TRENDS AND FRAUD ATTEMPTS NOWADAYS:

I. A fake letter from a contracting party, partner, relative or friend regarding a change of their bank accounts

You may receive a fake e-mail from a partner of yours to whom you make regular payments or transfers. The e-mail will inform you that your contracting party has new bank accounts which shall be used for any future payments. You should know that this is a fraud attempt which is designed to make the customer order a transfer to the fraudster's account.
When you receive information about any change of your contracting parties' data (accounts, address, phone number, etc.), you should always contact them personally in order to confirm the changes with them. Carefully compare the received e-mail with previous e-mails from the same sender.
When there is a change of an account for invoice payments, always contact your contracting party through a channel other than e-mail, in order to confirm the payment details. When you buy goods advertised on the Internet, give the retailer's website and the advertisement a close check.

II. A fake phone call or e-mail

This fraud scheme involves a phone call or an e-mail from a person that claims to be acting on behalf of a renowned institution (the Bank, a courier service company, an Internet provider, various state institutions, utility services providers, etc.). In the conversation or the e-mail, on the pretext of providing assistance – correction of a wrong transfer, an expected delivery, etc., you are requested to provide the code you have received via SMS or other important information. You should know that institutions do not require personal and bank information. Therefore, never provide SMS codes, passwords for access, bank card numbers, etc. to people over the phone or in response to an e-mail. Write down the phone number of the person who is calling or forward the message to the Bank and contact its 24/7 Call Center.
If you receive e-mails from institutions, as mentioned above, with information that your card has been blocked, that your profile has to be updated, etc., with instructions for recovery of the access by clicking on a link and providing personal data, you should know that this is a phishing attack intended to get confidential information from you, which will then be misused. If there are attached files to the e-mail, do not open them. They may corrupt your device. Do not install any remote access applications on your devices that you use for generating and sending payment orders via electronic channels. Follow the security recommendations of the manufacturer and the Bank.

III. Fake lending offers via social media

This scheme involves receiving offers for credit products from fake profiles of the Bank or other institutions on social media and through channels such as Viber, WhatsApp and other similar ones. If you receive such an offer, be vigilant and do not provide your personal data and your bank card data, or any relevant one-time passwords or activation codes for a particular service. Do not provide photos (copies) of ID or bank cards and do not send your bank cards to third parties.
Be particularly careful when asked to deposit amounts of money as a fee, commission or for other reasons to accounts of individuals at bank institutions in relation to applying for financing.

IV. Bank card frauds

Using debit and credit cards is a part of our everyday life and it is becoming more and more popular for online payments. Therefore, people engaged in fraudulent schemes are particularly interested in this sphere. We recommend that you be vigilant when making purchases from new and/or unfamiliar websites and online retailers offering attractive prices of goods and subscriptions. Make sure you are using the website of the actual online retailer and not of someone that strongly resembles it and copies it.

Read carefully the delivery conditions, the return policy and the right to reject an order. Check the available information about the retailer, including reviews and recommendations by people you know.
Choose websites that are a part of the programs of Visa and Mastercard for secure bank card payments - Verified by VISA and MasterCard Secure Code. If the website does not support them, check if it is protected - look for the key or the padlock symbol, and for https:// before the web address.
Keep your card data safe, do not provide them to other persons and do not leave them unattended at public places. Do not keep your PIN code together with the card on paper or other medium.
Be vigilant when making purchases and when selling items on various platforms. Do not follow links that third parties have sent to you and do not enter your bank card data before making sure that the counter party is reliable. Do not provide the dynamic password received by you for confirmation of a particular online card payment to third parties in a phone call or chat application. This password is unique and intended for personal use only when you make purchases from Internet retailers.

In case you have any suspicions about a fraud, loss or theft of a card, please, contact the Call Center of the Bank in due time at 0700 1 84 84 (short number 1 84 84) or via e-mail: CallCentre@UniCreditGroup.bg.

V. Investment frauds

With this type of schemes the fraudsters try to lure people to invest funds by promising high profitability and low risk. They may ask you to invest in shares, bonds, commodities, currency, etc. A fraudster may lie to you or give you false information about an existing investment.
More often than not, people who try to mislead you, pretend to be professionals by creating fake profiles on social media, e.g. in LinkedIn. Usually, the fraudster creates an account and directs the user to a legitimate investment platform. However, after winning his/her trust over a period of several months, the fraudster would ask the victim to move the investment to a website under his/her control. As a result, the victim's account is drained.
In order to avoid such a fraud scheme, you should check if the company offering investment services has a license. You can find information about licenses on the website of the Financial Supervision Commission. It is also important not to trust people contacting you on social media and promising investment assistance, unrealistic profit and zero risk.

VI. Phone frauds

There are telephone fraud attempts from international phone numbers with a single call. You should know that the point of these calls is to attack your phones remotely in order to gain control over them and steal personal and financial information recorded there. These malicious acts are possible if you answer the call or call back.
Therefore, you should answer and call back only if you know the phone number. You shouldn't answer or call back international phone numbers or follow any instructions to call a phone number comprising untypical symbols. If you had such a call and you answered or called back, change the passwords to all of your accounts that you use on your phone. If the services you use have an option for a higher protection level (additional confirmation, second password), you should activate it. Check if you are the only administrator of your phone. If there is a process or administrator other than the ones you know, you should remove it.
If you are in the slightest doubt about a misuse of your personal data, you should immediately contact the bank at 0700 1 84 84 or 1 84 84.

VII. Other types of frauds

Very often fraudsters create a fake online identity in order to establish a relationship and win the victim's trust. Criminals hide behind a fake identity on various dating websites, social media and in e-mails. The fraudster's intention is to establish a connection as fast as possible, make the victim like him/her and win their trust. Fraudsters may propose to the victim, or make plans for dates, but this will never happen. Eventually, they will ask for money. Criminals often say that they are abroad, which makes it easier to avoid a date and is more

plausible when they ask for money for emergency medical help, to buy airplane tickets or to pay for unexpected charges and expenses. Remember that you should not send money to people who communicate with you on the Internet or over the phone, or provide personal or bank data.

There are types of frauds where the victims receive an e-mail or a letter on behalf of a bank, lawyer, etc. stating that they are the heirs of a distant relative they have usually never heard of. In this type of frauds the criminals say that it is difficult to access the supposed inheritance because of governmental orders, taxes or bank restrictions in the country where it is kept and that a particular amount has to be paid and/or personal data provided in order for the inheritance to be received. Remember that there is no shortcut to becoming rich: if it sounds too good to be true, it probably is.