FINANCIAL SCHEMES

Debit Cards

Despite the convenience and popularity of debit cards, there is a risk of fraud. It is important to protect your debit card, just as you would cash, credit cards and checks/. Some of the risks associated with debit card fraud are the same as credit cards, so protect your account numbers in your wallet, online and over the phone. However, there is another threat to debit card users that is unique-and it is called “skimming.”

Fortunately, there are steps you can take to protect yourself from skimming and other forms of fraud. In addition, it is important for you to know that if you are the victim of debit card fraud, your bank will protect you. The Electronic Funds Transfer Act (EFTA) protects consumers from losses due to debit card fraud artists if you report fraud in a timely fashion. Visa and MasterCard have taken the protection a step further for all debit cards that bear their logos, by instituting a zero liability policy. This policy states that consumers will not have to pay from any purchases made fraudulently using Visa and MasterCard debit cards, regardless of the time it takes to report the incident.

Make sure you are vigilant when protecting your wallet, cash as well as credit and debit cards. If you do notice something suspicious, report it to your bank immediately, whether it’s a possible skimming device or an unauthorized charge on your statement.

Consumer Tips:

- Check your bank statements immediately. Make sure all payments are yours
- Periodically check your account balance and transactions, by utilizing online banking, by telephone, or by printing interim statements at the ATM.
- Contact your bank immediately if your card is lost, stolen or subject to fraudulent use.
- Keep a record of card numbers, PINS, expiration dates and 1-800 numbers for banks so you can contact the issuing bank easily in cases of theft.
- Memorize your PIN number. Do not use your birth date, address, phone number or social security number. Never store your PIN with your card, and do not make it available to others.
- Keep your receipts. You’ll need them to check your statement. If they have your account number on them, tear up or shred receipts before throwing them away
- Mark through any blank spaces on debit slips, including the tip line at restaurants, so the total amount cannot be changed.
- Know your limits. Many issuers limit daily purchases and withdrawals for your protection.
- Do not use an ATM if it looks suspicious, it could be a skimming device
- Be wary of those trying to help you. Especially when an ATM “eats” your card, they may be trying to steal your card number and PIN.
- Do not give your PIN number to anyone over the phone, often thieves steal the cards and then call the victim for their PIN, sometimes claiming to be law enforcement or the issuing bank.

Phishing

Con artist now use email to try to hijack your personal financial information. In a scam known as "phishing," swindlers claim to be from a reputable company and send out thousands of fake emails in hopes that consumers will respond with the bank account information, credit card numbers, passwords or other sensitive information.

These emails can look quite convincing, with company logos and banners copied from actual Web sites. Often, they will tell you that their security procedure has changed or that they need to update (or validate) your information, and then direct you to a look-alike Web site. If you respond, the thieves use your information to order goods and services or obtain credit.

When the IRS learns about schemes involving use of the IRS name, it tries to alert consumers as well as authorities that can shut down the scheme, if possible. The most recent schemes are:

- A new variation of the refund scheme is directed toward organizations that distribute funds to other organizations or individuals. In an attempt to seem legitimate, the scam e-mail claims to be sent by, and contains the name and supposed signature of, the Director of the IRS Exempt Organizations area of the IRS
- In a variation, an e-mail scam claims to come from the IRS and the Taxpayer Advocate Service. The e-mail says that the recipient is eligible for a tax refund and directs the recipient to click on a link that leads to a fake IRS Web site.
- A scam e-mail that appears to be a solicitation from the IRS and the U.S. government for charitable contributions to victims of the recent Southern California wildfires has been making the rounds.
- A recent e-mail scam tells taxpayers that the IRS has calculated their "fiscal activity" and that they are eligible to receive a tax refund of a certain amount.
- In a news phishing scam, an e-mail purporting to come from the IRS advises taxpayers they can receive $80 by filling out an online customer satisfaction survey.
- In another scam, consumers have received a "Tax Avoidance Investigation" e-mail claiming to come from the IRS "Fraud Department" for which the recipient is asked to complete an "investigation form," for which there is a link contained in the e-mail, because of possible fraud that the recipient committed. It is believed that clicking on the link may activate a Trojan Horse.
- An e-mail scheme claiming from the IRS's Criminal Investigation division tells the recipient that they are under a criminal probe for submitting a false tax return to the California Franchise Board. The e-mail seeks to entice people to click on a link or open an attachment to learn more information about the complaint against them.

Consumer Tips:

- Never give out your personal financial information in response to an *unsolicited* phone call, fax or email, no matter how official it may seem.

- Do not respond to email that may warn of dire consequences unless you validate you information immediately. Contact the company to confirm the email's validity using a telephone number or Web address you know to be genuine.
- Check your credit card and bank account statements regularly and look for unauthorized transactions, even small ones. Some thieves hope small transactions will go unnoticed. Report discrepancies immediately.
- When submitting financial information online, look for the padlock or key icon at the bottom of your Internet browser. Also, many secure Internet addresses, though not all, us "https" to signify that your information is secure during transmission.
- Report suspicious activity to the Internet Crime Complaint Center, a partnership between the FBI and the National White Collar Crime Center.
- If you have responded to an email, contact your bank immediately so they can protect your account and your identity.

Affinity Fraud

Affinity fraud refers to investment scams that prey upon members of identifiable groups, including religious, elderly, ethnic, and professional groups. The fraudsters who promote affinity scams are group members, claim to be members of the group, or enlist respected leaders within a group to spread the word about an investment deal. In addition, fraudsters are increasingly using the Internet to target groups with email spams. These scams exploit the trust and friendship that exist in groups of people who have something in common. Because of the tight-knit structure of many groups, it is usually more difficult for regulators or law enforcement officials to detect an affinity scam. Victims of such scams often fail to notify authorities or pursue their legal remedies, but are more likely to try to work things out within the group.

Many affinity scams involve "Ponzi" or pyramid schemes where new investor money is used to make payments to earlier investors to give the false illusion that the investment is successful.

This ploy is used to induce or "trick" new investors to invest in the scheme and to lull existing investors into believing their investments are safe and secure. In reality, the fraudster amost always steals investor money for personal use. Both types of schemes depend on an unending supply of new investors – when the inevitable occurs, and the supply of investors dries up, the whole scheme collapses and investors lose most, if not all, of their money

The Bureau of Consumer Protection under the Federal Trade Commission works to protect consumers against unfair, deceptive, pr fraudulent practices in the marketplace. The Bureau conducts investigations, sues companies and people who violate the law, develops rules to protect consumers, and educates consumers and businesses about their rights and responsibilities.

How To Avoid Being a Victim in an Affinity Fraud

Making investment decisions can be risky. You can minimize the risk by asking questions and demanding the facts about any investment. To avoid affinity and other scams, you should:

- Check out everything – no matter how trustworthy the person is who brings the investment opportunity to your attention. Never make an investment based solely on the recommendation of a member of an organization, or religious or ethnic group to which you belong. Investigate the investment thoroughly and check the truth of every statement you are told about the investment. Be aware that the person telling you about the investment may have been fooled into believing that the investment is legitimate when it is not.

- Do not fall for investments that promise spectacular profits or "guaranteed" returns. If an investment seems too good to be true, then it probably is. Similarly, be extremely leery of any investment that is represented to have no risks; very few investments are risk-free. Generally, the greater the potential return an investment offers, the greater the risks of losing money on the investment.

- Be skeptical of any investment that is not fully documented in writing. Fraudsters often avoid putting things in writing, but legitimate investments are usually in writing. Avoid an investment if you are told they do "not have the time to reduce to writing" the particulars about the investment. You should also be suspicious if you are told to keep the investment opportunity confidential.

- Don't be pressured or rushed into buying an investment before you have a chance to think about – or investigate – the "opportunity." Just because someone you know made money, or claims to have made money, doesn't mean you will too. Also, watch out for investments that are pitched as "once-in-a-lifetime" opportunities, especially when the promoter bases the recommendation on "inside" or confidential information.

The Securities and Exchange Commission actively investigate investment scams that prey on members of affinity groups and has taken quick action to stop such scams. If you believe you are a victim of affinity fraud or are aware of any affinity scam, you should contact the Securities Exchange Commission Complaint Center, your state's securities administrator at http://www.sec.gov/investor/pubs/affinity.htm

The executive director for the Utah Department of Commerce announced that the Division of Securities has released a top ten list of investment scams predicted for 2008. The list details fraudulent activity tracked by the Division of Securities over the past year and offers predictions on which investment schemes to watch for in 2008.

Utah Division of Securities Top Ten Investment Scam Predictions for 2008

1. Real Estate Notes
2. "Secret" Homeland Security Projects

3. Hedge Funds Run by Unlicensed or Unqualified Advisors
4. Hedge Funds Run by Unlicensed or Unqualified Advisors
5. Unsuitable options Trading Programs
6. Letter of Credit Schemes and Advance Fee Schemes
7. Free Meal Sales Seminars advertised ad “Educational”
8. Fake Internet Sites that Solicit Investments
9. Oil and Gas, Mining Schemes
10. “Phishing” for Information on Internet Stock Trading Accounts
11. Not Realizing that 36% Interest is “Too Good to be True”