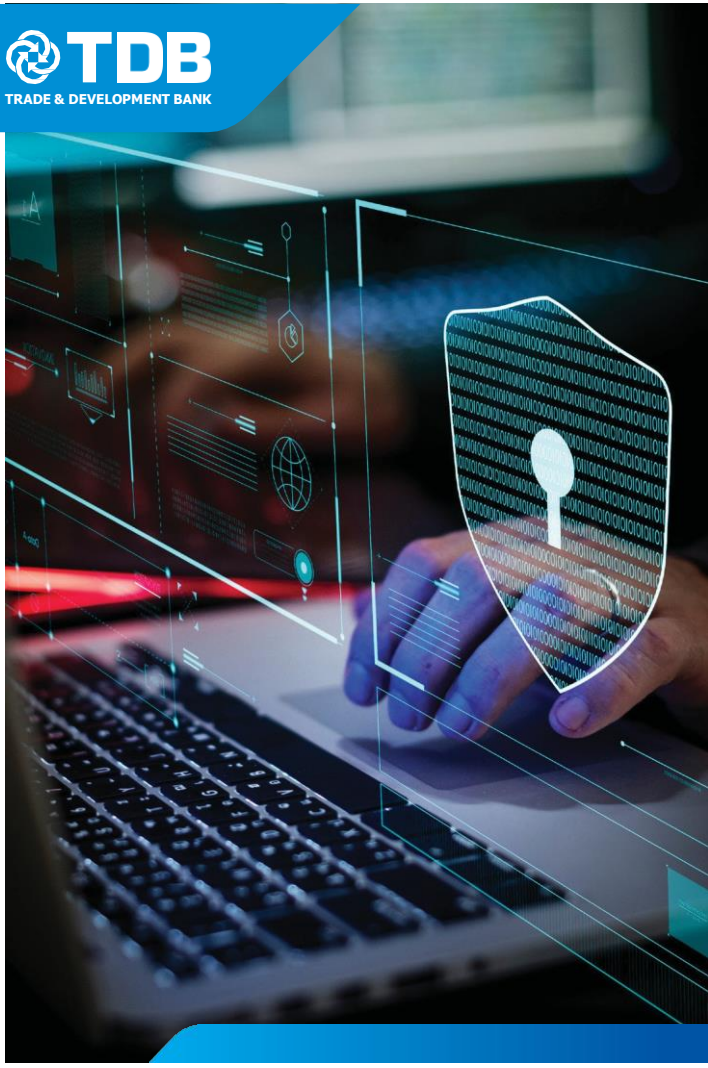
TDB
TRADE & DEVELOPMENT BANK



RECOMMENDATIONS FOR EXECUTING INTERNATIONAL TRANSFERS AND PREVENTING CYBERCRIME

RECOMMENDATIONS FOR EXECUTING INTERNATIONAL TRANSFERS AND PREVENTING CYBERCRIME

The Bank is committed to ensuring the fast and efficient processing of its customers' international transactions and to delivering banking products and services in accordance with international standards. Therefore, the Bank adheres to the Law on Anti-Money Laundering and Combating Terrorist Financing, international standards, as well as the requirements of regulatory authorities, and correspondent banks.

As part of this compliance framework, the Bank may place specific monitoring measures on certain customer transactions. Within the scope of this monitoring, the Bank collects and verifies relevant documents, declarations, and information to identify and know its customers and their transactions.

With the rapid development of modern technology, fraud, illegal activities, and criminal offences in the digital environment have significantly increased. For example, incidents such as phishing, fraudulent communications from foreign countries, the use of third-party accounts to route online gambling transactions, scams, and money laundering have become more prevalent in recent times. These indicate a growing trend in the use of digital channels for illegal purposes.

Therefore, in accordance with international best practices and insights gained from long-term observation, the Bank has prepared the following recommendations to protect customers from potential risks and from becoming victims of criminal activities.

We kindly request that our customers carefully review the recommendations provided below prior to initiating any international transactions and take precautionary measures to protect themselves from potential risks and criminal exploitation.

In instances where a financial relationship is being established for the first time with the beneficiary of an international transaction and an international transaction is being conducted:

Recommendations:

- Avoid transferring funds to individuals from foreign countries whom you have only encountered online and have never met in person;
- Conduct appropriate due diligence using official sources to confirm whether the beneficiary is legitimate, active, and engaged in genuine business activities (particularly for entities);
- Refrain from transferring funds derived from money borrowed from family, friends, or colleagues, or obtained by mortgaging or selling real estate or vehicles;
- Carefully verify the International Bank Account Number (IBAN). European banks utilize the IBAN system and process payments solely based on the IBAN, without cross-verifying the beneficiary's name. If the IBAN is entered incorrectly, funds may be transferred to an unintended account. In such circumstances, returning or tracing the transaction may be impossible or may require significant time and expense, potentially resulting in permanent loss of funds;
- Obtain appropriate documentation. Ensure that you possess an invoice or relevant supporting documents from the beneficiary, detailing the transaction. These documents should include the particulars of the parties involved and must be stamped or officially verified.

If you have not verified the beneficiary, and the beneficiary has notified you remotely or via electronic channels that their receiving bank or account number has changed, and you are about to initiate the transaction based on this newly provided information:

Recommendations:

There are instances in which hackers gain access to the email accounts of foreign business entities and notify their partners of a change in bank or account details, supplying their own fraudulent account information instead. As a result, payments for goods and services may be transferred to these fraudulent accounts. In many such cases, your business partner may be unaware that their email has been compromised, as all other communications may appear normal.

If your business partner notifies you of a change in banking details, you should always:

- Verify through a separate and trusted channel (such as by phone call) before making any payments;
- Confirm through official sources that the beneficiary is a legitimate, active entity with a physical presence;
- Transfer funds only to verified and confirmed accounts;
- Request a stamped and officially verified invoice from the beneficiary that includes all relevant transaction details;
- Do not rely solely on emails to confirm sensitive changes, always make a phone call to verify such changes.

In cases where a third party, with the intent to conceal their identity, information, and actions, covertly controls another customer's account and executes transactions through it by offering compensation to the account holder, and obtains the customer's internet banking credentials:

Recommendations:

- Do not disclose your confidential information or permit its use by third parties due to the influence or persuasion of others;
- If a third party gains control over your account, you will bear full responsibility. Be aware that your information will appear in the transaction records of related accounts; therefore, do not accept such requests.

Hacking a customer's personal information in order to commit fraud and conduct illegal transactions:

Recommendations:

- Regularly update your personal information and do not share it with anyone to maintain security;
- Never share your internet banking credentials or one-time passwords (OTPs) with anyone under any circumstances;
- If you notice or suspect any suspicious activity in your account or internet banking, immediately contact your bank and report it.

In cases involving advance payments regarding the internet advertisements, coins, artificial pricing, fraudulent projects, financial assistance, loan services, trade, or commercial offers:

Recommendations:

- When trading cryptocurrency or making investment transactions, always research the investment project or coin using reliable sources;
- Avoid taking loans or making investments under the pressure or intimidation from others, or without proper financial planning;
- Be cautious of social media advertisements, such as "Foreign currency exchange at low rates", "Cheap items for sale" or "Loan offers". These advertisements often attract attention and may require advance payments or service fees before delivering the product or service. Such conditions are highly likely to be part of fraudulent schemes. Individuals involved in these scams often reside abroad to evade law enforcement, but they typically use domestic commercial bank accounts to receive funds. Remain vigilant and avoid falling for such false or baseless advertisements. Protect yourself from the risk of financial loss.

If you are asked to make a payment in order to receive a gift, goods, inheritance, or business investment:

Recommendations:

- **A Romance Scam**, a type of fraud committed through romantic manipulation, is a common international scheme. Scammers establish long-term relationships with victims via social media, chat platforms, or other online channels to gain their trust. Once they have gained the victim's trust, scammers often claim to have sent gifts, cash in a safe, or valuable items that are "stuck at customs" in a foreign country, and ask the victim to pay related fees. Other common tactics include requesting money for travel expenses or plane tickets to visit the victim. To receive money quickly, scammers frequently use money remittance services such as MoneyGram. These services typically involve currency exchange agents or non-bank financial institutions (NBFIs) as receiving agents, making it nearly impossible to trace or recover the funds once sent. Therefore, please protect yourself from such romance scams and prevent financial loss by recognizing these tactics and avoiding suspicious online relationships.

- **Fake Investment Scam** - This is a common international fraud scheme in which individuals or entities are deceived into believing that scammers will invest a large sum of money in their business project or proposal. Scammers convince victims to pay various fees under the guise of legal, notary, or service charges. These fraudsters often present themselves as professionals in the investment sector, promising foreign currency investments ranging from millions to billions. To gain trust, they may send fake business partnership agreements or fabricated transaction documents claiming that large sums have been sent. It is also common for such scammers to operate under fictitious company names, use counterfeit seals, and create fraudulent websites. Therefore, please protect yourself from becoming a victim of such deceptive schemes. Avoid risking your financial assets, time, and the reputation of your organization by engaging with suspicious investment offers.

- **Inheritance Scam** - This type of fraud is common and targets individuals regardless of family background, financial status, age, or gender. Scammers initiate contact from foreign countries, claiming that "your name matches the beneficiary of a deceased person's inheritance". They attempt to gain trust by promising to send packages or large sum of money. Initially, they persuade victims to transfer payments for legal services or notary fees. To receive money quickly, scammers often use money transfer services. These services typically involve currency exchange agents or non-bank financial institutions (NBFIs) as receiving agents, making it extremely difficult to trace or recover the funds once sent. Please protect yourself from falling victim to such scams and avoid the financial risks associated with these fraudulent schemes.

TDB
TRADE & DEVELOPMENT BANK

FOR MORE INFORMATION:

Phone: +976 1800-1977
E-mail: info@tdbm.mn
Website: www.tdbm.mn