



Account Take-Over Fraud

Identity theft related to financial fraud is a top concern for banking customers and banking institutions in all parts of the world including St. Paul. In fact, identity theft is the fastest growing type of fraud in the United States, the United Kingdom, and many other developed countries.

Account takeover fraud is one of the two basic forms of financial identity theft (the other being application fraud), and it occurs when a fraudster obtains and uses a victim's personal information to take control of existing bank or credit card accounts and carries out unauthorized transactions against them. Application fraud occurs when a perpetrator uses someone else's personal information to establish new accounts.

Fraudsters employ a variety of techniques to obtain the personal and financial information typically needed to take control of existing accounts. Obtaining such information can be as simple as dumpster diving or cold calling. Alternatively, fraudsters may use more technology-reliant methods, such as phishing, SMiShing, or establishing fake websites to collect payment details.

See [Scam Alert](#) page on Website for information on “smishing” and “phishing”

The following list provides some useful methods to protect against identity fraud:

- Always check bank and credit card statements for inaccuracies.
- Check your financial information regularly, looking for what should and should not be there.
- Order and check your credit report at least once a year.

- Before providing personal information, make sure the individual or business requesting it has a valid reason for requiring the information.
- Never write your credit card numbers or Social Security number on checks or on the outside of envelopes.
- Do not put your Social Security number on any document unless you are legally required to do so.
- Do not give account numbers over the telephone or to persons/companies you are not familiar with.
- Do not use cordless or cellular telephones or e-mail to transmit financial or private personal information.
- Keep all financial documents in a secure place.
- Purchase a shredder, and use it!
- If you have your driver's license information pre-printed on your checks, shred canceled checks before discarding them.
- Shred pre-approved credit applications, statements, or bills that contain personal information.
- Shred any papers with financial information and identifiers rather than simply throwing them in the trash.
- Have yourself taken off "pre-screened lists."
- Mail bills from the post office or your business.
- Consider having your name, telephone number, and/or address removed from the telephone directory.
- Do not provide personal information over the telephone unless you initiated the call and know who you are speaking with.
- If telemarketing companies call, tell them: "Under the federal Telephone Consumer Protection Act, I want to be on your 'do not call' list."
- Keep your birth certificate in a safe place.
- Make sure your computer security (spam filters, virus protection, firewall, passwords, etc.) is robust and up-to-date.
- Choose passwords that will be difficult to crack and use different passwords for all accounts.
- Change passwords and PIN codes often.
- Use different PIN numbers for all of your cards.
- Do not store your PIN numbers on mobile phones or laptops.

Excerpted from Mark Scott, J.D.

© 2009 The Association of Certified Fraud Examiners, All Rights Reserved.