FROM THE IUSTORIA BLOG

A Fraudster Emptied My Bank Account. What to Do in the First Hours and When the Bank Must Refund the Money

> *The "bank's security team" called and the money vanished. What to do now, when the bank must refund you by the end of the next business day and when not, and what the Financial Arbitrator can do.*

IUSTORIA TEAM

5 November 2026 · 10 min read

Your phone shows your bank's number. The voice at the other end introduces itself as the security department, knows your name and knows which bank you are with. Someone, you are told, is trying to break into your online banking right now and you need to act fast: confirm the "cancellation of a suspicious payment" in the app, read out the code from a text message, or move your money to a "safe account". An hour later the account is empty.

People who come to us afterwards usually hold one of two opposite beliefs. Some are convinced the bank has to give them everything back, because security is its responsibility. Others are ashamed and think they are entitled to nothing, because they read out the code themselves. The truth lies somewhere in between, and a great deal depends on what you do in the first hours and on exactly how the fraud happened.

We explain what to do straight away, when the bank must refund the money and how much of the loss you may have to bear yourself, and when it is worth turning to the Financial Arbitrator (*finanční arbitr*).

The first 24 hours: what to do straight away

Time is working against you. Money usually disappears from the account it was sent to within hours, and fraudsters who have access to your online banking can keep making payments, changing limits or applying for loans. We recommend the following steps:

1. **Hang up, whoever the caller claims to be, and call the bank yourself.** Use the number on the bank's website or on your payment card, never a number the caller gave you. Report the misuse and ask the bank to block your card as well as your internet and mobile banking. The law requires you to report misuse of a payment instrument without undue delay (Section 165(b) of the Czech Payments Act), and the bank must give you a way of doing so that is available at any time (Section 166(1)(c)). Once you have reported it, the bank must prevent any further use of the card or online banking (Section 166(1)(e)), and any loss that arises after that point falls on you only if you yourself acted fraudulently (Section 182(3)(a)).
2. **Insist on a block, not on advice.** In its annual report for 2025, the Financial Arbitrator notes that some banks merely advised customers to change their password instead of blocking access, and it regards that as a failing on the bank's part. Also ask for confirmation that you reported the misuse; the bank must issue it on request, and you can use it to prove your report for 18 months (Section 166(1)(d)).
3. **Ask your bank to contact the recipient's bank.** It should try to have the account the money went to blocked. Success is not guaranteed, but every hour of delay lowers the chances.
4. **Disconnect your devices.** If you installed a remote access app on your computer or phone for the fraudster, disconnect the device from the internet at once and take a photo of the app. Uninstall it only after an expert or the police have examined the device; it is evidence that the attacker made the payments.
5. **Check everything that happened in your online banking.** According to the Financial Arbitrator, attackers often do not just drain the balance but take out consumer loans in the customer's name running into hundreds of thousands of crowns, change limits and set up new cards. Go through any other accounts you have access to as well, including business accounts. If the fraudster took out a loan in your name, write to the bank that you did not enter into the contract, and do not spend any of the loan money still sitting in your

account. In such disputes, the Arbitrator examines whether it was your act at all and whether the bank properly assessed your ability to repay before granting the loan.

6. **File a criminal complaint**, even if the loss is small; how to classify the offence is a matter for the police. How to draw up the complaint is explained in our guide to criminal complaints (in Czech).
7. **Secure the evidence.** A screenshot of your call log (time and number), the text messages with the codes and their wording, the links you clicked and your account statement. Do not write to or call the fraudster again.

A 13-month time limit does not mean you have time. You can have an unauthorised payment put right only if you report it to the bank without undue delay after learning of it, and no later than 13 months after the money was debited from your account (Section 188(1) of the Payments Act). If you report it late and the bank objects, neither a court nor the Financial Arbitrator will grant you the correction (Section 188(4)). Call the bank as soon as you notice the fraud, and send a written complaint within a week as well.

Authorised or unauthorised: everything turns on this

The law divides payments into two groups, and the whole dispute that follows depends on which one yours falls into. A payment is authorised if the payer consented to it (Section 156(1) of the Payments Act). With an authorised payment the bank simply carried out your order, and the refund obligation under Section 181 does not apply.

An **unauthorised** payment is typically one that the fraudster entered and confirmed. They tricked you into giving away your login details on a fake website, or the code from a text message, and sent the payment themselves, from your online banking but without your consent.

An **authorised** payment is one you entered and sent yourself, even if you did so because the fraudster misled you. The typical case is a transfer to a “safe account” or an “investment” recommended by a fake adviser. The Financial Arbitrator puts in the same group cases in which the customer gave the fraudster remote access to their computer or phone.

With transfers you sent yourself, keep your expectations realistic. The Arbitrator examines whether the customer's mistake was excusable and whether the bank contributed to it. In its annual report for 2025, it states that in these cases the evidence gathered did not show that the bank had any part in the customer's mistake. For authorised payments, the main question left is therefore whether the bank neglected its duty to detect fraudulent payments: whether it could have caught the suspicious activity, whether it reacted quickly enough and whether it asked other banks to block the receiving account. Where the Arbitrator found such failings, it steered the parties towards a settlement.

Less clear-cut is the case where you confirmed something in the app that the caller told you was something else, such as cancelling a suspicious payment. The bank may argue that you authorised the payment. In such cases the Financial Arbitrator examines who actually acted and whether the mistake could have affected the validity of the consent. In your complaint, therefore, describe precisely what the app showed and what the caller said you were confirming, and ask for the unauthorised payment to be put right.

You can claim the return of unjust enrichment from the fraudster or from the holder of the account the money went to (Section 2991 of the Czech Civil Code), including as an injured party in criminal proceedings. The account holder, however, is often a front man with no assets.

When the bank must refund the money and how much you bear yourself

For an unauthorised payment, the bank must, without delay and no later than by the end of the following business day after it learned of the payment or you reported it, restore your account to the state it would have been in had the payment not taken place, or refund the amount together with any charges and lost interest (Section 181(1)). The time limit does not start to run as long as the bank has reason to believe that you acted fraudulently and notifies the supervisory authority of this in writing, giving its reasons (Section 181(3)). Banks also rely on Section 181(4), under which the refund obligation does not apply if the payer bears the loss. How that provision should be read after the judgment of the Court of Justice of the EU is explained below.

How much of the loss you ultimately bear is determined by Section 182:

- **up to EUR 50** if the loss was caused by a lost, stolen or misused card or online banking (Section 182(1)(a)). Even this does not apply if you could not have detected the misuse before the payment, or if the bank caused it (Section 182(2));
- **in full** if you acted fraudulently or, intentionally or through gross negligence, breached your obligation to protect your security credentials or to report misuse (Section 182(1)(b) and Section 165);
- **nothing** if the loss arose only after you reported the misuse, if the bank did not give you a way to report misuse at any time, or if it did not require strong customer authentication where the law requires it (Section 182(3)). Strong customer authentication relies on at least two mutually independent elements, such as a password and a phone (Section 223(3) and (4)).

If you claim that you did not authorise the payment, the bank must prove that the payment was authenticated, accurately recorded and entered in the accounts, and not affected by a technical breakdown; otherwise it is treated as unauthorised (Section 187(1)).

The law does not define gross negligence, and that is precisely what most disputes are about. According to the Financial Arbitrator, banks most often argue that the attack would not have been possible without the customer's actions. In most cases of unauthorised payments, the Arbitrator found that the customer had breached the contractual obligation to protect their security credentials, typically by entering them on a fraudulent website or handing them over to a caller. At the same time, it always examines whether the bank applied strong customer authentication to every step that made the attack possible: logging in, activating the app on a new phone, changing limits or adding a card to a mobile wallet. Where it was missing, the bank must put the payment right.

With business customers, the bank may agree to depart from, among other things, Section 182, Section 187(1) and the time limits under Section 188 (Section 128(6)). For a business account, the bank's terms and conditions therefore matter as well.

The bank alleges gross negligence? It must refund the money first

When a bank alleged that the customer had been grossly negligent and refused to refund the money, the customer had to sue or go to the Arbitrator. In its judgment of 15 October 2026 in Case C-70/25, Tukowiecka, the Court of Justice of the EU ruled that a bank cannot refuse an immediate refund of an unauthorised payment merely because, in its view, the customer made the payment possible through gross negligence. It can claim compensation from the customer only afterwards. The Czech Section 181(4) is worded differently; in our view it can be interpreted in line with the directive, so that until the bank proves gross negligence, it refunds the money. We discuss this in detail in our article Your Bank Must Refund an Unauthorised Payment Immediately. Gross Negligence Is Decided Later.

For your first steps, this means just one thing: in your complaint about an unauthorised payment, ask for a refund under Section 181(1) and cite judgment C-70/25. If the bank refuses, pointing to your negligence, that is grounds for an application to the Financial Arbitrator. The judgment does not cover transfers you sent yourself.

Call the bank on the number on its website or your card, ask it to block both your card and your online banking, and request confirmation of your report. Follow up the call with a written complaint the same day or within a week at the latest.
In the complaint, describe who entered and confirmed the payment. If it was the fraudster, the transaction is unauthorised and the bank should refund it by the end of the following business day (Section 181(1) of the Payments Act and judgment C-70/25).
Go through your entire online banking, not just the balance: loans taken out in your name, new cards, changes to limits and to your phone number. Dispute each such transaction separately.

When the bank refuses: the Financial Arbitrator

A dispute between a consumer and a bank over payment services can be decided by the Financial Arbitrator as an alternative to a court (Section 1(1)(a) of Act No. 229/2002 Coll., the Czech Financial Arbitrator Act). The condition is that you first asked the bank to put things right without success and can prove it (Section 10(1)(b)). Send the request in writing, according to the Arbitrator preferably by registered post, and give the bank a reasonable time to reply. With your application you then enclose a copy of the request, the certificate of posting and the bank's reply, if there was one.

The proceedings are free of charge and each party bears its own costs (Section 18). Filing the application has the same effect on limitation as filing a court action (Section 8(2)). The Arbitrator gathers evidence on its own initiative, and the bank must submit the documents and records requested within 15 days (Section 12(3) and (6)). This is crucial in fraud disputes, because only the bank's systems show who confirmed the payment and from which device. The Arbitrator issues an award within 90 days of gathering the evidence, or in complex cases no more than 90 days later (Section 15(1)). Objections can be raised against the award within 15 days (Section 16(1)), and a final award is enforceable like a court judgment (Section 17). If the Arbitrator finds for the con-

sumer, it also orders the bank to pay a penalty of 10% of the amount awarded, at least CZK 15,000, which goes to the state (Section 17a). The Arbitrator will not hear a dispute that a court has already decided or that is pending before a court (Section 9).

The Arbitrator has plenty of work. In 2025, 12,050 proceedings were opened, 294 of them concerning payment transactions. Payment services disputes concluded that year took 384 days on average, more than twice the overall average of 167 days. The Arbitrator itself counts disputes over unauthorised payments following phishing and fraudulent phone calls among the most complex. Either party can challenge its decision by bringing an action in court.

The Financial Arbitrator decides only consumer disputes. A company whose business account was emptied by a fraudster has to go to court.

At a glance

Question	Answer	Provision
When should misuse be reported to the bank?	Without undue delay, no later than 13 months after the debit	Section 165(b) and Section 188 of Act No. 370/2017 Coll.
When is a payment authorised?	When the payer consented to it, even if a fraudster induced them to do so	Section 156 of Act No. 370/2017 Coll.
By when must the bank refund an unauthorised payment?	By the end of the following business day after learning of it or being notified of it	Section 181(1) of Act No. 370/2017 Coll.
How much of the loss does the customer bear?	Up to EUR 50; all of it in case of fraud, intent or gross negligence; nothing after notification or without strong customer authentication	Section 182 of Act No. 370/2017 Coll.
May the bank refuse a refund because of gross negligence?	Not the immediate refund; it can claim compensation afterwards and must prove gross negligence	Court of Justice of the EU judgment of 15 October 2026, C-70/25, paragraphs 34, 40 and 46
Who has to prove that the payment was properly authenticated?	The bank	Section 187(1) of Act No. 370/2017 Coll.
What do proceedings before the Financial Arbitrator cost?	Nothing; a prior request to the bank to put things right is required	Sections 10 and 18 of Act No. 229/2002 Coll.

Has your bank refused to refund money a fraudster took from your account? We will go through your statements and how the attack unfolded, assess whether the payment was unauthorised and prepare a complaint, an application to the Financial Arbitrator or a court claim. We handle disputes with banks as part of our dispute resolution practice. Get in touch.

Conclusion

A dispute with a bank is often decided in the first hour after the fraud. What counts is how quickly you told the bank, whether it really blocked your card and online banking, and whether you have kept the traces. The second decisive question is who made the payment. Under the Tukowiecka judgment, money that a fraudster sent from your online banking must first be refunded by the bank, which can argue about your negligence only afterwards; cite the judgment and ask for the refund right away in your complaint. Money you sent yourself is much harder to get back.

We wrote about fraud when buying from online listings, where the victim sends the money themselves, in our article Anatomy of a Scam. What to do after filing a criminal complaint is covered in our guide on that subject (in Czech).

Sources

- Act No. 370/2017 Coll., on Payments, Sections 128(6), 156, 165, 166, 181, 182, 187, 188 and 223 (as in force from 1 October 2025).
- Act No. 229/2002 Coll., on the Financial Arbitrator, Sections 1, 8 to 10, 12 and 15 to 18.
- Act No. 89/2012 Coll., the Civil Code, Sections 554 and 2991.
- Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market, Articles 72, 73 and 74.
- Judgment of the Court of Justice of the EU of 15 October 2026, Case C-70/25, Tukowiecka.
- Annual Report on the Activities of the Financial Arbitrator for 2025 (May 2026), pp. 3–4, 15, 25, 28 and 33–37.
- Financial Arbitrator, Frequently asked questions (request for a remedy), finarbitr.gov.cz.

This article is for information only and does not constitute legal advice. It reflects the law as at the date of publication; whether a court or the Financial Arbitrator treats a payment as authorised, and whether you acted with gross negligence, always depends on how the specific attack unfolded and on the bank's records.

A Fraudster Emptied My Bank Account. What to Do in the First Hours and When the Bank Must Refund the Money

IUSTORIA team · Published 5 November 2026

https://www.iustoria.cz/en/blog/a-fraudster-emptied-my-bank-account/

This text is protected by copyright. Sharing the document whole and unaltered is welcome; reuse of parts in other texts requires attribution. © IUSTORIA, advokátní kancelář, s.r.o.