Online Wire Transfer Best Practices

At First State Bank, your security is of the utmost importance. We believe that the best defense against fraud is for us to keep you as informed as possible.

Wire Transfers are the perfect target for fraud. Here are a few reasons why:

- Speed of the transaction/Same day availability
- Transactions are Irrevocable
- Most banks match incoming wires **by account number only**

Information Requested prior to sending a Wire Transfer:

- Creditor information. Creditor refers to the beneficiary party of the wire payment. An address of at least the town and state (country) is now required per ISO format.
- Creditor Agent information. Creditor Agent refers to the beneficiary bank. Instructed Agent will be the same as the Creditor Agent in most cases. An address of at least the town and state (country) is now required per ISO format.
- Full wire transfer instructions
- Purpose of the wire transfer
- Your relationship to the creditor/beneficiary
- An invoice or copy of the wire transfer instructions

Stay Informed! Common Examples of Wire Transfer Fraud:

- Romance Scams occur when a criminal adopts a fake online identity to gain a victim's affection and trust. The scammer then uses the illusion of a romantic or close relationship to manipulate and/or steal from the victim.
- Investment Scams happen when people try to trick you into investing money. They might want you to invest money in stocks, bonds, notes, commodities, currency, or even real estate. A scammer may lie to you or give you fake information about a real investment. Or they may make up a fake investment opportunity.
- Identity Theft Scams is a type of fraud that involves using someone else's identity to steal money or gain other benefits.
- Timeshare Scams include scammers who call sellers of timeshares, posing as a reseller or real estate agent. The scam artist claims to have a buyer for the timeshare or guarantees he can sell the timeshare for a good price.
- Business Email Compromise OR Account Takeover are a sophisticated scams that targets both businesses and individuals who perform legitimate transfer-of-funds requests. In a BEC scam, criminals send an email message that appears to come from a known source making a legitimate request, with fraudulent payment information.

Online Wire Transfer Best Practices

Tips to avoid wire transfer fraud. Help us keep your money safe!

- Use Proper **Call Back** Procedures
- Call a phone # that is already on file or known prior to the request
- Callbacks should be made by **phone call** (Email and Texts are **not** sufficient)
- Always verify the routing and account number
- Always verify the amount of the request
- Use Online Wires with Wire Templates
- Protect your computers & your online banking access