



My town, my bank™

Identity Protection



Identity Protection

What you need to know.

Hundreds of thousands of people are the victims of identity theft each year in what has become one of the fastest growing crimes in our society. Identity theft is a crime where someone wrongfully steals and uses someone else's personal information (such as name, credit cards, Social Security number, bank account numbers, driver's license) to commit fraud and/or theft.

Identity Theft: How it works.

Identity thieves use a number of different methods to steal your personal information:

- By stealing purses or wallets containing your personal ID, bank and credit card information,
- By intercepting your mail, including new checks, tax information and credit card information,
- By searching through your trash for personal information in a practice known as "dumpster diving",
- By fraudulently obtaining your credit report by posing as someone of authority,
- By discovering personal information in your home,
- By purchasing your personal information from sources such as store employees, and
- By using personal information found on the Internet.

Email Fraud

The Bank of Fairfield does not contact customers via email to verify or request security information.

However, you could receive fraudulent emails from another source, which could include the Bank's name and/or logo, asking for personal information. This is often called "phishing" or "spoofing." The purpose of fraudulent emails is to get you to divulge personal information in order to commit identity theft or to take money from your accounts. These fraudulent emails request the recipient to send personal information, such as Social Security or account numbers back to the sender via email. In other cases they include a web site or a link, which will then request the visitor to enter their private information.

Identity Protection

The Bank of Fairfield 2248 Black Rock Turnpike Fairfield, CT 06825 (203) 659-7610

Preventing a Fraud

The Bank of Fairfield highly values its customer relationships and we are committed to ensuring your privacy. As a customer you can also help protect your private information through theft education, practicing good security habits and reporting any suspicious contacts you receive via email, phone calls or mail.

Here are some things you can do to help protect your personal information:

- Use caution when selecting your PIN number and passwords. Create passwords and Personal Identification Numbers (PINs) that are unpredictable. Remove all PINs and passwords from your purse or wallet.
- Be cautious about revealing account numbers, Social Security or Tax I.D. numbers and other private information to other people.
- Protect your account numbers, card numbers, PINs and passwords. Keep items that carry your personal information in a secure place, including all credit cards, account numbers, expiration dates and the customer service numbers you would need to contact your creditors in the event your cards are lost or stolen.
- Never release personal data through the mail, by phone or over the Internet unless you have initiated the contact. Identity thieves may pose as bank representatives, Internet service providers, credit card companies and even government agencies in an effort to find out your SSN, account numbers and other personal information.
- Keep your Social Security card in a secure place. Do not carry it with you. Give your SSN only when absolutely necessary, and ask to use other identifiers whenever possible.
- Do not print your telephone number, driver's license number or Social Security number on your checks.
- Do not email confidential information to the Bank using your personal email accounts. You may email us using our secure Internet banking service.
- When you are making a purchase or conducting a financial transaction online, make sure that the web sites you visit are secure and protect your information from Internet theft. Be sure to use a secure browser that encrypts or scrambles purchase information and make sure your browser's key icon or padlock is active.
- Be sure to carefully review your monthly accounts, credit card statements and utility bills for any unauthorized transactions as soon as you receive them. If you suspect unauthorized use, contact the provider's fraud and customer service departments immediately.
- Periodically contact the major credit reporting companies to review and verify your credit information.
- Be wary of any promotional scams. Identity thieves may use phony offers to get your personal information.

Reporting a Fraud

If you have been the victim of identity theft regarding your accounts at The Bank of Fairfield, call us at 203-659-7610 or toll free at 877-966-1944. If you have received or responded to a suspicious or fraudulent email regarding your account, forward it to us at TBF@thebankoffairfield.com. In addition, take the following steps:

Notify the Credit Bureaus

Contact the fraud departments of each of the three major credit bureaus right away. Ask each agency to immediately place a "fraud alert" on your credit report and have them send you a copy of your credit file.

Equifax

1-888-766-0008
P. O. Box 740241
Atlanta, GA 30374
www.equifax.com

Experian

1-888-397-3742
P. O. Box 9530
Allen, TX 75013
www.experian.com

TransUnion

1-800-680-7289
Fraud Victim Assistance Division
P. O. Box 6790
Fullerton, CA 92634-6790
www.transunion.com

Identity Protection

The Bank of Fairfield 2248 Black Rock Turnpike Fairfield, CT 06825 (203) 659-7610

Contact Your Local Police

In the event of identity theft, it is important that you notify your local police department and file a report. Be sure to request a copy of the report for your records.

Contact the Federal Trade Commission

Call the Federal Trade Commission's (FTC) Identity Theft Hotline at 1-877-ID THEFT (1-877-438-4338). The FTC will put your information into a secure consumer fraud database and may, when appropriate, share it with other law enforcement agencies.

Check Your Mail Carefully

If you receive statements for accounts you do not have, contact the creditor. An identity thief may have opened an account in your name. Make sure no one has requested an unauthorized address change, title change, PIN change or ordered new cards or checks to be sent to another address.

Review All of Your Accounts

Check transactions on all credit account statements including credit cards, home equity lines of credit, bank accounts, investment accounts and telephone bills. Close accounts that have been tampered with and open new ones with new PINs and passwords. If an identity thief has tampered with your savings or checking account or ATM card, close the account immediately. When opening new accounts, avoid using easily available information for a password. Keep an eye on all of your accounts going forward.

You may also want to contact other agencies for other types of identity theft:

- The **Social Security Administration** if you suspect that your Social Security number is being fraudulently used (call 800-269-0271 to report the fraud).
- The **Internal Revenue Service** if you suspect the improper use of identification information in connection with tax violations (call 800-829-0433 to report the violations).
- Your local office of the **Postal Inspection Service** if you suspect that an identity thief has submitted a change of address form with the Post Office to redirect your mail, or has used the mail to commit frauds involving your identity.

Maintain a written record of what happened, what was lost and the steps you took to report the incident to the various agencies, financial institutions and firms impacted. Be sure to record the date, time, contact telephone numbers, person you spoke with and any relevant report or reference number and instructions.

Identity Protection

The Bank of Fairfield 2248 Black Rock Turnpike Fairfield, CT 06825 (203) 659-7610