Banking Loan Fraud Cases on the Rise: Dozens of Cases Reported Each Month by Consumers to CSALB

9 September, Bucharest. This year, consumers have submitted more than 170 requests to the **Centre for Alternative Dispute Resolution in Banking (CSALB)** concerning fraud carried out through banking channels. Most of these requests describe cases in which defrauded consumers found themselves indebted to banks after cybercriminals took out bank loans in their names. In most cases, consumers allowed strangers to gain access to passwords, confidential information and even their own phones or online banking applications.

Moreover, CSALB is also reviewing cases in which consumers themselves took out loans and then transferred the funds to unknown accounts, seeking to purchase crypto assets, shares or to cover other alleged fraud or debts.

In their requests for negotiations with banks, consumers describe complex fraud schemes, with losses reaching as much as EUR 20,000 in the cases analysed by CSALB. Unfortunately, in most situations, banks do not accept these requests for conciliation through CSALB. The main reason is that the cases described are currently under investigation by the police, but also because the perpetrators did not breach the banks' security systems; instead, they accessed the accounts with the assistance of the account holders themselves.

The cases selected from requests received by CSALB use fictitious names to protect consumers' identities, while their locations (the counties indicated) are real. Presenting these cases is intended to help prevent future fraud attempts by describing the methods used by criminals. All of these requests were closed or rejected by the banks.

Adriana H., Bucharest: *"I was the victim of a malware cyberattack involving remote control of my phone through an application installed via WhatsApp. First, the criminals opened an online bank account in my name and then applied for a RON 29,000 loan on my behalf. They told me that the money was mine and that I could use it. I requested the cancellation of the loan the following day, reported the case to the police, and notified the bank, first by phone and then in writing. The thieves also gained access to my accounts, from which they stole RON 90,000. Half of the amount was in an account for which I was an authorised representative and belonged to other people; the rest was from my personal account. The funds were withdrawn through a series of successive transactions in order to circumvent security limits. All communication with the criminals took place via WhatsApp and by phone, and in some cases these conversations lasted more than four hours."*

Bank's response:

"The payments and transactions from the consumer's accounts were made through the home banking application, in compliance with customer authentication requirements, by entering the security code defined when the application was activated or by using the phone's biometric authentication. Regarding the transactions carried out on the account where the defrauded person was an authorised representative, the funds corresponding to these payments were transferred to the user's personal account and subsequently used. The bank carried out all transfers in accordance with the instructions received. Under the law, a payment order is considered correctly executed if it is carried out in accordance with the IBAN indicated by the payer."

Ion R., Ifov: *"I was called by a criminal who claimed to be an employee of a commercial bank and told me that someone had used my personal data to apply for a personal loan. When I told him that I had not requested it, he connected me to another person who claimed to be from the police. The latter then directed me to someone else who said they were from the National Bank of Romania. This person told me that I had to take out a loan of approximately RON 100,000 from the bank, withdraw the money in cash and use it to purchase crypto assets from a crypto ATM. I deposited amounts of RON 10,000 into the ATM, as instructed, and requested proof of deposit for each amount. After I had deposited the entire sum, they told me to call two phone numbers to approve the transactions."*

. **Mădălina E., Iași:** *"I was the victim of a complex banking fraud and identity theft, resulting in a personal loan being taken out in my name in June 2026. My consent was compromised, and the funds were immediately transferred to external accounts for the purpose of money laundering. The loan was obtained through psychological manipulation and identity theft. There is an ongoing police investigation. I notified the bank and the National Directorate for Cyber Security (DNSC). In view of the above, I request the immediate suspension/cancellation of my obligation to pay the instalments related to this loan until the criminal investigation is completed. I also request that any payment delays not be reported to the Credit Bureau, given the fraudulent nature of the loan agreement."*

Mihai U., Prahova*: "Between March and September, based on a friendship with a person who used a false name and claimed to be a lawyer, I handed over control of my mobile phone to this person. They accessed my home banking applications and gained access to my accounts held with three commercial banks. They then requested the issuance of a credit card from one of these banks and carried out several unauthorised transactions, causing me losses of more than RON 15,000. The bank is asking me to repay the loan, claiming that access was authorised by me. Having no other option, I agreed to a 36-month repayment plan in order to avoid enforcement proceedings."*

Emil D., Vrancea: *"A RON 66,000 loan was fraudulently taken out in my name without my consent or signature. The situation was caused by identity theft. Although I completed a video identification process for an investment broker on Facebook and for an investment application, I do not consider this to constitute my consent to the loan that was taken out. The police have opened a criminal investigation in rem concerning computer forgery."*

Toader D., Caraș-Severin: *"I was the victim of fraud after being contacted by individuals who falsely claimed to be representatives of the National Bank of Romania and criminal investigation authorities. Under the pretext that my banking details had been compromised, I was deceived and induced to take out a RON 110,000 personal loan without giving my genuine consent. The money was taken by the criminals. A criminal investigation has been opened in this case. I request the temporary suspension of the payment obligations related to the loan until the situation is clarified."*

Dumitru L., Ilfov: *"I request the negotiation of an amicable solution for suspending loan instalments or rescheduling the loan following a complex banking fraud involving 'social engineering'. I was manipulated into withdrawing cash and depositing the RON 70,000 loan proceeds through 14 transactions at a Bitcoin ATM. I immediately reported the incident to the Ilfov Police and the bank. I am requesting a grace period until the criminal investigation progresses, in order to avoid enforcement proceedings and being reported to the Credit Bureau. The monthly instalment of RON 1,450 on the loan through which I was defrauded represents more than 30% of my monthly net income."*

Viorel V., Covasna: *"After accessing a fake website, I was contacted by a person who convinced me to buy shares in Hidroelectrica, and I was subsequently put in contact with a broker. I provided my personal details and agreed to trade the shares. I realised that something was wrong and tried to call the phone numbers from which I had been contacted, but they were no longer valid. Although I blocked my bank accounts, the criminals had managed to access one of them and withdraw RON 10,600, representing my savings. They also took out a RON 67,000 personal loan in my name, repayable over 60 months. The loan was obtained online through the bank's application installed on my mobile phone."*

Alexandru Păunescu, representative of the National Bank of Romania on the CSALB Coordination College: *"A worrying phenomenon is increasingly affecting consumers of financial products and services.* ***Fake loans*** *are causing losses of tens of thousands of euros, and in most cases the losses are borne entirely by consumers who allowed criminals to access their accounts, home banking applications or even their own phones and laptops.*

Most fraudulent loans are taken out online, after criminals emotionally manipulate their victims and claim to be 'from the bank', 'from the police' or 'from the National Bank of Romania'. However, CSALB also receives cases in which people took out loans under psychological pressure from criminals and subsequently transferred the money to accounts controlled by them.

Another type of fraud *involves criminals exploiting consumers' desire to make money quickly by purchasing shares or crypto assets. Through remote-control applications, criminals can steal savings accumulated over years within seconds or take out loans in the names of their victims.*

Our primary recommendation *is to carefully verify the authenticity of calls or messages received that ask consumers to carry out financial transactions urgently, under various pretexts.*

Particular attention *should also be paid to situations in which consumers are asked to undergo video identification, as such recordings can subsequently be used through deepfake techniques to authenticate access to banking applications. In practice, attackers can use video and audio recordings to bypass banks' security systems.*

We ***remind consumers*** *that banks never ask for access credentials (username, password) or authorisation codes (PIN, CVV), regardless of the communication channel. Avoid accessing links received via SMS, WhatsApp, email or social media messages that appear to come from your bank, especially if you are asked to act quickly or provide personal or banking details.Do not download applications at the request of other people and do not follow instructions received by phone, which typically involve supposedly urgent situations requiring you to make payments or transfers or block/unblock accounts. Check your transactions and account balances regularly and enable notifications so that you can immediately identify any suspicious activity. Secure your phone and applications with passwords and never share them with anyone."*

***

About CSALB: CSALB is an entity established as a result of a European Directive and provides free conciliation and negotiation services, within less than three months, between consumers and banks or non-bank financial institutions (NBFIs) regarding ongoing contracts. Consumers from any county in Romania can submit requests to the Centre for Alternative Dispute Resolution in Banking (CSALB) by completing an online form directly on the www.csalb.ro. If the bank agrees to enter the conciliation/negotiation procedure, a conciliator is appointed. CSALB works with 16 conciliators, among the leading legal experts with expertise in the financial and banking sector. The process is entirely amicable, and the agreement reached by the parties has the force of a court judgment. More information about the Centre's activity is available by calling 021 9414 (standard-rate call).