

Union Bank

(from You Can Prevent Fraud)

putes. Be aware that having "no complaints" against a seller is no guarantee of legitimacy. Fraudulent operators open and close quickly, so the fact that no one has made a complaint yet doesn't mean that the seller or charity is legitimate. You still need to look for other danger signs of fraud.

Don't believe promises of easy money. If someone claims that you can earn money with little or no work, get a loan or credit card even if you have bad credit, or make money on an investment with little or no risk, it's probably a scam.

Understand the offer. A legitimate seller will give you all the details about the products or services, the total price, the delivery time, the refund and cancellation policies, and the terms of any warranty.

(For more information about shopping safely online, go to www.nclnet.org/shoppingonline.)

Resist pressure. Legitimate companies and charities will be happy to give you time to make a decision. It's probably a scam if they demand that you act immediately or won't take "No" for an answer.

Be cautious about unsolicited emails. If you are familiar with the company or charity that sent you the email and you don't want to receive further messages, send a reply asking to be removed from the email list. However, responding to unknown senders may simply verify that yours is a "working" email address and result in even more unwanted messages from strangers. The best approach may simply be to delete the email.

Beware of imposters. Someone might send you an email pretending to be connected with a business or charity, or create a Web site that looks just like that of a well-known company or charitable organization. If you're not sure that you're dealing with the real thing, find another way to contact and ask the legitimate business or charity.

Guard your personal information. Don't provide your credit card or bank account number unless you are actually paying for something. Your social security number should not be necessary unless you are applying for credit. **Be especially suspicious if someone**

claiming to be from a company with whom you have an account asks for information that the business already has.

Beware of "dangerous downloads." In downloading programs to see pictures, hear music, play games, etc., you could download a virus that wipes out computer files or connects your modem to a foreign telephone number, resulting in expensive phone charges. Only download programs from Web sites you trust. Read all user agreements carefully.

Pay the safest way. Credit cards are the safest way to pay for online purchases because you can dispute the charges if you never get the goods or services or the offer was misrepresented. Federal law limits your liability to \$50 if someone makes unauthorized charges to your account, and most credit card issuers will remove them completely if you report the problem promptly. There are new technologies, such as "substitute" credit card numbers and password programs, that can offer extra measures of protection from someone else using your credit card.

IDENTITY THEFT: If you believe that someone is using your identity illegally, report the crime to a law enforcement agency. Making an official "identity theft report" can help you solve problems resulting from the ID theft. The "identity theft report" is a document that subjects the person filing it to criminal penalties for providing false information. (This discourages people from filing phony reports to try to avoid paying legitimate debts.) When a financial account is involved, contact the bank immediately. If your credit card, debit card, ATM card, or checks have been lost or stolen, or if you suspect that someone has obtained your account number for fraudulent purposes, inform the financial institution promptly and ask what you need to do to protect your money.

Know your payment rights. Your bank has specific information about the terms of your account. Your responsibilities for fraud are specifically outlined in your terms, and are a reflection of bank policy and federal laws. At Union Bank, you will have been advised of your terms at the time you opened your account. If you have any questions about your Union Bank account, please contact us at your convenience.

Respond quickly to debt collectors. If debt collectors contact you about accounts opened in your name or unauthorized charges made to your existing accounts, respond immediately in writing, keeping a copy of your letter. Explain why you don't owe the money and enclose copies of any supporting documents, such as an official identity theft report. You have the right to ask that business for copies of the credit applications or other documents relating to any transactions that you believe were made by the ID thief. Contact one of the three major credit bureaus to place a fraud alert; it will be shared automatically with the other two: Equifax, 800.525.6285, TDD 800.255.0056, www.equifax.com; Experian, 888.397.3742, TDD 800.972.0322, www.experian.com; TransUnion, 800.680.7289, TDD 877.553.7803, www.transunion.com.

Avoid being "phished" for your card numbers and personal data from email requests. No reputable Merchant or Company will ask you for this information via email or telephone. If you have a question, call the company you are dealing with BEFORE you offer your information, or call us at (802) 888-6600 or 1-866-862-1891.

Avoid schemes that are "too good to be true." There is no such thing as a free lunch. If something seems unlikely, such as you "won" a large amount of money but have to submit a "service fee" to receive it, it's a scam and should be promptly reported to law enforcement.

Avoid the potential for skimming devices, which can be illegally attached to ATM structures. Also, make certain if you hand your card to a retail attendant, that it is being used ONLY for your purchase and not being "double swiped" for ANY reason.

Your card is like cash in a wallet. Make sure you have it a safe place when not in use and in a secure place on your person when with you.

You'll find many more links to organizations and government agencies who are united against fraud on our website: <http://www.unionbankvt.com/UBSecurity.html>

Union Bank
1.866.862.1891 www.unionbankvt.com Member FDIC

UB100306 ANTI FRAUD - 02.2008

Defeating Fraud



Union Bank
1.866.862.1891 www.unionbankvt.com Member FDIC

If it seems too good to be true, it's probably a scam in progress!

Fraud is on the rise. Due to technical advances in communication, the way criminals attempt to deceive you has become increasingly sophisticated. **At Union Bank, we want you, your identity, and money to remain out of the reach of criminals.**

Mass Marketing Fraud

Mass Marketing Fraud is a **general term** for fraud that exploits mass-marketing media, such as telemarketing fraud, Internet fraud and identity theft. Advanced electronic communications, along with modern payment systems such as credit and debit cards have created a substantial increase in fraud. Illegal mass marketers use **three primary methods** to choose potential victims. First, they attempt to contact individuals with whom they have had no prior relationship and attempt a scam. Second, they prompt perspective victims to contact their own organization by sending messages that “guarantee” rewards or other benefits. Third, they purchase lists of prior individuals known to have been victims of previous scams...individuals the crooks believe will be receptive to investing in “lottery”, “rich relatives” and other pathetic, but successful hoaxes.

Advanced Fee Fraud

In these scams, victims are told they have won a lottery, received an inheritance or are otherwise entitled to some miraculous sum of money. Victims are informed, that in order to receive the “money to which they are entitled” they must first send funds to cover taxes or processing fees.

Foreign Lottery Fraud

In a Foreign Lottery Fraud, victims are notified that he or she has won the prize, but first must pay “various taxes and fees” before being able to claim the money. The criminals, posing as “lottery agents” often send counterfeit checks representing all or a portion of the fake winnings and require that the victim return money back to cover the fraudulent taxes and fees. **REMEMBER:** If you play a foreign lottery — through the mail or over the telephone — you’re violating U.S. federal law.

Overpayment Fraud (Forged Checks)

Overpayment fraud often occurs when a person advertises an item for sale, either in print or online. The seller is contacted by the criminal acting as an interested purchaser. The criminal then sends a counterfeit check to the seller for an amount greater than the asking price of the item and asks the seller to deposit the check and return the balance to another person posing as a shipper or agent, working for the criminal.

The Mystery Shopper

Victims respond to an ad looking for a “mystery shopper” or a secret shopper. When they contact the company about the position, they are told they can earn money by purchasing items at different stores or dining at different restaurants. The company then sends an “employment packet.” The packet includes business evaluation forms, a training assignment, and a cashier’s check, often ranging between \$2,000 and \$4,000. The training assignment is to cash the check, pose as a customer, and wire the money to the fraudster’s address. **The check is counterfeit.** The check fraud is exposed after the victim wires the money, leaving the victim liable for the fake check.

The Jury Scam

The phone rings, you pick it up, and the caller identifies himself as an officer of the court. He says you failed to report for jury duty and that a warrant is out for your arrest. You say you never received a notice. To clear it up, the caller says he’ll need some information for “verification purposes”—your birth date, social security number, maybe even a credit card number. This is when you should hang up the phone. It’s a scam.

Phishing

Phishing is the act of attempting to fraudulently acquire sensitive information, such as passwords and credit card/debit card details, by masquerading as a trustworthy person or business with a real need for such information in a seemingly official electronic notification or message (most often an email, or an instant message). It is a form of **social engineering** attack. Perpetrators ask the victim to reveal his or her password, under the guise of “verify your account” or to “confirm billing information”. Once the victim sent their password, the attacker could access the victim’s

account and use it for criminal purposes. Phishing has been widely used by criminals who create email messages masquerading as large banks, eBay® or even PayPal®. **These fraudsters can copy the code and graphics from legitimate websites and use them on their own sites to create fake web pages that appear legitimate.** They can also link to the graphics on the legitimate sites to use on their own scam site. These pages are so well done that most people can’t tell that they have navigated to a scam site. Fraudsters will also put the text of a link to a legitimate site in an e-mail but manipulate the source code to links to their own fake site. This can be revealed by using the “**view source**” feature in the e-mail or browser application to view the destination of the link or by putting the cursor over the link and looking at the code in the “status bar” of your web browser.

Auction and Retail Schemes Online

Fraudsters launch online auctions on eBay® or Craig’s List® with a low price and no reserve, mostly for high priced items: watches, computers or high value collectibles. They take payment then don’t ship, or they deliver an item that is less valuable than the one offered, such as one that is counterfeit, refurbished, or used. Some fraudsters also create complete webstores that appear to be legitimate, but never make good on the transaction. In some cases, some stores or auctioneers are legitimate and from one day to the next, they stop shipping (after cashing customers’ payments).

Stolen credit cards

Most Internet fraud is done through the use of stolen credit card information which is obtained in many ways, the simplest being copying information from retailers, or directly asking customers for the information while posing as a legitimate business. There have been many examples of thieves posing as eBay® or PayPal®, and attempting to solicit financial and identity info.

Purchase Scams

The most straightforward type of purchase scam features a buyer in another country approaching many merchants (through email spamming) and then directly asking them if they can ship to them while using credit cards (often stolen) to pay.

An example of such email is as follows:

From: XXXXXX XXXXXX [XXXXXXX@XXXXXX.com] Sent: Saturday, October

01, 2008 11:35 AM Subject: International order enquiry

Gooday Sales, This is XXXXXX XXXXXXX and I will like to place an order for some products in your store, But before I proceed with listing my requirements, I will like to know if you accept credit card and can ship internationally to XXXXXX XXXXXXX. Could you get back to me with your website so as to forward you the list of my requirements as soon as possible. Regards, XXXXXX XXXXXX, XXXXXXXX Inc. 9999 XXXXXX street, XXXXXX XXXXXXX Telephone: 234-1-99999999, Fax: 234-1-9999999, Email: XXXXXXXXXX@XXXXXX.com

Most likely, a few weeks or months after the merchant ships and charges the credit card, he/she will be **hit with a chargeback from the credit card processor and lose the value of the goods plus the shipping.**

Counterfeit Postal Money Orders, Traveler’s Checks and fake “official” documents.

According to the FBI and postal inspectors, there has been a massive increase in the use of counterfeit official documents. The “quality” of these counterfeit documents is so good that consumers are easily fooled. Counterfeit documents run the gamut from fake cash to fake Money Orders to fake Traveler’s Checks to fake Treasurer’s checks using legitimate bank logos. The simple questions recipients of these counterfeit items need to ask themselves are: “what is the source?” and “**is this too good to be true?**” These two simple filters will save you a world of financial woes that are created when you attempt to cash or process a counterfeit document.

You Can Protect Yourself

Know who you’re dealing with. If the person or business you are considering a transaction with is unfamiliar, check with your state or local consumer protection agency and Better Business Bureau. Some Web sites have feedback forums, which can provide useful information about experiences with particular sellers. Get a physical address and phone number in case there is a problem later.

Look for information about how complaints are handled. It can be difficult to resolve complaints, especially if the seller or charity is located in another country. Look for information about programs the company or organization participates in that require it to meet standards for reliability and help to handle dis-

(continued on following panel)