Beware of attempts to defraud bank accounts! Requests on this ground have grown in numbers at ABDRC

14 December, Bucharest. This year, the **Alternative Banking Dispute Resolution Centre (ABDRC)** received 46 requests grounded on account fraud, with an increasing number of requests in December, also caused by the fact that online transactions have increased in number as well. Only one third of these requests (14 cases) were accepted by the banks for negotiation, the rest were rejected after the merchants invoked the fact that the bank is third party to the obligation of restitution or the payments were made by **consumers who disclosed their personal information and entered all security data themselves**.

Examples of cases where banks have accepted negotiation with consumers at ABDRC

Cloned websites / online payments: L.S. from Iași made an online payment amounting to RON 40,000, which the consumer later challenged, after noticing that the website was a clone of the original one. Following negotiations at ABDRC, the bank offered, as a commercial gesture, the amount of RON 20,000. The resolution mentioned that, should the prejudice be recovered following police intervention, the consumer undertakes to return the amount received from the bank.

Card data sent by SMS/e-mail: The consumer C.L. from Bucharest disclosed her personal card data following an ad posted on a sales website. The prejudice amounted to RON 17,280, and the bank offered, as a commercial gesture, the amount of RON 8,640. The consumer undertakes to return this amount to the bank should the prejudice be recovered.

International payments / account fraud: Consumer F.S. from Harghita noticed that, without his consent, payments were made from his personal account to multiple companies in Spain. The bank returned the entire amount (RON 2,400) of the challenged transactions. The resolution mentions that the bank is to recover this amount if the prejudice is recovered following the criminal action carried out in this case.

Alexandru Păunescu, representative of the National Bank of Romania in the ABDRC's Steering Board: *"The issue of account fraud, card fraud or personal data theft entails a great deal of responsibility from both consumers and banks. We recommend consumers to check their account more often, in particular during these times. If they do not have online banking applications to do this remotely, one method would be to access SMS notification services of payments made from the account. Even if this involves a fee charged by the bank, it is better safe than sorry in such cases, and the benefits are indisputable. Then, if they notice that money has vanished from their account, they should immediately notify the bank and the Police and file a refusal of the payment that they consider fraudulent. Banks have a responsibility to resolve consumer chargebacks as quickly as possible, so that payments made unlawfully are not processed and money is not transferred from consumer accounts. Our recommendation is that banking institutions optimize their procedures for blocking payments reported by consumers as fraudulent. These claims of fraud should be flagged and filtered through all banks' customer relations channels, whether we're talking about call-centers, e-mail, chat or complaint pages. In addition, it would be advisable for banks to mention, in a*

place as visible as possible on their own websites, the recommended timeframe for consumers sending the refusal of payment for cases when they notice an attempted account fraud."

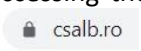
How are cybercriminals trying to defraud you

- Through e-mails in which you are notified that you have won an expensive gift (or even received an inheritance) following a contest in which you did not even participate;
- Through cloned sites that have different content from the original ones. They often announce unnaturally high discounts, even for newly launched products;
- Through phone or social media messages that include links and appear to be sent by friends, relatives or colleagues;
- Through placing fake ads on Google, which sometimes appear when you type the name of a bank into the browser or search engine. The ads mimic the bank details and direct you to a page that clones the screens of the Internet Banking platform. Thus, when you enter your login details, they are copied by criminals to fraudulently log into your account.

Phishing refers to banking information fraud: Consumers are misled by messages that appear to be sent by the bank **asking them to communicate confidential information (card number, PIN, user or authentication codes)**; they receive text messages in the name of the bank in which they are asked for activation data, passwords or activation codes, or they are asked to change the existing security data. If you received such a message, call the bank or write to the bank representative you are in contact with and explain what happened.

How to avoid fraud? Check the information received!

If you receive messages informing you that you are about to collect a sum of money or a cash prize in your account, you can verify the authenticity of the message based on the information requested. Thus, **in order to receive an amount of money, it is necessary to transmit only the IBAN and your name**, not the card data. You only need to enter your card data if you want to make an online payment yourself.

When shopping online, you can check if the site is safe for entering personal data by accessing the information available in the padlock displayed next to the website name → 

Do not proceed with the payment if you suspect anything, and if you already made the payment, request the bank to block the transaction immediately.

Another verification method is the name of the e-mail address from which you receive the message or the phone number from which it is possible to receive the text message. If you notice grammar mistakes, abbreviations, or unusual graphics in the message you receive, these are additional signs that it does not originate from the bank, but from a fake or fraudulent account.

Another important tip is not to access **online banking applications** through search engines. Do not share your login data and passwords to online banking applications to anyone!
Do not enter your PIN on any website you visit, **no genuine online transaction will ask for this data from you!**

Pay close attention to envelopes sent by banks containing cards/PINs. They must be intact and the initial PIN set by the bank must be changed at the first opportunity. In addition, **never keep your personal card and PIN in the same place.**

About ABDRC: ABDRC is an entity set up under a European Directive, and intermediates, free of charge and in not more than three months, negotiations between consumers and banks or NBFIs, for contracts/agreements in progress. Consumers from any county of the country may file applications with the Alternative Banking Dispute Resolution Centre (ABDRC) filling-in an online form directly on the website www.csalb.ro. When the bank accepts to enter the conciliation negotiation procedure, a conciliator is appointed. ABDRC works with 19 conciliators, of the best specialists in law and with relevant experience also in the financial and banking field. Everything is settled amicably, and the understanding between the parties has the power of court judgment. More information about the work of the Centre is available by phone at 021 9414 (charged a normal rate).