OLD NORTH STATE TRUST, LLC

Defend Against Identity Theft with Common Sense and Skepticism

"Who steals my purse steals trash, "Shakespeare famously wrote. "But he that filches from me my good name . . . makes me poor indeed." Nowadays, savvy thieves can use what they find in your purse or wallet to do exactly that: Steal your good name for their own profit.

Identity theft is a serious problem and is likely to get worse. Thieves are becoming smarter and more ruthless every day and, sadly, they have no qualms about taking advantage of older folks.

Why are older people such prime targets for identity thieves? First, of course, is what the 1930s robber Willie Sutton supposedly said about banks: "That's where the money is." People who have accumulated a lifetime's worth of assets are obviously lucrative targets for crooks. The second reason is that, in a time of rapidly changing technology, older people are perceived as being less knowledgeable about such things as internet security.

But back to Shakespeare: While your purse may not carry much cash anymore, it could still give a thief priceless entrée into your bank and credit accounts, even your investments. One little piece of cardboard, which way too many people carry in their wallets, can be the key that opens your personal bank vault if it falls into the wrong hands.

We're talking, of course, about your Social Security card. We are continually surprised to learn that clients are carrying that card, with that all-important number. Don't do it!

With your Social Security card, plus your birthdate – which will be on the driver's license that's probably in the same wallet – a thief would have access to all kinds of sensitive information. Combine that with the numbers from credit and debit cards, and your identity – and your money – could be stolen in a heartbeat.

An acquaintance told us recently that he had just sent his 20-something son off to begin his first full-time job, and in the process cope with such requirements of adult life as car registration, employee benefits, insurance, and taxes. The father opened a locked file drawer and pulled out the Social Security card that had sat safely in a folder since his son was an infant. He sternly instructed him to carry the card only as long as absolutely required to get himself enrolled with his employer's human resources department, and then immediately tuck it away in his own permanent financial filing system.

That's excellent advice for anybody, at any age.

Even though it says "Not for identification" right on the card, the fact is that Social Security numbers have become essential to modern life. All the more reason to be skeptical about giving your number to just anybody. When a business asks for it, ask them why they need it, who will have access to it, and how it will be kept confidential. If you have to prove your identity, a driver's license or other photo ID is a much safer alternative.

If you still use checks, don't have them imprinted with either your driver's license number or your Social Security number.

A word about credit cards: if a credit card is stolen, federal law limits your potential loss to just $50. But if unauthorized charges are made before the theft is reported, you may find the account has "maxed out," blocking your access to your own credit until the fraudulent transactions are reversed. So it's always a good idea to report a lost or stolen credit card to the issuing bank as soon as possible. If you report the theft before the card is used, your liability is zero.

Debit cards, unfortunately, are a much more serious matter. Because these draw money directly out of your bank account (unlike credit cards, which borrow money from a bank) stolen cash likely is gone forever. But promptly reporting a stolen card limits your liability: To $50 within the first two days, and to $500 if it's within the first sixty days. For similar reasons, it's much safer to use a credit card, not debit, for internet purchases. In fact, keep one card with a low limit for online transactions only in your desk drawer.

Consumers have stronger protections if they lose money because of a stolen card number, as long as the card itself remains safe. These are all good reasons for limiting the number of bank cards you carry. Many of our clients use certain credit accounts only for online commerce, or for large balance transfers, and carry just one or two cards to use for day-to-day purchases.

Whether you carry the card or keep it in a file folder, it's a very good idea to make a copy of the front and the back – including that all-important three-digit security code. Why? Because if you do lose the card, you may not be able to access your account without all the numbers, including expiration date and security code. You won't find that information on your statement. Nowadays it's rare even to have account numbers printed in full.

Those statements are still very important, though. It's always wise to review them as soon as they arrive, either in the mailbox or through your online account. Look for charges you don't recognize, and question them promptly. Fighting fraud is much easier the sooner it's caught.

Shredding unwanted financial documents, including old bank statements and those pesky "pre-approved" credit card offers, helps keep sensitive data out of the wrong hands. Another wise precaution: don't leave your mail, either outgoing or incoming, in an unsecured receptacle.

When it comes to shopping and banking online, or even using an ATM, your password or PIN is your last line of defense. We're constantly warning clients against using obvious, easy-to-guess passwords, or carrying lists of passwords in their wallets. Securing an important account with the likes of "password" or "1234" is the cyber equivalent of hiding your front door key under the welcome mat. It's the first thing a crook will try. (And plenty of crooks won't even have to guess; they use "brute force" computer programs to try literally thousands of likely combinations of letters and numbers when trying to break into your online accounts.)

There are far too many precautions to be able to list them all here. A good reminder to everybody is to be careful about who you trust. Is somebody calling you on the phone, asking you to buy something or make a contribution? Insist on getting something in writing before you provide any information. Did you get a phone call or an email claiming to be from your bank, or the IRS, asking you to "verify" your contact information? Don't believe it. Legitimate entities

never do that. It's a so-called "phishing" scam, designed to trick you into giving up your vital data. And don't click on those internet links in emails, if you aren't absolutely sure they're from a trusted source.

Not sure who to believe, or how to secure your computer or online accounts? Talk to a trusted banker, financial advisor, or tech-savvy relative who can help with cyber-security issues.

To get a "security freeze," preventing identity thieves from applying for credit in your name, and for more tips on fighting identity theft, go to the N.C. Department of Justice website: www.ncdoj.gov.

Old North State Trust, LLC (ONST) periodically produces publications as a service to clients and friends. The information contained in these publications is intended to provide general information about issues related to trust, investment and estate related topics. Readers should be aware that the facts may vary depending upon individual circumstances. The information contained in these publications is intended solely for informational purposes, is proprietary to ONST and is not guaranteed to be accurate, complete or timely.