concerning due diligence obligations with respect to fraudulent activities, it is notable that providers of bank accounts warn frequently and in various places about the risks of fraud and scams, in some cases whenever a transaction is made and even when there is no cause for suspicion. Consumers are expected to take note of this information in various places and at all times, to examine the respective case in each situation, and to weigh up whether, for example, a service providers' GTCs do in fact permit unusual behaviour under certain circumstances. Even informed consumers face a challenge in fully complying with this task. Information provided by service providers under these conditions also seems to serve the purpose of subsequently accusing consumers who have suffered harm of not having paid attention to the information and thus not being entitled to a refund. Furthermore, warnings do not always seem to be sufficiently comprehensible to fulfil their purpose. In vzbv's view, an overload of non-specific information in combination with warnings that are specific but hard to understand offers very little benefit to consumers and instead serves more to protect service providers from harm. If service providers really wanted to fulfil their due diligence obligations, they would have to provide very precise information in a manner that the vast majority of consumers can understand.

In addition, while the technology for digital banking does seem to fulfil legal requirements, vzbv is of the opinion that the technology is not sufficiently resilient to prevent it offering a gateway to scammers who are adept communicators.

On the whole, there are almost no clearly defined due diligence obligations for service providers. One of the few requirements is that providers can be contacted by telephone at all times. In cases of doubt, however, it can be difficult for consumers to prove that contact by phone was not possible, especially if, as in some cases, there is the additional factor of improper or confusing instructions. An additional service provider obligation – proof of gross negligence – is often minimised in jurisprudence by accepting prima facie evidence, supported by the supposed violation of due diligence obligations on the part of consumers who have missed warning messages.

However, if scammers gain access to bank accounts and change settings, carry out highly varied activities, or send unusually large amounts of money at an unusual tempo to new recipients, banks have no legal obligation to identify and prevent this in the interests of minimising harm. Monitoring unusual transactions and account activities, and ensuring that their own payment instruments are technologically resilient, seems to be a purely voluntary task for payment service providers. In vzbv's view, the providers fail to fulfil this task adequately.