CALGARY POLICE SERVICE

Protect Yourself From Scams

Practical Information on

- Identity Theft
- Cheque Overpayment Scams
- Advance Fee Letters
- Inheritance Schemes
- Advance Fee Loans
- Phishing & Vishing
- Lottery Scams
- Travel
- Internet Auction Second Chance Offers
- Payment Card Skimming
- Reporting Fraud

CAA ALBERTA AMA

ALBERTA MOTOR ASSOCIATION

Identity Theft

Identity theft occurs when your personal information is collected and used by persons without authorization to do so. The result of this illegal activity includes, but is not limited to, applications in your name being made for credit with financial institutions, retail outlets, mortgage companies, etc. Once your identity is compromised, it may take tremendous amounts of effort on your part in order to restore your good name and credit rating.

Tips on how to reduce your chances of becoming a victim of identity theft include:

- Before you reveal any personal identifying information, find out how it will be used and if it will be shared with others.
- Pay attention to your billing cycles. Follow up with creditors if your bills do not arrive on time.
- Guard your mail. Deposit outgoing mail in post office collection boxes or at your local post office. Promptly remove mail from your mailbox after delivery. Ensure mail is forwarded or re-routed if you move or change your mailing address.
- Utilize passwords on your credit card, bank and phone accounts. Avoid using easily available information such as your mother's maiden name, your birth date, the last four digits of your SIN or your phone number.
- Minimize the identification, personal information and number of cards you carry.
- Do not give personal information on the phone, through the mail or over the internet unless you have initiated the contact or know with whom you are dealing.

- Keep items with personal information in a safe place. An identity thief may pick through your garbage or recycling bins. Be sure to tear or shred receipts, credit applications, insurance forms, physician statements and credit offers you get in the mail.
- Give your SIN only when absolutely necessary. Ask to use other types of identifiers when possible.
- Do not carry your SIN card or birth certificate; leave them in a secure place.
- Become familiar with schemes such as Phishing and Vishing which are designed to glean personal information from you via the Internet or telephone.

Cheque Overpayment Scams

Cheque overpayment scams are currently widespread and target several different groups of individuals. The most common targets for this scam are landlords with a property to rent and anyone who is advertising an item for sale. You will initially be contacted – usually via the Internet – by the scam artist posing as a legitimate renter or buyer, whichever the case may be. Once terms have been agreed upon, you will receive a cheque from the scam artist in an amount in excess of the amount actually owed. You will then be asked to deposit the cheque into your bank account and immediately wire the excess funds – usually by way of Western Union or MoneyGram – back to the sender or to the sender's agent or shipper. The deposited cheque is subsequently returned by the bank as counterfeit and the amount will be charged back to your account by the bank.

Tips on how to avoid overpayment scams:

- Know with whom you are dealing – independently confirm your renter/buyers name, street address and telephone number.
- Never accept a cheque for more than your asking price.
- Never agree to return excess funds to a renter/buyer via wire transfer – a legitimate renter/buyer will not pressure you to do so. You have minimal recourse if there is a problem with a wire transfer.
- Resist pressure to "act now." If the renter/buyer's offer is good now, it should be good when their cheque clears.
- Never return funds until the cheque has cleared.

Financial Agent/Payment Processor Offers

Very similar to cheque overpayment scams, you may fall prey to an online work offer if you have posted your resume on the internet. An international "employer" will contact you offering a position as the company's debt collector in Canada. Your job will be to collect payments from their Canadian clientele that have balances outstanding on their accounts. In due course, you will receive cheques in the mail with instructions to deposit them into your bank account, keep a commission for yourself (usually 10%-20%) and then forward the remaining funds to the "employer" via Western Union, MoneyGram or bank wire transfer. As with the overpayment scams, the cheques will eventually be identified as counterfeit and you will be required to replace the funds owing to the bank. The possibility of recovering your funds once they have been sent is essentially zero.

vareness

This scam is a glowing example of: "If it sounds too good to be true, it likely is." The same principles that underly the advice to protect yourself against overpayment scams apply to this scam as well.

Advance Fee Letters (Nigerian Letters) & Inheritance Schemes

These letters are commonly referred to as **Nigerian Letter Scams** or **West African Fraud Letters**.

The scheme begins once you receive a letter with a request for assistance with an urgent business transaction involving millions of dollars. Letters may be received by mail, fax or email. In addition to stressing the urgency and confidentiality of the transaction, these letters will also stress the importance of trust and honesty in an effort to make you believe in the letters validity. Furthermore, the authors of these letters will commonly claim to be a doctor and/or a corporate entity with a major corporation in Nigeria. There may also be some mention of government involvement.

After receiving a letter, you will be required to respond either by phone, fax or email in order to obtain further information on the requirements and procedures for the transaction. Once contact is established, the author of the letter will normally ask for an up-front processing fee and, in some cases, arrange for a meeting to discuss the transfer of funds. Most letters come with a percentage breakdown of the money each party involved will receive once the transaction is final. A typical breakdown would be 30% for the account holder (you), 60% for the author and his partners and 10% to be used in offsetting taxes and expenses.

Copies of letters of this nature, regardless of country origin, can be directly forwarded to PhoneBusters via fax at

(888) 654-9426 or by email at wafl@phonebusters.com.

Please contact PhoneBusters by phone at (888) 495-8501 if contact has been made with a "Nigerian" representative.

Inheritance Schemes

Inheritance schemes generally share the same origin as Nigerian Letters and are based on similar premise. You receive a wordy letter or email message from a stranger seeking your assistance in moving large amounts of money (often millions of dollars) to your bank account. A very wealthy individual—who happens to share the same last name as you—has died and you are asked to assist with banking and to share the wealth. You are promised a very significant percentage for little or no effort on your part, perhaps as high as 20%, for simply providing your bank account details.

This scam will soon lead you down one of two roads. You may be asked to provide bank account information for the transfer of funds to be facilitated. Compliance with this request will likely lead to your account being taken over and drained of its funds. Alternatively, you may be asked to provide money up front for one of any number of reasons ranging from administration fees to bribe money. Regardless of the request the result is the same; you will lose your money and there is no million dollar inheritance for you.

Your best defence against Nigerian Letters and Inheritance schemes is to not begin correspondence from unknown sources. If you receive requests of this nature, recognize them for what they are and do not begin correspondence or dialogue with the sender.

Advance Fee Loans

Ads that promise loans generally appear in classified sections of local and national newspapers, magazines and tabloids.

Some companies claim they can guarantee you a loan even if you have bad credit or no credit. They usually request an up-front fee, which may range from hundreds to thousands of dollars. Once you send your money to these companies, you never get your promised loan and you cannot get your money back. If you cannot get a loan through traditional lending institutions, it is unlikely that you'll get one in response to a classified ad.

In most jurisdictions, it is illegal for a company to request an up-front fee prior to obtaining a loan. Ask the loan company to take the amount of their fee off of the total amount of the loan that is promised to you.

Be sure to independently verify the legitimacy of the loan company through your own efforts. This may include Internet, Better Business Bureau and Service Alberta enquiries.

Remember: Simply advertising through recognized media outlets does not ensure the legitimacy of the company behind the ad.

Phishing & Vishing

The word **phishing** comes from the analogy that Internet scammers are using email lures to "fish" for passwords and financial data from the sea of Internet users.

Phishing, also called "brand spoofing", is the creation of email messages and web pages that are replicas of existing, legitimate sites and businesses. These web sites and emails are used to trick users into submitting personal, financial or password data. These emails refer to security issues related to your account. A website link is provided for you to check your account or update your information. You will then be asked for information

such as credit card numbers, bank account information, social insurance numbers and passwords.

The goal of criminals using brand spoofing is to lead you to believe that a request for information is coming from a legitimate company. In reality, it is a malicious attempt to collect your information for the purpose of committing fraud.

Tips on how to spot and avoid phishing scams:

- Protect your computer with anti-virus software, spyware filters, email filters and firewall programs which are updated regularly, daily or weekly.

- Contact the financial institution immediately and report your suspicions.
- Do not reply to any email that requests your personal information.
- Look for misspelled words.

Always report phishing or "spoofed" emails.

If you've received one of these suspicious emails, report it to **info@phonebusters.com** or the financial institution that it appears to be from.

Creative thieves are now switching their efforts to "**vishing**," which uses Voice over Internet Protocol (VoIP) phones. Rather than asking you to click on links that direct you to a malicious website, criminals have shifted to having you place a phone call instead. However, the phone number isn't to a bank or credit card company. It is a VoIP phone that can recognize telephone keystrokes. The thieves will blanket an area using a VoIP system. A recorded message tells you that your credit card has been breached and to "call the following (local) phone number immediately."

When you call the number, another message is played which states: "This is account verification; please enter your 16 digit account number."

vareness

Vishing scams can be made to look and sound very authentic. In light of this, if you receive an email that would direct you to a telephone number, do not use that number. Do not use the phone number provided in the email. Use a phone number that you have independently found from brochures set to you from the bank or through a search using phonebooks or the Internet.

Contact your credit card provider or the company which holds the account with a known number that is good in order to establish to validity of the request.

Lottery Scams

Although there are thousands of legitimate lotteries in regular operation around the world, criminals have seized the opportunity to victimize unsuspecting individuals by means of the lottery scam.

You receive a letter in the mail – usually from a foreign country such as Spain or the UK – advising that you have won a sum of money. Some details are provided, however you are required to contact a representative for further instruction. Once contact is made, you will be asked to provide a sum of money – usually a small amount to several thousand dollars – in order to cover administration fees, taxes, etc. In some cases, the perpetrators may even provide you with a cheque in the amount requested. You will then be directed to cash it and forward the funds to them prior to you receiving your winnings. As with other scams of this nature, the preferred method of money transfer will likely be Western Union or MoneyGram. The cheque, of course, is counterfeit and the winnings do not exist.

While you cannot necessarily avoid receiving such communications, you need not become a victim of

them. Legitimate lotteries do not require you to pay fees in advance of receipt of your winnings. You should be suspicious of any notice of winning a lottery or sweepstakes if you have no recollection of ever having entered the contest.

Travel

By simply filling out a ballot to win a vacation at a home, boat or auto show, you may be set up for a "suckers list". Shortly after filling out this ballot, you may be contacted over the phone by someone claiming to offer you a "free" or "low-cost" vacation. They will ask for your credit card number and personal information in order to hold the vacation for you, or they may request money in advance.

Do not give out your credit card information over the phone. If you want to check out the value of these promises, seek the advice of a legitimate travel agency in your area. If you have provided credit card information to the telemarketers, be aware that most companies have policies that allow you to cancel your reservation within 30 days. **Do not let anyone pressure you into committing to any type of agreement over the phone.**

Internet Auction Second Chance Offers

Following your unsuccessful bid to purchase an item online, you are contacted by the "seller" who notifies you that the item is still available. The "seller" wants to complete the transaction outside of the regular channels of the Internet auction site in order to save costs. Instructions for payment may include use of a

wire service, such as Western Union or MoneyGram. Alternatively, the "seller" may suggest the use of an escrow service which will prove to be bogus and actually controlled by the "seller" as a means of obtaining your credit card information.

Never agree to deals outside of the legitimately established online auction site that you are using. Should you choose to do so, you are likely setting yourself up to be scammed.

Beware the "seller" who insists on your use of an escrow service of their choice to the exclusion of all others. Do your homework to ensure the legitimacy of the service. **The mere existence of an official looking website does not guarantee the service's legitimacy.**

Payment Card Skimming

With more than 100,000 payment cards being compromised by criminals each year in Canada, debit/credit card identity theft – commonly known as "skimming" – is costing Canadians in excess of 400 million dollars annually.

Payment cards are usually skimmed when the legitimate cardholder presents their card for retail transactions at businesses such as gas stations, convenience stores and other retail locations whose point of sale equipment has been "compromised". This occurs when fraudsters have successfully gained control of the point of sale terminal and subsequently installed hardware designed to capture and store the data embedded in the magnetic stripe on the back of the payment card. In the case of debit card skimming, the fraudsters also install hardware to record the cardholder's PIN: Either

a concealed camera or a computer memory chip inside the PIN pad is used. The fraudsters then "write" this skimmed data onto a counterfeit payment card (a clone) and use this card for retail purchases or ATM cash withdrawals.

Until payment cards with more advanced security features are available, cardholders are reminded to safeguard your PIN by **shielding the PIN pad from view as you enter your PIN at any terminal**.

Never share your card or PIN with other persons.

Carefully review your account statements on a regular basis to verify that all transactions recorded therein are legitimate.

Contact your financial institution or credit card company if you observe any problems related to your account.

Reporting Fraud

If you are a victim of any of these scams, please report the fraudulent activity to PhoneBusters. PhoneBusters is the central agency in Canada that collects information on scams including telemarketing, advanced fee letters and identity theft complaints. Information collected by PhoneBusters is forwarded to the appropriate law enforcement agency.

Phone: 1-888-495-8501

Mail: PhoneBusters
Box 686
North Bay, Ontario P1B 8J8

Email: info@phonebusters.com

Copies of Advanced Fee Letter Fraud (419 / West African / Nigerian Letters) should be emailed directly to: walf@phonebusters.com

The information provided in this booklet was prepared by the Calgary Police Service, Fraud Detail, in collaboration with Phonebusters, The Canadian Anti-Fraud Call Centre.

www.phonebusters.com

Notes

CALGARY POLICE SERVICE

www.calgarypolice.ca

AMA

ama.ab.ca

GD00365 3M 03/10 16032

ALBERTA MOTOR ASSOCIATION