

## Consumer Warning: 12 Scams to Watch Out for This Holiday Season

Updated: Thursday, 09 Dec 2010, 3:47 PM CST  
Published : Thursday, 09 Dec 2010, 3:29 PM CST

FOX Chicago News

Chicago - Consumer fraud is rampant during the holidays. Professor Fraud, aka Bill Kresse, of St. Xavier University's Center for the Study of Fraud and Corruption, made a list of 12 common consumer frauds that Chicagoans should be aware of while out and about this holiday season.

### 1) Pickpockets and ID Theft

It's the Holidays, and that means Holiday shopping! The streets and the malls will be filled with fellow festive shoppers, along with pickpockets and purse-snatchers.

Now-a-days, these thieves aren't just out to steal your cash, they're out to steal your identity, too. A study by the Saint Xavier University Center for the Study of Fraud and Corruption showed that the second greatest source of stolen identities was stolen purses and wallets.

So this season, while you're shopping, be constantly aware of your purse or wallet. If you can, carry your purse or wallet inside your coat or jacket, and never, ever, carry your Social Security card in your wallet!

### 2) House Parties and ID Theft

It's that time of the year when folks of good cheer open up their houses for holiday parties. If you're hosting a Holiday house party, here's something you should remember: a study by the Saint Xavier University Center for the Study of Fraud and Corruption showed that a majority of identity thefts can be traced back to a friend or relative of the victim – just the sort of folks you'll be inviting into your home!

So if you'll be hosting a Holiday house party, be sure to lock up your valuables, including potential identity theft items such as credit cards, checkbooks, social security cards, even bank statements and tax returns. You want your guests leaving with a warm Holiday glow, not your identity.

### 3) Counterfeit Goods

"Psst, hey, buddy, how about a designer purse for one-tenth the prices?"  
"For real?"

Of course not. It's just another transaction in the multi-billion dollar market in fraudulent counterfeit goods. But what's the harm?

Well, some counterfeit goods have been tied to international organized crime and terrorist groups. Besides that, counterfeit goods are generally low quality. Fraudulent software and peripherals have been known to trash computers, some counterfeit appliances have started fires and guys, when your gal's girlfriends inform her that that designer handbag you got her is really a cheap knock-off, I assure you, you'll wish you had paid full price for the real thing.

### 4) Phony Order Confirmation - Phishing Fraud

Just checking my emails. Oh look, an email from a retailer informing me that there's a problem with the Christmas presents I ordered. That's funny, the email isn't addressed to me, but to "Dear Customer," there are some misspellings and poor grammar. And you know, I don't even remember ordering from this store. It's undoubtedly an example of a growing phishing scam known as the "False Order Confirmation Fraud."

What the fraudsters would like you to do is click on the link in the email, which will take you to a site where you'll be asked to supply them with your personal identifiers, such as social security number, credit card numbers, bank account information, etc. If you receive such an email, ignore it. But if you think there might

be a problem with an order you've made, DO NOT click on the link in the email. Instead, contact the retailer directly to check on your order.

The holidays are all about giving, but not giving away your identity.

### **5) Charity Scams**

The holidays are about giving, and nothing gives you that holiday glow like contributing to a charity. And besides, at this time of year, it can be great tax strategy, too.

While there are many worthwhile charities, there are also plenty of unscrupulous fraudsters more than willing to masquerade as a charity in order to get at your money. Adding to this situation is the fact that many charities use telephone solicitation campaigns and, because of low processing costs, prefer online giving.

Be wary of telephone solicitations, especially high-pressure calls. Do not rely on caller ID: That too can be manipulated. Any good charity will allow you to call them on an independently verifiable telephone number.

If making a contribution online, be cautious with responding via a link in a solicitation email. Instead, go on your own to the charity's official website. When you're at the screen for making your contribution, make sure that the URL, or the webpage address, begins with the letters "https", not just "http," in order to ensure a secure transaction.

So go ahead and include in your Holiday celebration generous contributions to your favorite church, non-profit or university of your choice. Just make sure that your money goes toward good works, not to evil-doers.

### **6) Credit Card Refund Fraud**

It happens every holiday season. You buy too many gifts, or you find a better gift for that special someone. You're back at the store where you bought the item, asking the clerk to apply the return credit to the credit card on which you purchased the gift. The clerk goes away, processes the transaction, and returns with a long slip of paper which the clerk has conveniently folded up, and drops it into one of your shopping bags.

Do you look at the slip? Carefully?

You should, because some unscrupulous clerks have been known to process these transactions fraudulently. Instead of applying the return to your credit card, they apply it to their own. Or they process it as a cash return, pocketing the cash, and handing you just a long, folded slip of paper.

If you don't examine the return receipt, you might not realize that you were scammed until weeks later when you get your credit card bill. By then, it may be difficult to prove that you were defrauded.

So always carefully examine your return receipts. Check to make sure the transaction wasn't processed as a cash return. If it was processed as a credit card refund, make sure it was credited to your credit card.

### **7) RFID Credit Card High-Tech Pick Pocketing**

Do you a credit card that has a radio frequency identification chip (RFID) embedded in it? They're the ones that you just have to wave in front of the credit card terminal and when the lights go on, your transaction goes through.

Some fraud researchers have found that by using a well-concealed, souped-up scanner, they've been able to capture RFID credit card account numbers and other identifying information off of people in a crowd just by standing near a cardholder's wallet or purse.

While many banks encrypt the data on RFID credit cards, and there have been few police reports to date on this sort of high-tech pick pocketing, many fraud experts feel that potential for massive fraud is there.

How do you foil these potential electronic fraudsters? With foil. While there are many good security sleeves for RFID cards available on the market, a number of experts suggest that by simply bundling your RFID credit cards together and wrapping them in a piece of crinkled aluminum foil, the RFID signal should become so weak and garbled that it is too difficult for a high-tech pickpocket to capture any information in a casual or crowd setting.

### **8) ATM Frauds**

You're heading out for a Holiday party with some friends and colleagues, but first you need to get some cash. Why look! There's an ATM right over there.

Before you use that ATM, make sure that you're just getting cash and not getting scammed. There are a number of fraudsters who can manipulate ATMs to get what they want: your ATM or debit card account number and your PIN. With these two pieces of information, a scammer can drain your bank account.

So what can you do? Always be vigilant when using an ATM. Especially be careful at ATMs that suddenly appear on the street or in unsecured building lobbies. Fraudsters have been known to place their own ATMs temporarily in high traffic areas just to capture card numbers and PINs.

Even the most trustworthy ATMs can be tampered with by fraudsters for their evil purposes. Don't use an ATM if a replacement card reader, a "skimmer" or superimposed key pad has been placed on the ATM.

Also, be on the lookout for small pinhole video cameras that are aimed at the keypad. All of these devices are used to steal the valuable card numbers and PINs. Whenever you're entering your PIN, cover your one hand with the other so that any cameras or shoulder surfers can't make out your PIN.

So be careful when using an ATM, you don't want a simple cash-run to leave you with a pretty ho-ho-hopeless holiday.

### **9) Phony Salesclerk Scam**

Don't you just love holiday shopping? So many of the salesclerks are so courteous, maybe even approaching you on the sales floor, welcoming you to their store, and offering to relieve you of the burden of the items that you've already picked out so that you can continue shopping. You hand over the armful of merchandise, along with your credit card or cash so that the salesclerk can ring up the items you've selected so far.

But wait: Are you sure that was a salesclerk? Did you notice if they were wearing a store-issued nametag or the distinctive store vest? Or did you just fall victim to the phony salesclerk fraud? You are a victim if, after leaving you, the "salesclerk" walks out of sight, dumps the merchandise you handed over, and quickly leaves the store with your cash or credit card.

So what can you do to avoid being taken this way? If you can, take your merchandise to the sales register yourself. And if a store employee offers to help, see that the clerk is wearing the store's nametag, vest, or other identifying feature. Also, never have the clerk ring up a sale in your absence; just allow the clerk to take your selected items to be held at the sales register, where everything can be rung up once you are done shopping.

You have enough to do to complete your own holiday shopping, you don't need to help a fraudster with theirs.

### **10) Phony Cyber Shopping Sites**

Cyber shopping during the holidays is great. It's convenient, there are some great bargains online and you get to avoid the holiday mob at the mall.

But are you certain that you've been shopping on your favorite retailer's actual website? Recently, federal agents have shut down and seized a number of bogus sites that appeared to be the authentic websites for legitimate stores. While the Feds took down a bunch of these sites, it is believed that there are a lot more out there.

The fraudsters who run these sites aren't out to sell you goods, they are only out to con you into handing over to them your credit card or debit card information.

Before you cyber shop, make sure you have the authentic website. If necessary, telephone the store and ask for their their web address. Enter web addresses meticulously; some fraudsters have been known to register web addresses that are spelled just slightly different from a legitimate retailer's URL. Examine web addresses for extensions, especially ones that seem to redirect you to another site. And don't use a retailer's website if the URL ends with an unfamiliar or inappropriate country code.

Cyber shopping can be wonderful, but cyber fraud can leave you as empty as a Christmas stocking on Dec. 23.

### **11) Fraudulent Check Scam**

This one is for you small business owners. You've been working hard so that your Holiday sales put you in the black when suddenly you receive a great email. It seems that a brand new customer wants to place a huge order!

Everything looks normal, except for one thing: this customer says that since a third party owes him a lot of money, you will be receiving a check (or some money orders) from this third party in payment for the order.

You are told, since the check may be for a sum greater than the order, please deposit the check, keep your share for the cost of the order, and then wire any excess funds to the customer via Western Union.

The check arrives, it's for a huge sum, and you deposit the check at your bank, ship the order, and when the funds become available, you wire the excess amount to your new customer, per his instructions.

Then days later, your bank calls. It turns out the check was bogus. Now you're not just out for the cost of the order, but you're also on the hook to the bank for all the funds you wired out to a customer who you'll never see again!

Business people, unless you really know and trust your customer, avoid any sales with a third-party payer that is structured in this way. If you do accept such a sale, remember: after you deposit a check, banks are required to make the funds available, sometimes long before the check clears. Hold off shipping merchandise or wiring excess funds until you're sure that the check has cleared and has been honored.

While red is a popular color during the holidays, the one place you don't want to see it is in the ink in your ledger.

### **12) Secret Skimmer Fraud**

Suddenly it's January. You had a great holiday season, but the piper must be paid and the credit card bills start rolling in. While looking over one of the bills, you notice a slew of charges that you didn't make, mostly for online purchases. How could this be? Your wallet wasn't stolen or your pockets picked. Your credit card was never out of your sight.

Or was it?

Suddenly you remember that day when you were finishing up your holiday shopping, and that one store clerk. He was very helpful, but said that his sales register wasn't working properly, so he had to take your credit card to another register to ring up the sale. The receipt he handed you seemed fine, but you had a funny feeling there was something more going on.

Well, your instincts were right. You're a victim of a duplicate skimmer fraud. Some unscrupulous store clerks have been known to carry their own credit card readers, maybe hidden in a purse, in a drawer under the sales register, or even under a jacket. They go ahead and skim your credit card in a register to complete your sale, but also give it a quick swipe in their own credit card reader to record the valuable information contained on your credit card's magnetic stripe. A quick look on the back of your card to get the three-digit code back there, and the clerk has everything that's needed to start charging on your account.

While you're doing your holiday shopping, try to avoid losing possession of your credit card. If you must hand a clerk your card, keep the clerk and your card in sight at all times. Walk with the clerk to the other register if that's what it takes to keep an eye on your credit card.

Be careful out there. Don't let a quick, fraudulent credit card swipe rob you of your