



News Release

FOR IMMEDIATE DISTRIBUTION

Saskatchewan Policing Agencies Remind Consumers March is Fraud Awareness Month: Focus on Mass Marketing Fraud and On-Line Fraud

The Commercial Crime and Fraud Sections with the Saskatoon Police Service, Saskatchewan Financial Services Commission, the RCMP “F Division and Regina Police Service have joined forces to promote March as Fraud Awareness Month to Saskatchewan residents and consumers.

During this the third week of Fraud Awareness Month, the fraudulent activity to be profiled is Mass Marketing Fraud and On-Line Fraud. Over the past year, Saskatchewan Police Agencies have received an increase in the number of complaints where the public is making purchases over the internet for items which are priced at an amount which could be described as “too good to be true.”

What is Mass Marketing and On-Line Fraud?

In most incidents, a big ticket item such as a vehicle, travel trailer, boat, ATV or property, is advertised on an on-line classified website at a significantly discounted rate. The seller will often use an on-line auction site as a broker and sends an email that appears to be from the on-line auction site to the buyer, however the email is only a copy of an actual on-line auction site email. The seller will also provide the name and website address of a shipping company which is also fake. As part of the agreement, the on-line auction is to act as the broker. The payment is to be sent to a person acting as the “agent” for the on-line auction site and the payment for the item is to be sent to the agent through a money transfer service where the funds will be available instantly. The seller will often say they have to sell the item for different reasons that they have to sell the item at the reduced price such as:

- o Marriage Breakdown
- o Job Transfer, and they have been moved out of the country
- o Visiting relatives out of the country and they need the money
- o Were in Canada working, have returned to their home country, and did not bring the item with them
- o Have stated they are with the Canadian military and are currently deployed out of the country

The purchaser will be informed that the item is in storage, or is in care of a friend or relative who are in Canada or the United States. Once the on-line auction site receives the payment, they will have the shipping company transport the item to the purchaser. It is stated that the on-line auction site will hold the money until the item is received by the purchaser, allowing them to see the item and determine if they are satisfied with it. If the purchaser is satisfied they will notify the on-line auction site which will then release payment to the seller. If the purchaser is not satisfied they are to notify the on-line auction site which will then return the money to the purchaser, and the item will be returned to where it was sent from.

In the end the item is not received by the purchaser because it does not exist. The money sent to the “agent” for the on-line auction site has been obtained, and will not be returned to the purchaser because the on-line auction site does not act as a broker for purchases. The investigation of these types of incidents is difficult because the money is often sent out of the country and the payment is received by persons using fake identification at locations where surveillance video is not used.

Has this ever happened in Saskatchewan?

A complaint was received and the victim advised he had purchased a vehicle through an on-line classified website and sent the funds to purchase the vehicle. The victim had not yet received the vehicle and was unable to have any other contact with the seller. The vehicle, advertised at a specific location in the United States, was offered at a price substantially less than the vehicle’s regular price tag. Pictures of the vehicle were sent to the victim that matched the vehicle description. The agreement was that the money would be sent from the victim’s account directly to a bank account located in the United States. The owner of this account was identified as a third party broker who would be holding the funds until the vehicle was received by the purchaser, inspected, and had determined that they would be keeping the vehicle. The victim believed they were sending the money to the broker account to a location in the United States. Most times, the seller will request that the money be sent via money transfer service to the third party broker as opposed to the money being sent through an account transfer.

The victim provided police access to his email account to view and obtain information from the email sent by the suspect which could be used to determine the location of the sender. The investigator was able to confirm that the emails were originating through an internet service provider located in the United States.

The bank responsible for the account was contacted and was able to confirm the transfer of the victim’s money into the account. They advised that part of the deposit had been withdrawn, but part of the victim’s deposit was still in the account. They also advised they would be obtaining surveillance video from the ATM where the money had been withdrawn from. The bank froze the account to avoid future withdrawals and the account was flagged so law enforcement could be contacted in the event attempts were made to withdraw money from the account. The bank advised that the victim should be able to get his money returned to him.

The FBI was contacted and stated that this was believed to be part of an organized crime group and that they would follow-up on the investigation. The investigator was contacted by the FBI approximately 3 months later and was advised that an arrest had been made of an individual in the U.S. This person was identified and confirmed as being part of a foreign organized crime group. This investigation was successful because the victim was able to have his funds returned. He contacted the police immediately which assisted significantly with the investigation. As the payment was made by the victim through a transfer from their account to another account allowed police and banking officials to track the payment. Often payment is made through a money transfer service which makes the tracking of funds extremely difficult and allows the perpetrator to obtain the funds immediately after they are sent.

It is necessary for the public to be cautious when purchasing items using an on-line classified website. The following tips can be used to keep the public safe from becoming victims:

- Don’t be pressured into making a purchase. The seller will often use high pressure tactics, informing the purchaser that they might have other people who are interested, or that if they commit to the purchase now, they will not take any offers from anyone else.

- o Perform price comparisons. Often the items that are being sold are higher end, and appear to be in excellent condition, with most or all of the available options, and low mileage. They will price the items often less than half the amount of what the item should normally be priced at. Question why a person would sell you this item at such a reduced price when you are a stranger to them.
- o Ask for serial numbers and pictures. Serial numbers can be taken to dealers for the items who can confirm if the numbers are valid, and inform where the item was purchased. Observe any pictures you receive, and look for details in the pictures such as the background of the picture, license plates, and details of the item such as the speedometer. If the speedometer is showing miles per hour as opposed to kilometers per hour when the vehicle is supposed to be located in Canada, it is important to question this detail.
- o Ask for an address to look at the item before purchasing it. If the seller does not have any contact with you after this request, this is a sign that the item does not exist.
- o Obtain as much information about the seller such as their name, address, email address and phone number. Use the internet and conduct web-searches to see if this information has been used in any other frauds. If there is a shipping company that is named, do an internet search of the shipping company name, and confirm whether or not they are an actual business.
- o Pay attention to the email address of the email that you are receiving from the on-line auction site. The email address may contain the name as part of the email address but it is not an actual email from them. The on-line auction site typically does not send email through web email providers such as hushmail, rocketmail, or gmail as examples.
- o Do not make a deal and send money on an item you have not seen. All purchases on-line resulting in frauds are in cases where the purchase is occurring sight unseen. Ask yourself if it is worth sending thousands of dollars to someone you don't know for an item you haven't seen.

Remember that if something sounds too good to be true, it likely is. Nobody is going to give you something for nothing.

Consumers should also be aware of fraud that is occurring involving rental property that is advertised in an on-line classified website. The rental ads are for apartments, houses or condos, and the rental rate is significantly less than what the normal rent on comparable property would be. The person who has listed the ad states they are willing to sublet the property to the person as they will be away for an extended period of time either because of work, vacation, or family. They inform the person that they believe they are good, and trustworthy, and are willing to rent them the property.

The only requirement is that they send the damage deposit to them through a money transfer service, and upon receipt they will be sent a key to the property. The money is always to be sent outside of Canada because the person is already gone. The amount of the damage deposit is usually \$500 to \$1000 which they are informed will be returned to them at the end of the rental. The addresses and pictures of the rental properties are obtained from the internet and are actual properties owned by people who are not aware of this taking place.

What is On-Line Fraud as a Seller?

Often a perpetrator's success depends on the victim's greed and haste. In a typical scenario, the potential victim is legitimately selling items on an on-line classified website. The buyer contacts the seller and proposes buying the item for sale but offers to pay an amount greater than the selling price with an agreement that the difference will then be forwarded to a third party who will act as a shipper for the buyer.

This money sent to the shipper is to be sent through a money transfer service. As an added incentive for doing this the buyer will tell the seller that they can keep a small amount or percentage of the money for their assistance with this. A cheque or money order will be sent to the seller which they are to deposit in their account and then forward the difference to a person referred to as the “shipper” using a wire transfer service. If the seller carries out these instructions, they eventually discover that the cheque or money order sent by the buyer is forged, and the deposit made into their account will be reversed by their financial institution. As a result the victim has lost the money he or she sent, plus whatever banking fees apply to the return or NSF charge.

These frauds are extremely challenging because they can originate from anywhere in the world making the identification of suspects and gathering evidence very difficult. It is important that people exercise caution in all internet-based business transactions. When selling items on an internet-based marketplace the following information is important to review:

- Any email where the name of the seller has biblical references (Gabriel, John, Elijah, etc.) and the content of the email uses poor grammar, spelling, and sentence structure.
- Location of the buyer. Question why the buyer who says they are located outside of Canada would want to purchase your item (which is usually available everywhere) and often pay a shipping cost that is greater than the cost of the item.
- Suspicious emails that use hotmail, gmail, or yahoo extensions as these can be sent from anywhere in the world.
- Buyers who offer an amount significantly higher than the value of the item for sale.
- Any requests to forward extra money to a third party combined with an offer to keep some of the cash by the seller.
- High pressure emails to carry out requests and conditions (like forwarding money) immediately. If the cheque or money order is successfully deposited in the sellers’ account, there is often 5-7 days before it is discovered by the banks’ clearing house that it is a forgery. The buyer will pressure the seller to immediately forward the amount of money to the “shipper” once the deposit is made into their account.

The internet can be used as a tool to prevent you from falling victim to this type of fraud. Use the internet to conduct searches of any information the seller gives you about themselves such as their name, location, contact information (email addresses and phone numbers) and information about the person or company acting as a shipper. In these types of frauds the same information is used on multiple victims or there may be similarities to previous frauds. Often people who are victim to these types of incidents will post information to specific websites pertaining to fraud on the internet to help prevent other people from becoming victims.

Through heightened awareness of Fraud Awareness Month, the trained staff of Commercial Crime and Fraud Sections with Saskatoon Police Service, Saskatchewan Financial Services Commission, RCMP “F” Division, and Regina Police Service will be able to share their knowledge and inform the general public. Education on fraudulent activities will help prevent consumers from becoming “victims.” Future fraudulent activities to be profiled in media releases during the month of March as part of Fraud Awareness Month include Social Networking/On-Line Dating Fraud and Securities Schemes.

For further information, contact:

March 15, 2010

Corporal Trevor Ellis
Commercial Crime Section
RCMP “F” Division
Phone: 306-780-6005

Or visit: www.sacp.ca/fraudawareness/

The following contact information is offered below as additional reference.

RCMP “F” Division: www.rcmp-grc.gc.ca/sk

RCMP: www.rcmp-grc.gc.ca/scams-fraudes/

Regina Police Service: www.reginapolice.ca

Saskatoon Police Service: www.police.saskatoon.sk.ca

Saskatchewan Financial Services Commission: www.sfsc.gov.sk.ca

Better Business Bureau: 1-888-352-7601, www.sask.bbb.org

Consumer Protection Branch: (306) 787-5560, www.justice.gov.sk.ca/cpb

Corporations Branch: (306) 787-2962, www.corporations.justice.gov.sk.ca

Bank of Canada: www.bankofcanada.ca/en/video_corp/dbo/dvd_fraud.html



**Saskatchewan
Financial Services
Commission**

