Planning Matters

Leith Wheeler INVESTMENT COUNSEL LTD.

Quiet Money.®

Contributors:

Tricia Wu, MBA, CFA, FRM
Principal, Portfolio Manager - Private Clients & Foundations

Mike Wallberg, CFA, MJ
Principal, VP Marketing & Communications

Visit our website to download previous Newsletters and read our latest Insights.

WINTER **2024** EDITION

Foiling Fraudsters

While the internet has democratized access to all human knowledge (and opinions), it has simultaneously created endless opportunities for fraudsters to separate trusting or uninformed citizens from their hard-earned money. Unfortunately, odds are you and your family will be targets at least once in your lifetimes, so we put together this resource to help you spot the trouble early. Forewarned is forearmed.

How big a probem is it?

According to the Federal Trade Commission, **American consumers reported losing nearly US$8.8 billion to fraud in 2022,** up more than 50% from 2021 levels and a more than 150% increase over 2020. The Canadian Anti-Fraud Center (CAFC) saw similar trends in Canada, with the largest losses coming from investment scams.

As forensic accountant Kelly Richmond Pope writes in her recent book, "Fool Me Once," these numbers are in fact heavily weighted to the elderly, and are very understated:

> "According to a recent AARP report, **people over the age of 65 are swindled out of an estimated $4.8 billion each year [in the US].** But this is just an estimate, since most crimes aren't reported. A study by the Consumer Financial Protection Bureau found that **older adults lose an average of $34,200** to financial exploitation… **$86,500 if fiduciaries – lawyers, trustees, financial professionals – are involved…** Although victims of fraud are not alone, they suffer their losses alone. Shame, guilt, embarrassment, and disbelief are among the reasons that **only an estimated 15 percent of fraud victims in the US report their plight to the police.**" (pp 109-111)

And it's not just the elderly – not one but **two** of our colleagues on the private client team had their grown sons fall victim to sophisticated scams in 2023. This is happening to people you know, and if the stats are any indication, most of the time it goes unreported. So be diligent and stay safe out there!

In the following sections, we take you through the high-level tactics being used by fraudsters, illustrate some common scams to watch out for, and finish with a checklist of To Dos and Not Dos when encountering a potential fraud.

What should you watch for?

Spelers Need N0t Apply: In written scams like emails or texts, watch for spelling or grammatical errors. Believe it or not, these are intentionally placed here to screen out more 'aware' recipients and thus not waste the scammer's time. It is also likely an unspoken term of war that keeps regulators off their backs – as making a scam too effective can raise the ire of entire populations (and their elected leaders).

Act Now to Avoid Disappointment! Fraudsters have to work fast to convert you in the time they have your attention, so they create a fictional deadline that forces you to give out your information before you have time to think it through or consult others.

Treats or Threats: They also home in on our fear and greed centres by making threats or offering extraordinary prizes, which can be powerful motivators to overrule reason.

Opportunity Knocks: Fraudsters are sophisticated and will tailor the scam to maximize their chance of success, such as shopping and delivery-related scams during the run-up to Christmas.

What are some specific scams to watch out for?

Telephone Scams (Vishing). In short, people pretending to be people who are either trying to help you or frighten you. Here are a few flavours:

The Threatening Authority Figure: A bad actor telephones you and pretends to be an authority figure (police, government official), threatening you with imminent legal action or steep fines unless you provide personal information and/or payments. A common one in Vancouver is for a Chinese-language speaker to impersonate a CRA officer, threatening jail time or fines unless the victim pays up.

What to do? Take a breath, and remember that creating that turmoil and panic is one of the key tools of scammers. Wherever they claim to be calling from, personally validate their claims by calling the agency directly from their posted phone number. Also, block the caller's number in your cell phone.

Jackpot!: For this one, scammers play to our desire to get a good deal, be delighted with a prize, or just feel lucky. There are generally a few red flags to watch for

here: there is a sense of urgency ("You have to claim your prize now before they're all gone!") which precludes you from being able to consult others before committing; the existence of this contest is news to you; and there is a requirement that you pay some fee to secure the prize. That fee, once paid, vanishes with the scammer.

What to do? If someone tells you you've won a contest you didn't enter, hang up. If they require you pay something to collect your prize, hang up. If they're pressuring you to commit on the phone, hang up.

The Grandparent Scam: In this scam, elderly people receive a call from a fake jailor or lawyer, informing them their grandchild has been arrested and requires bail money. The era of **artificial intelligence** has produced a new-and-improved (and frightening) version of this scam, in which the caller is able to credibly **mimic the *voice* of the grandchild,** by scraping the web for examples of them speaking and feeding it into an AI tool. Pope references a similar scam in her book, but the "son" sends an email to an aged parent claiming to have been robbed and needing money transferred immediately.

What to do? Do not engage. Ask for the name of the supposed jail, then independently contact your grandchild to verify their well-being. If you can't reach them, contact the jail from an independent source (i.e., do not accept the telephone number the caller may offer you). A proactive strategy you can employ is to have a **"safe word"** that only you and your family know – so if this scam is perpetrated, you can just ask the caller to tell you the word.

The Bank – Wi-Fi + Telephone + Text: In one of the frauds that happened to our colleague's son (let's call him Abdul), someone purporting to be from a Big 5 Bank called, saying they'd detected unusual activity in his savings account. Normally any of us would – with the pointers from this article maybe – know to be suspicious and not give any information out to a stranger, but this scam was in fact Part II of the fraudster's effort to steal from Abdul.

In Part I, while connected to an insecure Wi-Fi signal, maybe in a café, a nearby scammer likely hacked into his phone and recorded the keystrokes when he logged into his banking app. As a result, they already had his name, telephone number, username, and password, but couldn't get around the bank's 2-step verification – so they called him with the fraud story. They needed him to give them the PIN for his account, so they texted him a link, provided all they knew about him to gain his trust, and when he clicked in and entered his PIN they logged into his account, read off a few transactions to "test" for fraud (irony), hung up, and promptly drained his account. They also simultaneously opened a second account with the bank, deposited a phony cheque to it, and withdrew those funds too. Fraudsters can be very organized.

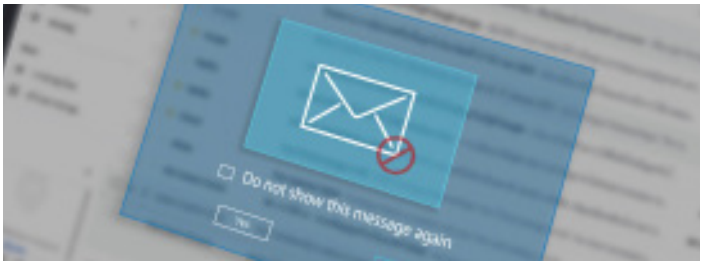
What to do? Always remember that if **they** are calling **you, you** can call **them**. Hang up, then call the number on the back of your bank card and explain what had been claimed to you. If it's real, you can deal with it. If it's not, you can dodge the scam.

For public Wi-Fi, only connect to a network you know and trust, such as hot spots by the big telcos, or ones that detail login and password details on a card at the till. Fraudsters will typically set up a similar-sounding network (possibly with a typo in it) and require you to download a program to "make your browser faster," but don't require a password. Again, it's independently verifying the access points to your data that will safeguard it. It's also a good idea to turn off your Wi-Fi connectivity when you're not using it, and avoid doing online shopping or banking while connected. Finally, using a "Virtual Private Network," or VPN, is the best way to ensure scammers can't penetrate your data.

Text Messages (Smishing): The other colleague's son (let's call him John) fell victim to a text scam (also called "smishing" for SMS phishing). Fraudsters are smart. They know when certain messages may ring as authentic – like a text two days before Christmas "from" Canada Post, providing an update on a package delivery and offering the chance to reschedule for a better time. For a fee. That requires clicking a link in the message. In this case, the son *was* expecting a delivery from Canada Post *and* wanted a different delivery window, so he clicked the link, which sent him "to" his bank's website... that was not a real website – it was a fake site into which he plugged his card number and password. Within minutes, the $1,500 in the account was gone.

What to do? In this case, he did the right thing and immediately called the bank when he realized what had happened and they were able to freeze the transfer and reverse the loss. To avoid it happening to you, save into your phone the name and contact numbers of vendors you've authorized to send you text messages. The easiest way to do this is to save the contact when they've sent you a text you're expecting (i.e., "Thank you for signing up for text messaging" arriving within minutes of approving it on a site). Then when you get a random one without previous ones in the chain, you'll know to be suspicious.

Email (Phishing): Any of these scams can be recreated as email versions, with the goal being to get you to click on a link which downloads malicious software. For texts or emails, you should watch for spelling or grammatical mistakes, watch for intense urgency, and for surprising threats or opportunities. Mainly, though, as discussed below, exercise extreme caution anytime you're being asked to click a link.



Fake online stores: In this scam, a realistic-looking online retailer is set up which offers unbelievable discounts. Those Ray-Bans that normally cost $500? Get them here for $47! They tend to pop up more around the holidays, and include (you guessed it) a time-limited sale price. You enter your credit card and mailing address, and inadvertently embark on a journey of credit card fraud and identity theft.

What to do? Sounds too good to be true? It probably is. Listen to your gut and take a beat before jumping on those deals. Also, beware of being asked to satisfy strange payment options such as gift cards or money orders as these are much more difficult to recover.

Fraud Hygiene - Best Practices

- If something sounds too good to be true, it probably is!
- Don't share your personal information online just to get a deal, or gain access to a website, app or service.
- Protect your files containing personal and sensitive information with passwords, use complex passwords, change them often, and don't write them down where others can have easy access to them.
- Don't click on any attachments or links from emails or phone numbers that you don't recognize. For inbound calls, when in doubt, hang up the phone and call them back with a number you know to be correct.

- Ensure that your financial institutions have your current Trusted Contact Person (TCP) information whom your advisors can contact if they suspect you are being financially exploited or are making poor decisions due to a potential diminishing mental capacity. (See this article on TCPs for more.)
- Educate yourself on emerging fraud trends so you can detect and identify potential fraud earlier. The CAFC is a great resource where you can browse through and learn more about reported and emerging scams.

In the unfortunate situation where you may fall victim to a fraud or scam, immediately notify your financial institutions and report the instance to the authorities, such as your local police and the CAFC (call toll-free at 1-888-495-8501).

Fight the stigma and share your experience as your experience may help someone else from falling into the trap of fraudsters!

About the Contributors

Tricia Wu joined Leith Wheeler in October 2016 with over six years of experience in treasury, pensions, corporate finance, and risk management. After spending three years with the Pensions & Institutions team, she began working with Private Clients and Foundations where she is responsible for managing discretionary investment portfolios.

Tricia earned a Master of Business Administration from the University of British Columbia and a Bachelor of Business Administration from Simon Fraser University. Tricia is a Chartered Financial Analyst (CFA®) charterholder and holds the Financial Risk Manager (FRM) designation. She served as a Director on the CFA Society Vancouver Board and sits on the Canadian Cancer Society's Organizing Committee for the Daffodil Ball.

Mike Wallberg joined Leith Wheeler in 2017. He is responsible for heading up the Marketing team, which manages the firm's thought leadership, social media, sponsorships, media relations, and digital initiatives. He graduated with a Bachelor of Commerce (honours - finance, UBC) and started his career as an investment banker with Merrill Lynch in Calgary and London, UK, and later spent 10 years with Phillips, Hager & North (now RBC GAM) as an equity analyst and institutional portfolio manager. Mike then earned a Master of Journalism (UBC) and produced television news for CBC before pivoting to marketing.

Mike is a Chartered Financial Analyst (CFA®) charterholder and Past President of CFA Society Vancouver (2021). He also hosts CFA Institute's flagship global investment podcast, Guiding Assets, where he interviews many of the leading minds from around the world on current issues and opportunities in our industry.

Vancouver Office
Suite 1500 - 400 Burrard Street
Vancouver, BC V6C 3A6
Tel: 604.683.3391
Email: info@leithwheeler.com

Calgary Office
Suite 750 - 215 2nd Street SW
Calgary, AB T2P 1M4
Tel: 403.648.4846
Email: info@leithwheeler.com

Toronto Office
Suite 2206 - 130 Adelaide Street W
Toronto, ON M5H 3P5
Tel: 416.646.8240
Email: info@leithwheeler.com