

Identity Theft

How To Prevent It

Frank McKinley

In 2004 there were a total of 9.3 million victims that suffered losses of more than \$52 billion.

Of those 9.3 million victims, half were perpetrated by the victims' friends, family, and neighbors – those around us that have easy access to our information.

Maybe you know someone this happened to or maybe it happened to you.

So what are your friends and families looking for, what do they use to steal your identity? Your credit cards, ID cards, receipts, statements of all sorts, your addresses, and your PIN numbers.

What do they do with it? The most popular thing is to open a credit card in your name and rack it up without your knowledge.

Some will drain your bank account. Others will use your ID or make a new one in order to get a job. And here's an interesting fact you mightn't have considered: 16% of all fraud complaints mention new phone accounts.

While we've come to rely on electronic data and communication more than we did, say, 10 years ago, the ID thief's methodology is still rather low-tech. Most of us think that identity theft is the result of some genius cyber crime.

The truth is, only 12% of the information used to commit identity theft is found online, and 68% is found offline.

Where's offline? Nearly one-third of the information is stolen from your wallet. Other sources are your garbage, mail stolen from

your mailbox, looking over your shoulder at the ATM.

Again, only 12% is online, so it's important to keep your purses, wallets, and paper copies of financial files safe.

One of the most popular and tricky methods is Phishing. This happens to all of us. Some of us may have unwittingly clicked on one of these emails before, and it's too late when we become suspicious.

Phishing is the act of sending email, posing as another business (EBay is a really common one), in order to get you to update your credit card or social security number.

Be wary of emails from phishers, and if a message looks suspicious, go directly to the web site of the legitimate company.

There, you most often find contact information in case you get phished, how a legitimate email would appear in your email, etc.

In addition to keeping a close eye on your inbox, there are a few things you can do to protect your computer and electronic information.

Shield your PC and wireless router with firewalls and software to catch viruses and spyware; turn on automatic software updates.

Create tough-to-crack passwords, change them often, and don't let financial programs or Web sites autosave them.

Ignore emails urging you to click on a link to verify account information. These are sent by phishers, not by banks or brokers.



Contact me for more details:

Phone
973-515-5184

Email
frank@franklyfinancial.com

Web
www.FranklyFinancial.com

Connect to your account only from your own PC; never connect from a public hot spot where eavesdroppers may lurk.

Avoid unknown sites offering free music and game downloads; hackers often plant spyware and viruses there.

Check out investor alerts on the NASD and SEC websites for information that might affect one of your accounts.

Taking these steps can help to ensure the security of, not only your mutual fund portfolio, but also your bank accounts, credit cards, utilities, and any business that you deal with online.

Identity Theft

What To Do If Victimized

In the event that you do become a victim of identity theft, here's what you should do:

- Close all financial accounts immediately
- Contact the three major credit bureaus (Equifax, Experian, TransUnion) to place a fraud alert on your credit report
- Replace ID cards, drivers licenses, passports
- File a report with local law enforcement
- File a complaint with the Federal Trade Commission
- Create new passwords for your new accounts

These are just the initial steps, and with any luck your problems will come to quick resolution.

The biggest downfall of being an Identity Theft victim is the time committed to cleaning up the mess and getting your credit back in good standing.

To recap some common preventative measures:

Order annual credit reports and review them thoroughly.

Do not carry your Social Security Cards or your PINs and passwords with you.

Use a secure outgoing mailbox for important mail, rather than your home mailbox.

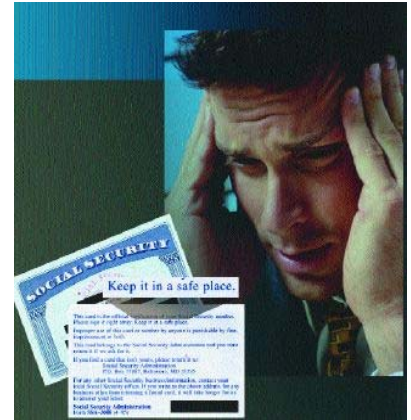
Retrieve your paper mail promptly.

Shred copies of credit applications, insurance forms, physician statements, checks and bank statements, and credit offers.

Don't give your personal information, Social Security or account numbers over the phone *unless you have initiated* the transaction with a direct call into the company regarding your account.

NEVER give out secure information via email.

Keep your security software up to date and run frequent anti-virus anti-spyware scans.



For more information on precautions to take, as well as steps to take in the event of theft, you may visit these web sites.

**Federal Trade
Commission**

www.consumer.gov

**Social Security
Administration**

[www.ssa.gov/pubs/
idtheft.htm](http://www.ssa.gov/pubs/idtheft.htm)

**US Department
of Justice**

[www.usdoj.gov/criminal/
fraud/idtheft.html](http://www.usdoj.gov/criminal/fraud/idtheft.html)



Frank McKinley is a
Registered Rep with
Cadaret, Grant & Co., Inc.,
Member NASD/SIPC

His Supervisory Office of
Jurisdiction is at 45 Morgan
Dr., Wantage, NJ 07461
973-875-5052