Keeping Identity Thieves at Bay

The more business you do and information you share online, the more identity theft becomes a growing threat to your financial security. At UBS, we thought it would be helpful for you to know that there are simple steps you can take to help protect your name, your credit and your loved ones from identity thieves.

UBS Financial Services Inc.
40 Congress Street
Portsmouth, NH 03801-6643

Rich DeMarco, Jr
First Vice President - Wealth Management
Portfolio Manager
603-422-8190
richard.demarco@ubs.com

Apryl Cowper
Senior Registered Client Service Associate
603-422-8189
apryl.cowper@ubs.com

Play it safe

Identity theft involves the unauthorized use or attempted use of existing credit cards or accounts, as well as the misuse of personal information to obtain new accounts, get loans or commit other crimes. Roughly 7% of all American households—nearly 9 million homes nationwide—have experienced an incident of identity theft, according to the U.S. Department of Justice.

To help keep your information safe, check monthly statements for credit cards, bank and brokerage accounts carefully, and be sure to get a free annual credit report from one of the three major credit bureaus: Experian, Equifax and TransUnion. Contact each by phone or mail, or go to *https://www.annualcreditreport.com/cra/order?phone*. You should also monitor your e-mail, social networking accounts and phone bills (both cell and landline), as thieves can "piggyback" on your plans.

If you notice something strange when reviewing your credit report or your financial statements—even a charge for just a small amount—call the issuing financial institution immediately and report it. Identity thieves test, or "phish," stolen account numbers by running a small charge or debit, often a dollar or less, to make sure the account number is legitimate. Sometimes, account holders don't notice the transaction or don't think it's worthwhile to alert their financial institution—until later when thieves rack up big purchases

E-mail and phone phishing

E-mail phishing is another common scam. Identity thieves often appear to come from a well-known organization and ask for your personal information—such as a credit card number, Social Security number, account number, user name or password. In order for Internet criminals to successfully obtain your personal information, they will almost always tell you to click a link that either downloads malware or a virus to your computer or takes you to a different site where your personal information is requested. The e-mails often have forged or unsecure links ("http:" in the address rather than ending with an "s" for "secure" in "https"), and express a sense of urgency or negative consequences if you don't take action.

Phone phishing, or telemarketing scams, operate much the same way. Identity thieves call and often use exaggerated or fake prizes or services as bait. These could include travel packages, loans or investment opportunities, and often have an immediate deadline to claim the prize. The goal is to get people to act on impulse and divulge personal or account information rather than take the time to analyze the situation.

Protecting your data

All mail and other documents with account numbers or other personal data should be securely discarded or shredded. One of the best ways to protect yourself from "dumpster diving" and mail fraud is to sign up for e-delivery of all your financial information. To reduce or even eliminate nuisance offers, you can opt out of the lists aggregated by credit bureaus, who then sell your name to lenders. Go to *www.optoutprescreen.com* or call 888-567-8688 to remove your name from these lists.

Also, register your home and mobile phone numbers with the National Do Not Call Registry. This won't stop all unsolicited phone calls, but it will stop most. If your number is on the registry and you still get calls, the caller is likely breaking the law. To add a phone number to the registry, call 888-382-1222 from the phone number you wish to register.

As for your social media accounts, vigilance is key. The more information you share with the world— say, by posting your birth date to your Facebook profile—the easier you are making it for thieves to find that information. Check your privacy controls, and keep checking as they change often. Also check the information your children are sharing online and the configuration of any file sharing software they've installed. They are less likely to be aware of privacy concerns and the consequences of divulgeing sensitive information. Finally, you should Google yourself periodically to see what type of information about you or your family is publicly available.

We can help

If you haven't signed up for eDelivery of your UBS statements, online bill pay through UBS Online Services (*ubs.com/fs*), or other services that may help protect you, let us know. We have relationships with several identity theft companies and may be able to refer you at a discount. If you have questions about other identity theft protections, please don't hesitate to contact us.

ubs.com/fa/richarddemarco