R. SETH WILLIAMS
District Attorney

DISTRICT ATTORNEY'S OFFICE
THREE SOUTH PENN SQUARE
CORNER OF JUNIPER AND
SOUTH PENN SQUARE
PHILADELPHIA, PA 19107

Press Release

Date: November 20, 2012

Contact: Tasha Jamerson
Director of Communications
W: 215-686-8711
C: 215-680-7383

Advice for Safe Thanksgiving Day and Black Friday Shopping Experiences

Philadelphia---Traditionally "Black Friday" marked the beginning of the hectic holiday shopping season, this year a large number of stores are opening on Thanksgiving Day; and with the increased hours comes increased safety concerns. The District Attorney's Office along with the Philadelphia Police Department wants to remind everyone while it's a busy time of the year for bargain hunters it's also the perfect time for criminals to pounce unsuspecting shoppers.

"There is always somebody looking to separate you from your money," said District Attorney Seth Williams. "The best course of action is prevention. Many thieves choose their victims because the thieves see an opportunity. If you take away the opportunity, chances are you won't become a victim. The last thing that anyone needs during these tough economic times is to lose their hard earned money because of a criminal."

With so many stores now opening on Thanksgiving there are new concerns about the physical safety of shoppers, as well as retail employees. Crowd related injuries during holiday sales events have increased over the past few years. In 2010 several people were trampled in Buffalo, NY during a "Black Friday" sale at a Target store, and in 2008 a Walmart employee died during the opening of a "Black Friday" sale in Long Island, NY. As a result of the increase in pre-"Black Friday" events

OSHA has issued a new set of safety guidelines for retailers which can be found on OSHA's website: www.osha.gov/OshDoc/data_General_Facts/Crowd_Control.

There are several new scams this year that the District Attorney's Office and the Police Department are monitoring:

New Scams of 2012

- ***Used gift cards***: Look up reviews for any 3rd-party seller offering used gift cards for sale. The FBI warns cards reported as stolen can later be disabled, leaving you with a worthless piece of plastic.
- ***"One day only" bargain e-mails:*** If you receive any unsolicited Black Friday e-mail, don't click the links, and don't give them your credit card number. It's most likely part of some kind of phishing scam.
- ***Fake auctions / classified ads:*** Just like with the used gift cards, make sure the seller is legit by doing a Google search of their name, username, e-mail address, or anything that might point to something suspicious.
- ***Steeply discounted electronics stores:*** No online store is going to sell an iPad for $10. You won't find new digital cameras for $5. There are dozens of "fake" online electronics stores that don't even have an inventory, and they won't ship you anything you order. They're only out to get your credit card number.
- ***Parking lot bait and switch:*** Don't buy electronics from strangers that approach you in a parking lot. It's always a scam. Always. Often someone will approach you with some wild story about how they need to sell "this $1,000 laptop" or "these $1,000 speakers" fast. The price is usually only $100 to $200, but when you're back home with the box you'll find they switched it on you and there's nothing inside. Some crooks are so sophisticated, they've figured out how to re-wrap packages in plastic. So what looks like an unopened iPad is actually a box with some notepads inside to weight it down.

Debit or Credit

Even though they can look and act the same, it is important to remember that debit and credit cards have very different legal protections before hitting the mall for holiday sales. Government regulations and voluntary industry policies will protect you if a credit or debit card is used to make unauthorized purchases. But the protections for credit cards are much broader.

- ***Credit cards*.** Under federal law, if someone steals your credit card you're only responsible to pay the first $50 of unauthorized charges. And if you

notify the issuer before the thief makes any charges, you may not be out anything. You're also free from liability if unauthorized purchases occur when the card is not physically present, for example if your credit card number is stolen.

Zero-liability policies, like those offered by Visa and MasterCard, add a second layer of protection. Under these programs you won't pay anything if someone fraudulently uses your credit card online or off.

- ***Debit cards*.** The rules are similar for debit cards, but there are a few restrictions. For example, your liability under federal law is limited to $50, but only if you notify the issuer within two business days of discovering the card's loss or theft. Your liability could jump to $500 if you put it off. And even this cap is lifted if you wait more than 60 calendar days from the time your bank statement is *mailed*.

  Federal protections are a bit more generous if a thief just steals your debit card number (and not the actual car), but you still have 60 days after receiving your bank statement to report any unauthorized transactions.

Places ***NOT*** to use your debit card

- ***Online***- Don't use the debit card online, if you have problems with a purchase or the card number gets hijacked, you are vulnerable because it is linked to a bank account. Most banks have voluntary policies that set their own customers' liability with debit cards at $0, but the protections don't relieve consumers of hassle of waiting for the stolen money to be credited back to their accounts.

- ***Big-ticket items***- With a big ticket item, a credit card is safer because credit card companies offer dispute rights if something goes wrong with the merchandise or the purchase. In addition, some cards will also offer extended warrantees. And in some situations, like buying electronics, some credit cards also offer additional insurance to cover the item.

- ***Restaurants-*** Restaurants are one of the few places where you have to let cards leave your sight in order to use them. This can always be problematic if an employee is unscrupulous. Also some establishments will approve the card for more than your purchase amount because, presumably, you intend to leave a tip. So the amount of money frozen for the transaction could be quite a bit more than the amount of your tab. And it could be a few days before you get the cash back in your account.

- ***Gas stations*** - Some gas stations will place holds on debit card transactions to cover the purchase. That means that even though you only bought $10 in gas, you could have a temporary bank hold for $50 to $100.

- ***Checkouts or ATMs that look 'off'***- Criminals are getting better with skimmers and planting them in more places you'd never suspect -- like ATM machines on bank property or supermarket checkouts. Take a good look at the machine before using it. Does the machine fit together well or does something look off, different or like it doesn't quite belong? Make sure it doesn't look like it's been tampered with.

<u>Cybercrimes to continue to watch out for</u>

- ***Malicious Mobile Applications*** -These are mobile apps designed to steal information from smartphones, or send out expensive text messages without a user's consent. Dangerous apps are usually offered for free, and masquerade as fun applications, such as games.
- ***Phony Facebook Promotions and Contests*** – Who doesn't want to win some free prizes or get a great deal around the holidays? Unfortunately, cyberscammers know that these are attractive lures and they have sprinkled Facebook with phony promotions and contests aimed at gathering personal information. A recent scam advertised two free airline tickets, but required participants to fill out multiple surveys requesting personal information.
- ***Scareware, or Fake Antivirus software*** – Scareware is the fake antivirus software that tricks someone into believing that their computer is at risk—or already infected—so they agree to download and pay for phony software. This is one of the most common and dangerous Internet threats today, with an estimated one million victims falling for this scam each day
- ***Holiday Screensavers***—Bringing holiday cheer to your home or work PC sounds like a fun idea to get into the holiday spirit, but be careful. A recent search for a Santa screensaver that promises to let you "fly with Santa in 3D" is malicious. Holiday-themed ringtones and e-cards have been known to be malicious too.
- ***Mac Malware*** – Until recently, Mac users felt pretty insulated from online security threats, since most were targeted at PCs. But with the growing popularity of Apple products, for both business and personal use, cyber criminals have designed a new wave of malware directed squarely at Mac users.
- ***Holiday Phishing/Smishing Scams*** – Phishing is the act of tricking consumers into revealing information or performing actions they wouldn't normally do online using phony email or social media posts. Cyberscammers know that most people are busy around the holidays so they tailor their emails and social messages with holiday themes in the hopes of tricking recipients into revealing personal information. A common holiday phishing

scam is a phony notice from UPS, saying you have a package and need to fill out an attached form to get it delivered. The form may ask for personal or financial details that will go straight into the hands of the cyberscammer. Banking phishing scams continue to be popular and the holiday season means consumers will be spending more money—and checking bank balances more often.

- ***Online Coupon Scams*** – An estimated 63 percent of shoppers search for online coupons or deals when they purchase something on the Internet, and many consumers are also using their smartphones and tablets to redeem those coupons. One popular scam is to lure consumers with the hope of winning a "free" iPad. Consumers click on a "phishing" site, which can result in email spam and possibly dealing with identify theft. Consumers are offered an online coupon code and once they agree, are asked to provide personal information, including credit-card details, passwords and other financial data.
- ***Mystery Shopper Scams*** – Mystery shoppers are people who are hired to shop in a store and report back on the customer service. Sadly, scammers are now using this fun job to try to lure people into revealing personal and financial information. There have been reports of scammers sending text messages to victims, offering to pay them $50 an hour to be a mystery shopper, and instructing them to call a number if they are interested. Once the victim calls, they are asked for their personal information, including credit card and bank account numbers.
- ***Hotel "Wrong Transaction" Malware Emails*** – Many people travel over the holidays, so it is no surprise that scammers have designed travel-related scams in the hopes of getting us to click on dangerous emails. In one recent example, a scammer sent out emails that appeared to be from a hotel, claiming that a "wrong transaction" had been discovered on the recipient's credit card. It then asked them to fill out an attached refund form. Once opened, the attachment downloads malware onto their machine.
- ***"It" Gift Scams*** – Every year there are hot holiday gifts, such as toys and gadgets, that sell out early in the season. When a gift is hot, not only do sellers mark up the price, but scammers will also start advertising these gifts on rogue websites and social networks, even if they don't have them. So, consumers could wind up paying for an item and giving away credit card details only to receive nothing in return.
- ***"I'm away from home" Scammers*** – Posting information about a vacation on social networking sites could actually be dangerous. If someone is connected with people they don't know on Facebook or other social networking sites, they could see their post and decide that it may be a good time to rob them. Furthermore, a quick online search can easily turn up their home address.

How to Protect Yourself

You can protect yourselves from cybercrime by following some of these quick tips:

- Only download mobile apps from official app stores, such as iTunes and the Android Market, and read user reviews before downloading them.
- Be extra vigilant when reviewing and responding to emails.
- Watch out for too-good-to-be-true offers on social networks (like free airline tickets). Never agree to reveal your personal information just to participate in a promotion.
- Don't accept requests on social networks from people you don't know in real life. Wait to post pictures and comments about your vacation until you've already returned home.

Also always keep a close watch on your bank account, especially for unauthorized transactions—no mater how big or small.

- **Small and Frequent Charges**
  What it is: Scammers will "test" victims, making small charges on their credit card to see if they are caught. If they go undetected, the scammer will later make larger and larger charges.
  What to do: Review your bank statement monthly, and call the company if you don't recognize any charges.

- **Skimmers**
  What it is: Scammers will capture keypad and card information when consumers input their PIN number at ATMs, gas stations, restaurants, etc. They can then use this to extract money from victims' accounts.
  What to do: Always select the "credit" option at retailers, gas stations, and restaurants, even if you are using a debit card. By selecting "credit," you do not have to input your PIN and you are less liable for fraud. With ATMs, try to use those at your bank whenever possible.

"Nobody is safe from thieves whether it is in stores, on the street or over the internet," said Mr. Williams. "If your identity is stolen, you could spend 18 months to three years in credit purgatory. Prevention is critical."

On the ground:
Since thieves work on the ground as well as on the internet, here are strategies to avoid becoming a victim of crime:

1. Guard the chain of custody of your credit card. If you give your credit card to a clerk or restaurant server who then takes it in the back and swipes it on a 'wedge,' the information on the magnetic stripe from your credit card can be duplicated.
2. **Do not put your purse in a shopping cart**.

3. Keep your wallet in an inside pocket, and strap your purse around you and tuck it under your arm. Beware of people bumping into you or distracting your attention by engaging you in conversation. This is an old scam to divert your attention in order to steal your wallet or purse.
4. Place your packages in the trunk so they cannot be seen. Always park in a well-lighted area.
5. Do not park next to a van. Criminals can pull you into a van as you go to your car, and nobody will see it happen.
6. Always accompany young children to the restroom. Tell your children in advance to look for a source of help ***within the store or mall***, such as a uniformed police officer or a salesperson with a nametag.

On the Phone:

"Crimes of persuasion" are the schemes, scams, and frauds that con artists use to steal your savings. Watch out for sob stories, sweepstakes, lotteries, and wacky investments, secured credit card offers, credit repair offers and even fortune tellers. While some telemarketers are legitimate, do not give out social security numbers or credit card numbers to unknown people on the telephone.

Other Methods:

1. Accessing your credit report by posing as an employer, loan officer or landlord.
2. Stealing mail from mailboxes to obtain credit card statements, bank statements or other personal information.
3. Taking trash bags from the street with old credit card and bank statements.
4. "Dumpster Diving" into trash bins to retrieve financial statements.
5. Motto: Shred, shred, shred, and be sure to use a **cross-cut shredder**. Vertical strips can easily be pieced together, and vertical shredders should be avoided.
6. Dishonest employees with access to your personnel records.
7. Misdirected mail or email with personal information.

Most Valuable Documents for Thieves:

1. Social Security Card—The 'magic' number. Do not carry your social security card with you, and do not give out the number. If you are asked for the number, ask the person what would happen if you didn't give it out. In many cases, it's not necessary.
2. Drivers license, Birth certificates and passports
3. Credit Cards