

10 Ways to Prevent Identity Theft

Identity theft is a serious crime, one that affects millions of Americans each year according to statistics published by the Federal Trade Commission (FTC). Identity theft occurs when someone steals your personal information in order to commit fraud or other crimes such as opening credit in your name or using your information to make unauthorized purchases.

Unfortunately, anyone can be victimized and it can cost hundreds of dollars and many hours of your time to repair the damage that can be done to your credit and your personal reputation. Salisbury Bank is committed to protecting your privacy, but there are specific steps you can take to reduce your risk of identity theft.

1. **Protect your mail.**

- Promptly remove your mail from your mailbox. Take outgoing mail to the post office.
- When available, sign up for electronic statements and bill delivery to reduce sensitive account information coming to your mailbox.

2. **Shred it for safety.**

Shred all documents with personal or sensitive information before discarding them. For example: financial statements, medical receipts, and credit card offers.

3. **Lighten up.**

Empty your wallet or purse of extra credit cards and other personal information.

4. **Keep it safe.**

Keep items with personal information in a safe place. Don't leave personal items out in the open, even in your office, dorm room, meeting room, or any place outside your home. Secure personal information at home.

5. **Protect your Social Security Number.**

Memorize your Social Security Number. Do not carry your Social Security card with you and do not give it to anyone unless absolutely necessary.

6. **Be careful when sharing.**

Never give out personal information over the phone, internet or by mail unless you really know who you are dealing with.

7. **Watch for "Shoulder Surfers" and "Skimmers".**

- Shield the entry of PINs, and be aware of people standing close by when using your ATM, credit or debit card in public.
- Use ATMs that are familiar, so you are in a better position to recognize when the equipment looks different or doesn't "feel right." Your increased awareness may reveal a skimmer's attempt to steal PINs and banking details at that site.

8. **Credit and Debit Cards.**

- Monitor your accounts and billing statements for any unusual activity and take immediate action when you spot it.
- If you have applied for a new credit or debit card and it has not arrived in a timely manner, call the financial institution.
- Sign up for MasterCard® SecureCode™ or Verified by VISA. These services allow you to choose a private code which provides added protection against unauthorized use of your debit or credit card when you shop online at participating merchants. You can find links to sign up at our website www.salisburybank.com under Customer Security.
- Report lost or stolen cards immediately.
- Sign new cards and add: ASK FOR ID.

continued

- Save all receipts and match them to your statement.
- Note your billing cycle and look for your bill in the mail. Or, better yet, sign up to receive your bill electronically so you no longer receive it in the mail.
- Shred pre-approved credit card offers.
- Use a separate card for web purchases.
- Notify card companies and financial institutions in advance of changes in address or phone number.
- Never loan cards to anyone!

9. **Secure your computer.**

- Never click on unsolicited emails and do not provide passwords or personal information on sites that you do not know or look unfamiliar.
- Protect your personal information on your computer by installing a firewall and updating your virus protection.
- Use complex passwords. Make them as long as possible and combine letters, numbers and symbols (For example: bb&8\$3@*97). The greater the variety of characters that you have in your password, the harder it is to guess.
- Use secure websites: 1) Check the web page URL. Normally, when browsing the web, the URLs (web page addresses) begin with the letters "http". However, over a secure connection the address displayed should begin with "https" - note the "s" at the end. 2) Check for the "Lock" icon. For example, Microsoft Internet Explorer displays the lock icon in the lower-right of the browser window. Click (or double-click) on it to see details of the site's security. This is important to know because some fraudulent web sites are built with a bar at the bottom of the web page to imitate the lock icon of your browser!

10. **Monitor your Credit Reports.**

Check your credit reports annually from all three major credit bureaus: Equifax, Experian, and Trans Union. Place fraud alerts on your credit report with the credit bureaus if you suspect suspicious activity.

www.annualcreditreport.com: The official site to help consumers obtain their free credit report. Or call 877-322-8228.

Helpful Hint - Order a credit report every four months, each time from a different credit bureau. Each will be free and will allow you to stay current with your credit reports.

What if my Identity is Stolen?

Having your identity stolen is a very stressful situation. It is important for you to be patient and stay calm. Remember your creditors are equally anxious to straighten matters out, and you may be one of many people victimized by the same perpetrator.

- Contact your creditors and verify that no unauthorized activity has occurred. Advise them to be on the lookout for new account requests.
- Close bank accounts immediately if they have been tampered with. Open new accounts with new PINs.
- Call local law enforcement – Always insist on a written police report and obtain a copy as soon as possible.
- Contact the Federal Trade Commission (FTC) and the fraud department of each of the three credit bureaus.
- Keep a journal of all of your activity, phone calls, etc.

For contact information for the FTC and credit bureaus, visit the Bank's website at www.salisburybank.com, and click on Customer Security.

© Salisbury Bank and Trust Company, November 2008

Salisbury Bank and Trust Company (the Bank) has provided the websites listed above solely for your convenience, but we are not responsible for the content, links, privacy policies or security policies of these websites and do not imply any endorsement of or responsibility for the opinions, ideas, products, information or services offered at such sites, or any representation regarding the content at such sites. The Bank makes no warranties, either expressed or implied, concerning the content of such sites, including the accuracy, completeness, reliability or suitability thereof for any particular purpose, nor does the Bank warrant that such site or content is free from any claims of copyright, trademark or other infringement of the rights of third parties or that such site or content is devoid of viruses or other contamination.

Member FDIC

Salisbury Bank and Trust Company

5 Bissell Street
Post Office Box 1868

Lakeville, Connecticut
06039-1868

t: 860.435.9801
t: 800.222.9801

www.salisburybank.com