

Fraud Information

Check Fraud

There are several basic forms of check fraud used by fraudsters, including:

- **Forged Checks** - Forged signatures are typically found on legitimate and unused check stock that is stolen by criminals when they then forge either the payer signature or an unauthorized signature on the check;
- **Counterfeit Checks** - Counterfeit checks are imitations or copies of genuine customer checks. They are drawn on valid bank accounts and may or may not be a precise duplication of an actual check. To produce a counterfeit check the counterfeiter just needs to have valid bank account information;
- **Altered Checks** - Occurs when a legitimate check is issued by a valid drawer and is altered without the drawer's approval. Either the payee or a criminal, who has illegally obtained the check, modifies the dollar amount or payee name and attempts to present the check; and
- **Washed Checks** - Washed Checks occur when a legitimate check is issued by a valid drawer and is washed with a chemical agent, which removes all written information, leaving the printed information. The criminal then completes the check with new information.

How Does Check Fraud Occur?

A criminal/fraudster obtains information to conduct check fraud by:

- **Mail Theft** - Stealing mail from mailboxes;
- **Car Break-ins** - Stealing checkbooks, purses and briefcases from vehicles;
- **Office Creepers** - These individuals are dressed like your coworkers or building service personnel and rely on the anonymity of busy office buildings to cover them during their crime. Also working in tandem criminals/fraudsters will enter an office, office building or business and while one keeps the employee/staff busy the other one goes through the office to find the checkbook. They then take checks out of the middle or end of the check stock
- **Dumpster Diving** - Exactly like it sounds, going through trash to find personal information.

How Can I Help Prevent It?

- Limit the amount of information on checks. Do not print your drivers license or social security number on your checks;
- Carry your checkbook with you only when necessary; and
- Store new and cancelled checks in a safe and secure location.

ATM\ITM and ITM Safety Precautions

Automated Teller Machines (ATMs) and Interactive Teller Machines (ITMs) provide a fast and convenient banking alternative for account holders. To ensure your safety when using an ATM\ITM, please follow these important safety precautions.

Before you go to an ATM\ITM:

- Have your ATM\ITM card out and ready to use;
- Protect your Personal Identification Number (PIN) and memorize it. Do not write your PIN on the card or carry it with you, and do not share your PIN with anyone, including family and friends; and
- Consider having someone accompany you when the ATM\ITM is used after dark.

Choosing an ATM\ITM:

- Be alert and aware of your surroundings and use an ATM\ITM that is in an open space with bright lights;
- If someone appears to be loitering around the ATM\ITM, go to another location;
- If anything looks suspicious, consider canceling the transaction and leave the area at once; and
- If the ATM\ITM looks different or appears to have any alterations or attachments to the card slot or PIN pad, do not use it Immediately report anything suspicious to the bank that operates the ATM\ITM.

At the ATM\ITM\ITM:

- Focus on what you are doing. Don't use a cell phone or do anything else that diverts your attention;
- Never allow a stranger to assist you in conducting an ATM\ITM transaction, even if you have trouble;
- If the ATM\ITM retains your card, notify the branch as soon as possible;
- Prevent others from seeing your PIN entry by using your body or hand to shield the ATM\ITM keypad;
- If you are in a vehicle at a drive-up ATM\ITM, only open your window when you are ready to make a transaction. Keep your doors locked and the engine running;
- When you are finished, put your receipt, card, and money away quickly. Count cash later in the safety of your vehicle, home, or other secure area;
- As you return to your vehicle after your transaction, have your car keys ready and observe the area around your vehicle;
- Go to the nearest public area where people are located if you are followed after making a transaction and call the police; and
- If someone does approach you and demands your money, do not resist. Remember everything you can about the person and call the police immediately.

Check Card Precautions:

Check cards provide added convenience in accessing your accounts. Please consider the safety precautions and additional protections listed below when using a debit card.

- Sign your card on the signature panel as soon as you receive it. Always keep the card in a safe place;
- When selecting a PIN, do not use your birth date, telephone number, or Social Security number;
- Never disclose your PIN to anyone. No one should ask for your PIN, including representatives from Third Coast Bank SSB;
- Do not disclose information about your card in response to an unsolicited e-mail or request;
- Look for secure transaction symbols (<https://> and a closed padlock icon) when shopping online to ensure your account information is protected. Consider using a credit card instead of a debit card for online purchases, as it may take more time to resolve unauthorized transactions or disputes with debit card fraud and money can be taken directly out of your checking account;
- Block the view of others when using a point-of-sale (POS) terminal in making debit card purchases;
- Check the purchase amounts on the sales receipt before signing. If the amount is different than the amount you owe, let the sales clerk know. Do not sign the receipt if the amount shown is erroneous;
- Review your bank statements or check your account history online regularly to verify if any unauthorized transactions are shown. Always keep your statements in a safe place;
- Destroy expired cards by cutting through the account number and signature area.