Protect Your Most Valuable Asset!

WHAT YOU NEED TO KNOW TO PREVENT IDENTITY THEFT AND FRAUD

Identity theft is a crime on the rise. In fact, the Federal Trade Commission (FTC) estimates that as many as 9 million people have their identities stolen each year.

Millbury Savings Bank wants to help you protect your information, your money, and yourself from identity thieves. Here are some important tips for keeping your personal and financial information safe.

Safeguard Your Identity

- **Keep your Social Security number private.** Other than banks and other companies that legitimately need your Social Security number (SSN) to open an account or for a credit application, be wary of giving that number to anyone. If a company uses SSNs as customer ID numbers, ask them to provide a substitute. Ask the Registry of Motor Vehicles to assign you a random number—typically beginning with "S"—in place of your SSN on your license. Don't write your SSN on your checks!
- **Shred anything that identifies you.** To avoid a crime called "dumpster diving" where crooks sift through landfills and dumpsters looking for information they can use, shred anything with your name, address, and other personally identifying information on it, especially credit card mailings and other offers of credit, bank and credit card statements, and receipts.
- **Review all bank and credit card statements**. Report any unauthorized transactions—even small ones—to your institution. If you act quickly, you will protect your right to dispute these transactions and may protect yourself from future fraud.
- **Watch for irregularities.** Signs that require immediate attention include bills that do not arrive as expected; unexpected credit cards or account statements; denials of credit for no apparent reason; calls or letters about purchases you did not make; and unusual credit or debit card activity.
- **Review your free credit reports annually.** Make sure that, once a year, you request your free credit reports from the three primary credit reporting agencies—TransUnion, Equifax, and Experian—by visiting AnnualCreditReport.com or by calling 1-877-322-8228. That way, you'll know if someone's been opening accounts in your name without your knowledge.
- **Check your children's credit reports.** Even children are not safe from identity theft. Often, crooks come across and try to sell "clean" Social Security numbers—those with no credit histories—which often belong to minors! Check the credit reports of your minor children to be sure no one's been opening accounts in their names.
- **Opt out of prescreened offers.** Under the Fair Credit Reporting Act (FCRA), credit reporting agencies can include your name on lists used by companies to extend you unsolicited "firm offers" of credit or insurance. But, the FCRA also provides you the right to "opt out," which prevents those agencies from providing your credit file information for firm offers. To opt out, visit OptOutPrescreen.com or call 1-888-567-8688. (Note: you will have to provide your Social Security number.)
- **Request a "security freeze."** Request a security freeze by sending a written request to each of the three credit reporting agencies directly. This prevents these agencies from releasing your credit report to third parties without your consent. Bear in mind, however, that this freeze can interfere with the timely approval of any requests you make for new loans, credit cards or other credit unless you take steps to lift the freeze. The fee will be waived if you or a spouse can prove you were a victim of identity theft.

For more information on preventing identity theft, visit the Federal Trade Commission (FTC) website or request their publications by logging on to Consumer.gov/idtheft or calling 1-877-ID-THEFT.

Protect Yourself Online

- **Know the problems.** Here are just some of the dangers that could be lurking online or in your computer:
  - **Malware.** A catch-all phrase for "malicious software," malware can be downloaded onto your computer unknowingly and without your consent in order to gain access to your personal information, send spam (unsolicited, bulk e-mail), and commit fraud. Malware can include:
    - **Spyware**. Designed to monitor your use, send pop-up ads, redirect your computer to certain websites, or record key strokes (called keylogging), which could lead to identity theft.
    - **Adware**. Often attached to free downloads, it's intended to monitor your computer use (including websites visited) and display targeted ads based on where you've been.
    - **Viruses**. Usually through an email attachment, viruses sneak onto your computer, copy themselves without your permission, and use up all available memory.
    - **Trojans**. These enable unauthorized people to access your computer and to send spam from it.
  - **"Social engineering" attacks.** To commit identity theft, these attacks lure you into giving up user names and passwords, PINs, account information, or debit or credit card numbers. They include:
    - **Phishing**. Fake email or pop-up messages made to appear authentic or from legitimate organizations and that include requests (or even threats) for information.
    - **Pharming**. Hackers redirect traffic from a legitimate site to a bogus one in order to gain users' login credentials or other information.
- **Keep your operating system and Web browser up-to-date.** Download free software "patches" to close holes in their systems that crooks could exploit. Set them to update automatically, and then set the built-in security and privacy settings higher than the default.
- **If not in use, disconnect.** When not using your computer, disconnect it from the internet altogether so it can't send or receive information and isn't vulnerable to hackers.
- **Use anti-virus and anti-spyware software, plus a firewall.** Anti-virus and anti-spyware software can protect you from inadvertently accepting unwanted or troublesome files, while a firewall blocks unauthorized access to your computer and will alert you if spyware already on your computer is sending information out. Download them individually or as a "suite" from your internet service provider or software companies, or buy them in retail stores.
- **Download software only from websites you know and trust.** Free games, file-sharing programs, and customized toolbars can come with malware. Be cautious!
- **Don't click on links within pop-ups and use a pop-up blocker.** Clicking on links may unknowingly install malware on your computer. Instead, close pop-up windows by clicking on the "X" icon in the title bar. To avoid receiving pop-ups, initiate a pop-up blocker—either through the setting within your browser typically found in the "Options" menu, or through a third party such as an antivirus or security software provider. Pop-up blockers sometimes affect the functionality of certain sites—like Millbury Savings' Online Banking site—and may need to be disabled temporarily to allow certain functions.
- **Don't click on links for free software.** Ads (called scareware) that claim to have scanned your computer and detected problems are a tactic scammers have used to spread malware. Don't click on those messages!
- **Don't reply to requests for sensitive information.** Legitimate companies—including banks like Millbury Savings—don't ask for your personal or financial information via email, and clicking on links in such emails can redirect you to bogus sites. If you are concerned about your account, call the company directly using a telephone number you know is real, or open a new internet browser session and type in the company's correct Web address yourself.
- **Back up your data.** Back up any photos, text files, or data that you'd want to keep in case of a computer crash. Copy them onto a USB drive, a CD or DVD, or an external hard drive, and store it in a safe place.

- **Don't email sensitive information.** Email is not a secure method of transmitting personal or financial information because it can be intercepted.
- **Beware when shopping online.** Look for indicators that a site is secure, like a lock icon on the browser's status bar or a URL that begins with "https:" (the "s" stands for "secure").
- **Protect your passwords.** Keep them secure and out of sight, and don't share them! Make passwords tough for hackers to figure out by using at least eight characters (12 would be even stronger) including numbers or symbols. Avoid using common words or your personal information or login name as your password, and don't use the same password for multiple sites. Change all passwords regularly, and don't enable the feature available in most internet browsers that offers to remember your passwords.
- **Use social media wisely.** People seem to post just about everything on Facebook, Twitter, and other social media sites. But these sites are quickly becoming a treasure trove of personal information. Your birth date, the place you were born, your school's mascot, your mother's maiden name, and other data provide would-be thieves the answers to commonly-used challenge questions on bank and online retail sites. Posting about daily routines or upcoming vacations also leaves you and your home exposed to break-ins. Be careful about what you share and with whom you connect. Use the sites' privacy control features to control who sees your information. Beware of seemingly harmless quizzes designed to harvest your data.
- **Dispose of your old computer safely.** Computers often retain passwords, account numbers, license keys or registration numbers for software programs, addresses and phone numbers, medical and prescription information, tax returns, and other personal documents. Before you dispose of it, do these things first:
    - **Back up important files.** Save them on an external storage device—for example, a USB drive, a CD or DVD, or an external hard drive—or transfer them to a new computer.
    - **"Wipe" your hard drive clean.** Use utility software available online or in stores where computers are sold. They're generally inexpensive; some are available online for free. If your old computer contains sensitive information that would be valuable to an identity thief, consider using a program that overwrites or wipes the hard drive many times. Or, remove the hard drive, and physically destroy it.
    - **Be sensitive about business-related data**. If you use your computer for business purposes, check with your employer about how to manage business-related information on your computer. The law requires businesses to follow data security and disposal requirements for certain customer information.

Beware of Phone and Text Scams

- **Never give out financial data.** Crooks use deceiving methods to pose as banks or credit card companies looking to "verify" your account, debit card, or credit card information. Some use robocalls—autodialed, pre-recorded messages asking customers to confirm their personal banking information by speaking or keying in account numbers or passwords. Caller IDs can be manipulated to look like the call is from your bank or an ambiguous local number when, in fact, it could be originating from somewhere overseas. Remember: No reputable institution, including Millbury Savings, will contact you unexpectedly to verify this kind of information. (However, they may ask you such questions to verify your identity when you initiate the call.) If you receive such a call or text, do not respond. Call your institution directly to report it.
- **Protect your smartphone.** Smartphones allow you to log in to websites, including Online Banking and Mobile Banking sites, or download money management or other apps. That makes your smartphone a target for criminals. At a minimum, be sure to use locking or password features, back up your information, log out of websites, and don't save passwords in your browser. You may want to consider adding tracking software and the ability to "wipe" (erase) data remotely.

Avoid Debit Card Fraud

- **Keep your contact information up-to-date.** Unfortunately, we can't ask you about a suspicious or potentially fraudulent charge unless we can contact you. Don't forget to tell us when your address or phone number changes!

- **Make a copy of the back of your card.** It contains important phone numbers to call if your card is ever lost or stolen, day or night. Be sure to keep the copy in a separate location from your card. Call us at (508) 865-5811 weekdays or 1-800-554-8969 nights and weekends if your debit card is ever lost or stolen.
- **Watch for "skimming."** If the card reader (particularly at an ATM) doesn't look right or looks different than it did before, a skimming device meant to capture your card data and PIN may've been attached. Instead, look for another machine you trust. When entering your PIN at a legitimate machine, cover the keypad with your other hand to block others, or a camera, from seeing which numbers you key in.
- **Save and check all receipts against your statement.** Save your receipts and record each debit card purchase in your checkbook register. Then, open your statement as soon as you receive it and check your receipts and entries against it. Let us know immediately about any charges that are questionable.
- **Don't ignore even small discrepancies.** Many people think scammers are out to make a single "big hit" on a card. The truth is, often times, many small purchases are made first, both to test the validity of the card and with the hope that they'll go unnoticed. Know your balance, track your activity, reconcile your checkbook, and call us at the first sign of suspicious activity, no matter how small.
- **Register for free MasterCard® SecureCode™.** This free service helps to confirm your identity and protect your account against unauthorized online purchases. You choose your own MasterCard SecureCode private code and enter it when you shop at more than 350,000 participating online merchants. To register your Millbury Savings Bank Cash & Check Debit MasterCard and select your code, visit MillburySavings.com/ Personal_Convenience.

Guard Against Other Scams

- **If it's too good to be true...** If you receive unsolicited mail or calls telling you you've won a lottery you never entered—particularly one in another country—or that you stand to inherit part of a fortune just by depositing or cashing checks against your account and wiring the money elsewhere, don't fall for it!
- **Never be pressured into signing anything you don't understand.** If you are unsure about whether to sign a document, have a trusted friend or advisor review it. Get clear, understandable answers to your questions.
- **Beware of "friendly fraud."** Almost 15% of identity theft cases involve so-called friendly fraud, where the fraudster is a friend, relative, co-worker, caregiver, roommate, or some other individual known to the victim. Don't share your personal information if you don't absolutely need to—even with people you trust!
- **Check references and credentials.** Insist on talking to references and viewing the credentials of anyone who wants to enter your home or work for you, including utility workers and town employees.
- **Don't fall for con games.** Don't give your money to anyone who claims to need your help investigating a crime or who claims to have just found a large sum of cash.
- **Verify charities.** Confirm they're legitimate with the Public Charities Division of the Attorney General.

Protect yourself and your money!

For more information, talk to a customer service representative in Millbury at (508) 865-5811 or in Worcester at (508) 757-0057.

Rev. 11.7.14

We're looking out for you.

Millbury Savings Bank

MillburySavings.com