UNAUTHORISED TRANSACTIONS - FIVE BANKS PRESSED WITH CHARGES

* **Your money vanished from your account without your permission, you reported it to the bank and the bank refused to reimburse the amount of the unauthorised transaction?**
* **Under the law, it is the bank’s responsibility to exercise the utmost care in safekeeping and protecting your cash.**
* **The bank must reimburse money to the consumer unless it suspects fraud on the consumer’s part and has reported it to law enforcement authorities.**
* **The President of UOKiK has brought charges against five banks - concerning unlawful refusal to refund the amount of unauthorised transactions and misleading consumers in responses to complaints.**

**[Warsaw, 18 July 2022]** The President of UOKiK has been [conducting preliminary investigations into unauthorised transactions](https://uokik.gov.pl/news.php?news_id=17682) for a year. With the evidence gathered so far, five banks have now been charged with infringing the collective interests of consumers. These are: **Bank Millennium**, **BNP Paribas Bank Polska**, **Credit Agricole Bank Polska**, **mBank** and **Santander Bank Polska**.

The charges followed the analysis of consumer complaints and the banks’ reactions and responses to reports of theft of money from consumers’ accounts. One of the cases under investigation is the one described by a 72-year-old female retiree who was saving money “for a rainy day” for 30 years. The fraudster accessed the woman’s credentials and wiped out PLN 170,000 in savings from the retiree’s account and took out a loan for PLN 80,000. **Quite recklessly, the bank converted the currency and transferred the money overseas, charging a processing speed fee on each transfer, and gave a substantial loan to a person with a low pension who used to be in for safe investments throughout her account history.** The financial institution also failed to react even when a fraudster impersonating a pensioner changed her marital status from married to widowed so that her husband’s consent was not needed to take out a loan. The bank, infringing EU-wide law - did not reimburse the victim. It authoritatively concluded that it was the retiree’s fault for the situation, which had put her in a difficult financial position.

There are thousands of similar stories in Poland. What varies are the amounts and methods of the fraudsters. What do they have in common? Stealing money from the accounts of unsuspecting consumers and generally negative reaction from banks in response to complaints. **Unfortunately, despite the statutory obligation, banks do not reimburse funds or, in the case of loans, force consumers who have fallen victim to fraudsters to pay them back.**

*- As a public trust institution, the bank is obliged to take all steps necessary to secure the funds of its customers. It is unfortunately quite often that fraudsters take funds out of consumers’ bank accounts or incur financial liabilities. In most cases, banks merely execute ordered operations thoughtlessly and do not feel responsible, even though they might have become suspicious just by analysing transactions at its early stage, e.g. due to unusual amounts, currency, made within a short period of time after a change of data or access channels. Meanwhile, banks should be much more proficient in developing mechanisms to identify and react to suspicious operations in good time, if only by using a customer’s existing order history or behavioural biometrics to enhance security even further. Instead, we witness a kind of discretion in rejecting consumers’ complaints, as well as a failure to comply with the law on the reimbursement of funds lost as a result of unauthorised transactions* - Tomasz Chróstny, President of the Office of Competition and Consumer Protection, says.

**Applicable law**

According to Article 46 [of the Payment Services Act](https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20111991175), implementing EU [PSD2](https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32015L2366&from=PL)\*, banks **are obliged to reimburse the payer with the amount of the unauthorised payment transaction or to restore the debited payment account to the status prior to such transaction - by the end of the next business day following the notification.** The exception is two situations: the consumer’s notification took place later than 13 months after the payment transaction or there is a reasonable suspicion of fraud on the part of the allegedly injured consumer, which was duly notified by the bank to the police or prosecutor’s office. In other cases, the bank is obliged to restore the account to the state prior to the execution of an unauthorised payment transaction by fraudsters – e.g. in the case of incurring a financial obligation by fraudsters - or to reimburse the money to the payer’s bank account.

– *The charges against the first five banks include, inter alia, failing to reimburse the payers with the amount of the unauthorised payment transactions within the statutory deadline, despite the fact that there were no circumstances that would have exempted the bank from this obligation* – Tomasz Chróstny, President of UOKiK, stresses.

**Authentication and authorisation of transactions**

When addressing the issue of unauthorised transactions, it is of crucial importance to distinguish between the concepts of ‘authentication’ and ‘authorisation’. Authentication, in accordance with its statutory definition, means “a procedure which allows the payment service provider to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user’s personalised security credentials” (e.g. the provision of PIN code). Authorisation, in turn - in addition to authentication, which is a technical operation - involves the user’s consent to the payment transaction in question. **Therefore, an unauthorised transaction will also be an authenticated transaction (e.g. by providing a PIN code), but lacking consumer’s consent.**

It should be noted, however, that under Article 45(2) of the Payment Services Act, the mere demonstration by a bank that a transaction itself was authenticated correctly is not sufficient to conclude that it was authorised by the user, or that the customer either wilfully or through gross negligence allowed the transaction to take place. The burden of proof of such circumstances rests with the bank.

The bank may claim that the unauthorised payment transaction occurred as a result of the consumer’s wilful misconduct, or as a result of the consumer’s wilful or grossly negligent breach of one or more of the obligations referred to in Article 42 of the Payment Services Act. Given such circumstances, the bank may enforce its claims against the consumer after having reimbursed the amount of the unauthorised payment transaction.

*- Only after having met the obligation to reimburse the amount due, may the bank pursue claims against the customer if it turns out that the customer has intentionally brought about the transaction or has demonstrated gross negligence, enabling fraudsters to use their authentication data. The burden of demonstrating these circumstances is legally incumbent on the bank. We do not question the right of the bank to pursue a claim in situations attributable to the consumer. However, in many cases the bank’s authentication and security tools do not protect the consumer against unauthorised transactions. In such circumstances, when fraudsters manage to crack down on banking procedures and safeguards, the bank cannot be the judge in its own case, dismissing consumers’ claims outright and withholding reimbursement in defiance of the law. It is up to the courts - impartial to both the bank and the consumer - to judge and acknowledge fault in questionable situations. Banks, on the other hand, should be exerting more effort to ensure that, through the use of systemic tools, such situations are as rare as possible* – Tomasz Chróstny, President of UOKiK, states.

At the same time, in the course of the preliminary investigation, the President of UOKiK determined that banks may mislead consumers in their responses to complaints concerning unauthorised transactions.

- *Based on the analysis of the banks’ responses to complaints, charges were also pressed of misleading consumers. For example, in their replies, the banks argued that the transaction had been authorised and at the same time the consumer might have exercised gross negligence, or that its mere evidence of the payer’s authentication relieved the bank of its reimbursement obligation. The consumers who received this type of feedback to complaints about money stolen from their accounts may have been misled as to the very fact of authorisation of such a transaction and the extent of the bank’s obligations and responsibilities. This may discourage consumers from pursuing their rights further* – Tomasz Chróstny, President of UOKiK, claims.

The President of UOKiK is still investigating the practices of the remaining 13 banks under preliminary investigation. Should irregularities be identified, the President of the Office may bring charges against other financial institutions. For infringing collective interests of consumers, the banks may be imposed a fine of up to 10% of its turnover.

**Consumer, stay sharp**

* Remember: fraudsters’ behaviour is evolving, but it boils down to one thing - trying to phish your account access details in order to steal your money using the banking system.
* Under no circumstances share your login or password to access your account. Do not install any applications. Hang up, call the financial institution’s official hotline to confirm this. Do not use a number provided by a person calling you and introducing themselves as a bank employee.
* Do not click on links or attachments sent in emails, text messages or instant messages if you are not sure they come from a verified sender. You can install dangerous software in this way.
* Proceed with caution if you are selling on an auction portal and the potential customer wants to contact elsewhere - e.g. only by email or instant messaging. Never provide them with your bank login details or your payment card number and CVV/CVC code - with these, fraudsters can authenticate virtually every transaction.
* Read carefully the content of the SMS codes sent by the bank so that you know what transaction is being made. They inform about the transaction in question - check the amount and transfer account. Also be careful not to approve, for example, changing the phone number to which you receive your transaction authentication details to one owned by fraudsters, who will then be able to confirm any transfer made from your account.
* Make sure you have anti-virus software and an updated operating system installed on the devices you use to log in to e-banking. With this, spyware is more likely to be detected early and fraudsters may be prevented from stealing your credentials.

**What to do if you are a victim of fraud?**

If fraudsters have made unauthorised transactions from your account, contact the bank via the official hotline as soon as possible, report such a transaction, change your login details for the banking app and e-banking and cancel the card. You have 13 months to notify a financial institution, but the sooner you do it, the better for you. Then contact the police. If the bank rejected your complaint, ask for assistance of [the Financial Ombudsman](https://rf.gov.pl/kontakt/) or municipal or county [consumer advocate](https://uokik.gov.pl/pomoc.php) in resolving your individual case.

**Consumer support:**

Phone: 801 440 220 or 222 66 76 76 – consumer helpline
E-mail: porady@dlakonsumentow.pl
[Consumer Ombudsmen](https://uokik.gov.pl/pomoc.php) – in your town or district
[Financial Ombudsman](https://rf.gov.pl/jak-pomaga-rzecznik-finansowy/porady/) - when a complaint has been rejected by a financial institution

\* PSD2 – is the Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market