

## Identity Theft Preventive Tips from Valley Bell CU

How Your Identity Is Stolen	How to Protect Yourself
<p><b>“Phishing” (pronounced “fishing”)</b> You may <b>receive an e-mail</b> that appears to be from a company you know or it may state it is from a government agency. There will always be a <b>request for immediate action regarding your account</b> and it will encourage you to “click” on a button to go to the company website or it will provide a toll-free telephone number for you to call. If you “click” the button, it may appear to go to the company’s website or it can go to the company website but a pop-up window may appear. In either case, there will be a request to update personal information or a request to verify password or other account information.</p>	<p><b>Do Not “click” or Do Not call the toll-free number.</b> Reputable companies do not ask for this type of information unless you contact them; they will only request such information to verify your identity. <b>Ignore unsolicited requests for personal information.</b> If you need to contact the company, use a telephone number found on your statement or in the phonebook.</p>
<p><b>Identity thieves steal purses and wallets</b> that usually contain driver’s license, credit card, Social Security card and other personal information.</p>	<p><b>Keep your purse or wallet secured.</b> Do not carry your Social Security card and carry only the identification, credit cards, or ATM/debit cards you need.</p>
<p><b>Identity thieves steal mail</b> from unsecured roadside mailboxes that contain bank account statements, credit card statements, personal checks, or tax information. They steal outbound mail from these same mailboxes that may contain credit card or other payments; one bill payment will have account number information and your checking account information.</p>	<p><b>Take your outgoing mail to a secure post office mailbox</b> and remove mail from your home mailbox as soon as possible. If you are going to be away for a few days, do not have your mail delivered; it is a sign to thieves of all kinds that your home is vacant. Contact the <b>U.S. Postal Service at 800-275-8777</b> or online at <a href="http://www.usps.gov">www.usps.gov</a> and request that they hold your mail until you return.</p>
<p><b>“Dumpster Diving”</b> – Discarded expired credit cards, credit card or bank statements, pre-approved offers of credit, deposit receipts, credit card receipts, ATM/debit card receipts, and insurance forms are just a few items that can be found in everyday trash that contain personal information and identity thieves know this. They also know that some businesses are careless with how they dispose of your personal information.</p>	<p><b>Shred these documents thoroughly</b> before placing in the trash. When a company collects your personal information, <b>it is your right to know how they will protect and store your information as well as how they will destroy the information when they no longer need it, so do not be afraid to ask.</b></p>
<p><b>The National Crime Prevention Council</b> reports that someone the victims know commits 50% of identity theft crimes.</p>	<p><b>Store your personal information in a secure place,</b> especially if you have roommates, visitors, employ outside help, or if you are having work done on your house. Share your personal information with family members only when necessary.</p>
<p><b>Theft of personal information at work</b> is a growing trend.</p>	<p><b>Ask your employer</b> if there is a policy to protect your personal information and who has access to it. Keep your purse or wallet in a secured place.</p>
<p><b>Personal Identification Numbers (PIN) and Passwords</b></p>	<ul style="list-style-type: none"> <li>• <b>Do not use</b> birth dates, Social Security numbers, favorites sports teams, name of pets, children’s names or other such information.</li> <li>• <b>Do not write your PIN</b> or account password on your ATM/debit card or checkbook.</li> <li>• <b>For passwords,</b> use a combination of numbers and letters; use small caps and large caps randomly.</li> </ul>
<p><b>Members of the Armed Services</b></p>	<p>If you are being deployed from your normal duty station, place an <b>“Active Duty Alert” in your credit file.</b> Creditors must verify your identity before granting any credit; this will help prevent anyone from using your personal information to obtain credit while you are away. The alert is <b>good for one year.</b> It can be renewed by anyone for you.</p>

**Be Alert to Signs that Indicate Your Identity Has Been Stolen**

- **Bills do not arrive as normal** – Identity thieves may have changed the mailing address with these companies and obtained new credit cards.
- **You receive unexpected credit card statements** or other similar items. Identity thieves have opened accounts with your personal information.
- **You receive denials of credit** when you did not apply.
- **You cannot identify transactions** on your account when reviewing your bank statement.

**What to Do if You Suspect or if Your Personal Information Has Been Stolen**

Place a “**Fraud Alert**” in your credit file by contacting any one of the three major credit bureaus:

- **Equifax:** 1-800-525-6285 or [www.equifax.com](http://www.equifax.com)
- **Experian:** 1-888-EXPERIAN (1-888-397-3742) or [www.experian.com](http://www.experian.com)
- **TransUnion:** 1-800-680-7289 or [www.transunion.com](http://www.transunion.com)
- **Order a copy of your credit report** and review your file. **Verify your personal information** such as Social Security number, address and employer. **If any of it is incorrect**, get it removed. The credit bureaus have forms and procedures for doing this.
- **Look for creditors reporting accounts that you did not open** or credit inquires you know you did not initiate.
- **Close the accounts that have been tampered with or opened fraudulently.** **Contact the fraud or security department** of each company to find out their procedures for reporting the fraud. Take notes of the conversation such as whom you spoke with, time and date. Do not end the call until you have all your questions answered or you fully understand what to do. Always **follow-up with a written notification** and **do this immediately** as the company must have this notice within 60 days of when they first sent the bill to you. **Send good photocopies** of the documents they request keeping the **originals for your file.**

A **Fraud Alert** can help prevent identity thieves from opening more accounts in your name. When the alert is in your credit report, a business has to verify your identity before they grant credit; this means they may need to talk to you first. **There are two types of Fraud Alerts:**

- 1) **Initial Alert** – Stays on in your credit file **for 90 days.** Use this when you suspect your identity has been stolen or if your purse, wallet or other critical documents have been lost or stolen. You are entitled to one free credit report from each of the three credit reporting agencies.
- 2) **Extended Alert** – Stays in your credit file **for seven years.** Use this when you are a victim identity theft and can provide a copy of an official Identity Theft Report filed with any of the law enforcement agencies. You are entitled to two free credit reports within the first 12 months from each of the three credit reporting agencies.

You will be required to prove your identity, so have your personal information available you when you contact a credit bureau.

**File a report with the local police**

Be sure to get a copy of the report – you will need it to help prove identity theft. If the police are reluctant to take the report, try the state police or the Attorney General’s office.

**Report the crime to the Federal Trade Commission (FTC)**

[www.consumer.org/idtheft](http://www.consumer.org/idtheft)

**Identity Theft Hotline at 1-877-IDTHEFT (877-438-4338)**

The FTC can refer your complaint to other government agencies for further action. Always contact them when you have information to update.

**If your driver’s license or Social Security card is lost or stolen**

Contact the local offices to alert them of the loss and for instructions.

**Contact all the companies in which you have credit or other accounts**

Alert them of the problem even though accounts may not be affected by the identity theft. **Find out their procedures** to protect you in the event the identity thieves attempt to commit fraud at these places. **Most companies will probably close all your accounts and re-open new ones with new account numbers and new passwords.**