Fraud Watch

This year, we have seen a significant rise in Identity Theft, Fraud and Scam attempts across the banking industry. At BSNB, we take the security of our customer's information and financial well-being seriously, and we continue to enhance our cyber security services and protections on a continuous basis. As a consumer, the best way to avoid being a victim is to be informed. Below is an excerpt from the Consumer Financial Protection Bureau (CFPB, a U.S. government agency that ensures fair treatment by banks, lenders, and other financial companies) and a link to the full article discussing what you can do to help prevent these types of attacks happening to you.

If you have any questions or doubts about a transaction or instructions concerning your accounts, please contact us immediately so we that can help protect you and your assets. Additionally, you can check out our Security Page on the BSNB website to stay current on mobile and on-line scams and how to keep your accounts secure.

Remember, per BSNB policy, we will **never** request information that is confidential in nature regarding you or your accounts via email or text message. If you receive an unsolicited email or text message that appears to be from BSNB and it requests confidential information, we recommend that you do not respond. If you receive such an email or text message, please contact your BSNB representative.

Online and Mobile Security | BSNB
What are some common types of scams? | Consumer Financial Protection Bureau (consumerfinance.gov)

Some Common types of fraud and scams

Imposter scams

Imposter scammers try to convince you to send money by pretending to be someone you know or trust like a sheriff; local, state, or federal government employee; or charity organization.

Mail fraud

Mail fraud letters look real but the promises are fake. A common warning sign is a letter asking you to send money or personal information now in order to receive something of value later. Examples of mail fraud might include notices of prizes, sweepstakes winnings, vacations, and other offers to claim valuable items.

Money transfer or mobile payment services fraud

Con artists use money transfers to steal people's money. If someone you don't know asks you to send money to them, it should be a red flag. Scammers also use mobile payment services to trick people into sending money or merchandise without holding up their end of the deal. For example, a scammer may sell you concert or sports tickets but then never actually give them to you. Or a scammer might purchase an item from you, appear to send a payment, and then cancel it before it reaches your bank account.

Using mobile payment services with family, friends, and others you know and trust is the safest way to protect your money. You should also be cautious when people you do know ask you to send them money. Before you send money, verify that they are the ones requesting it.

Never send money to someone you don't know. If you think you made a money transfer to a scammer, contact your bank or the company you used to send the money immediately and alert them that there may have been a mistake.

Common payment methods used by scammers

Never send money to someone you don't know. Scammers use a variety of ways to collect money from you, including:

- Wire transfers
- Person-to-person payment services and mobile payment apps
- Gift cards

Reporting fraud and scams

If you're a victim of a scam, you can report it to the authorities by:

- Submitting a complaint online with the Federal Trade Commission
- Contacting your local police or sheriff's office
- Reporting it to your state attorney general

BSNB
Ballston Spa National Bank