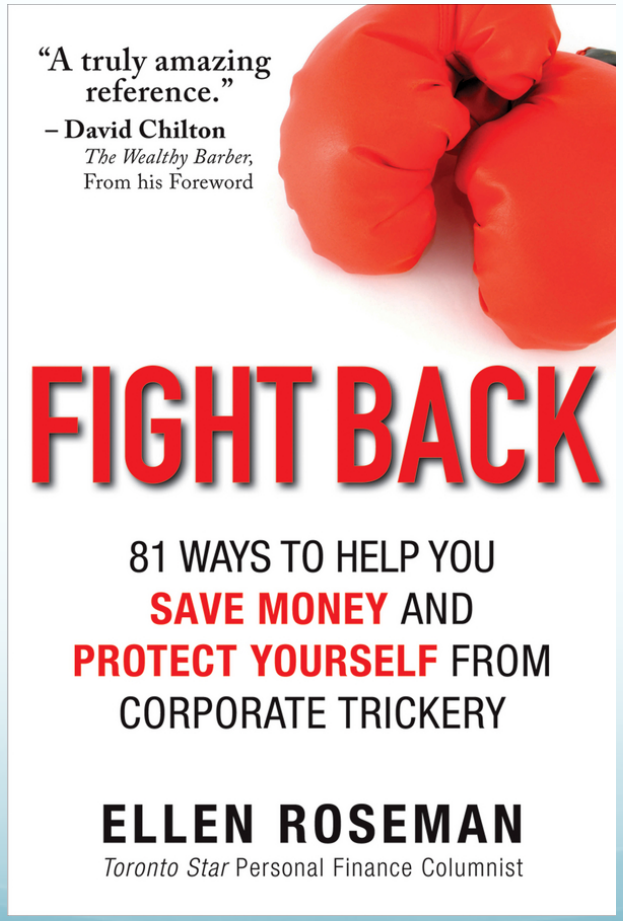
Preventing financial exploitation with Ellen Roseman

Fraud and scams



A huge spike in phone fraud

Politics

Scammers spoofing more than a dozen federal government departments to defraud Canadians

It's a new version of a scam that has ripped off thousands of individuals

Elizabeth Thompson · CBC News · Posted: Nov 06, 2019 4:00 AM ET | Last Updated: November 6

How does this fraud work?

- Some of the calls tell potential victims that their social insurance numbers (SINs) have been compromised. Others are told that they owe the government money and are in legal trouble.
- **To deceive potential victims who examine the numbers on incoming calls, the scammers "spoof" their calls, so they display the phone numbers of the relevant federal government departments.**

More on the SIN scam calls

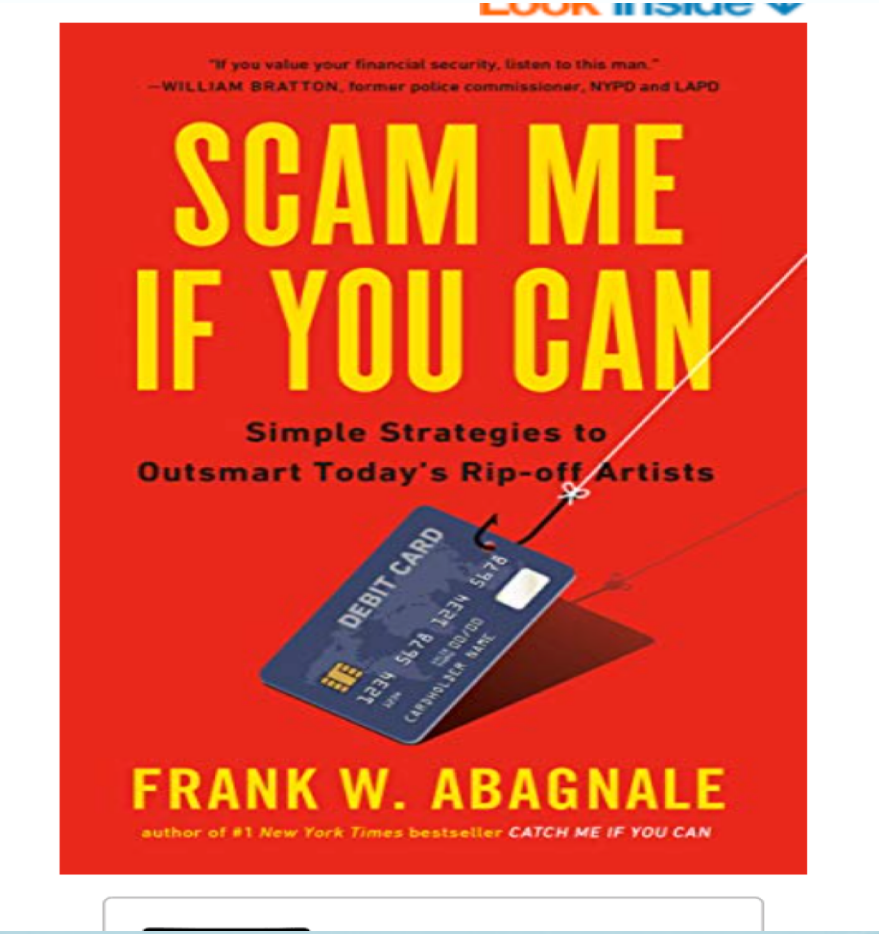
- In many cases, a scammer tells a victim they will be getting a call from a police officer — then spoofs the call that comes in a few minutes later, so that it appears to be coming from local police.
- The scam is having an impact on the ability of government departments to serve the public. They are being bogged down with phone calls from Canadians checking to see whether the calls they're getting are legitimate.
- **"It's hitting lots of Canadians," said Jeff Thomson of the Canadian Anti-Fraud Centre, who had 4 SIN scam calls on his own personal phone in one week.**

Why do we fall for fraud?

Many reasons why we bite

- **We like to believe we can get something for nothing. The word FREE is a huge motivator.**
- **We believe what our FRIENDS and relatives tell us. Sadly, fraud is often committed by people who prey on our friendship and trust to swindle us.**
- **Fraud artists are very convincing, with FAKE sites, ads and flyers the look just like those of real organizations we're accustomed to dealing with.**
- **Fraudsters FRIGHTEN us into not calling the police, government and our banks. This enforced secrecy helps crime go undetected.**

An excellent 2019 book



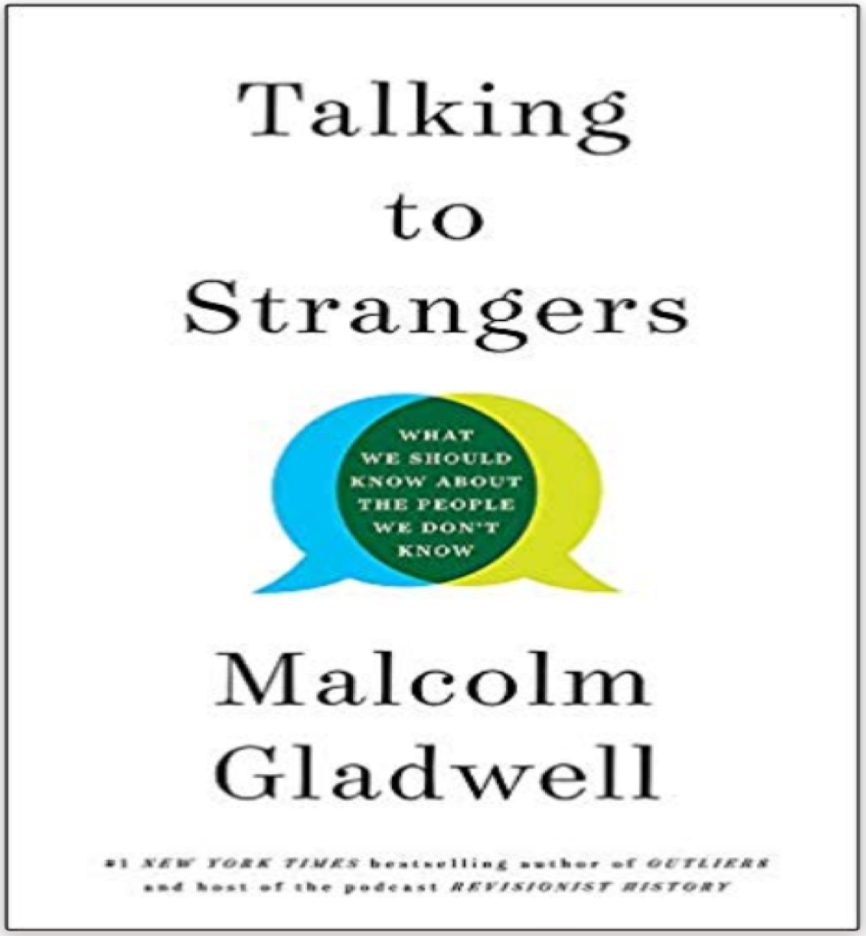
Who is scammed the most?

- **Frank Abagnale is a former U.S. con man and hero of a 2002 movie by U.S. director Steven Spielberg, *Catch Me If You Can***
- **"Believe it or not, millennials are scammed more often than seniors, because they give out their information so freely," he writes.**
- **"They give out their birthday and their place of birth, and that's all a criminal needs to get started.**
- **"But seniors lose more money."**

3 tactics used by scammers

- **Scarcity:** This dazzling deal disappears today!
- **Urgency:** Credit card payment is needed ASAP!
- **Flattery:** We only notify smart folks like you!
- **Abagnale says fraudsters become so immersed in the con that they believe whatever lie they're selling, making it easier to convince the victim**
- **They try to put you "under the ether," so you become irrational and drop your defenses**

Another book I like



Why we believe strangers

- **Malcolm Gladwell, a bestselling author and Canadian-born writer at the New Yorker magazine, says we have a lot of trouble knowing if strangers are lying or not**
- **We default to truth, an operating assumption that the people we are dealing with are honest**
- **We have an inherent belief in transparency, that we can "read" others like an open book**

Bernie Madoff is a good example

- **How did this U.S. money manager get away with his massive Ponzi scheme for so long?**
  - **No one could believe the truth and when some people did sound alarm bells, the authorities dismissed their concerns as too incredible**
- **Turns out that a large majority of us are pretty bad at spotting liars. Even supposed specialists in the field are not very good at it.**
  - **In a study, New York criminal judges scored as well as random selection when deciding who should or should not be granted bail**

New twist on old scam

Land lines vs. cellular phones

- **Police say scammers posing as bank officials call your home phone line and ask you to help them find fraudulent activity on your account.**
  - **You are told to buy things, usually gift cards, with a debit or credit card to help "bank officials" determine the difference between real and fake activity on the account.**
- **If you question the caller, you are told to hang up and call the phone number on the back of your debit or credit card to validate the call.**
  - **Because the landline does not terminate the connection when one person hangs up, the line is still open.**
- **When you hang up and call your bank, you're still connected to the scammer, who then answers the call as the bank and tries to get your personal data.**

Here's advice on call fraud

- Do not answer or call back any unknown calls, even if they appear familiar. Let them go to voicemail. Fraudsters rarely leave messages.
- If you do answer the call, do not respond to any questions asked by a recorded voice or a live voice.
- A legitimate financial institution will never call and seek your assistance in conducting an investigation, especially if the "investigator" requires you to make a purchase at the direction of the caller.
- Ensure the phone line has truly gone dead and wait for a dial tone before calling a verified phone number, especially if directed by an unidentified caller.

Perils of online shopping

The free trial scam

- You see a pop-up box at a company website (Costco, Bell, Rogers, Scotiabank, CIBC)
- You are asked to participate in a survey and promised an “exclusive reward”
- You get products, such as skin creams or diet pills, promoted by Dr. Oz or Oprah
- You must give your credit card information to pay a small shipping charge ($5)

What happens later

- Once you give your credit card information for a nominal payment, you are unknowingly signed up for a subscription
- You are trapped into making payments of $100 to $200 a month, which have not been properly disclosed
- Merchants will usually cancel when you call, but only give partial refunds
- Credit card issuers often refuse to help, despite zero liability for fraud guarantees

Buy online with a Visa card

Zero Liability Policy

Use your Visa card to shop anywhere--whether it's on the Internet or in a store--and you are protected from unauthorized use of your VISA card. The Visa Zero Liability policy eliminates consumer liability for fraudulent transactions.

No consumer liability on fraudulent transactions

The Visa Zero Liability policy provides you with protection against fraud**.

Should someone steal your Visa card number, you pay nothing for their fraudulent activity. This policy applies to any item purchased with your Visa card or card number including purchases made through the Internet.

If you notice fraudulent activity on your card, promptly contact your financial institution to report it.

It is important to continually monitor your monthly statement to identify any unauthorized transactions. Your cardholder agreement defines unauthorized transactions.

MasterCard has a similar policy

When you use your Mastercard, you're protected against fraud

As a Mastercard cardholder, zero liability applies to your purchases made in the store, over the telephone, online, or via a mobile device and ATM transactions. Have peace of mind knowing that the financial institution that issued your Mastercard won't hold you responsible for unauthorized use if:

1. you have used reasonable care in safeguarding your card, including not contributing to any unauthorized use, and safeguarding any related Personal Identification Number (PIN) or password; and
2. you report the loss or theft of your card immediately after becoming aware of it to your financial institution.

If you believe there has been unauthorized use on your account and you meet the conditions above, rest easy knowing you have the protection of Mastercard's zero liability promise.

Zero Liability does not apply to Commercial cards*, unregistered prepaid cards or gift cards.

Here's how it works

- To be reimbursed for an unauthorized transaction, you must take the following actions:
  - Immediately notify your card issuer when you become aware of an unauthorized transaction or when your card is lost or stolen
  - Keep your PIN confidential and never share it with anyone, including a family member
  - Avoid a PIN number someone could easily guess, such as a birthday or telephone number
  - File a formal complaint and wait for an investigation

Your right to an investigation

- **Financial institutions must always thoroughly investigate a disputed transaction**
  - **You need to report the incident within a short amount of time (60 to 90 days) and if not, you may not get the full amount back**
- **If you think your account was tampered with or is at risk of being tampered with:**
  - **Change your passwords immediately**
  - **Tell your credit card issuer of suspicious transactions**
  - **Check your credit file at Equifax or TransUnion for any credit you didn't apply for**

How to detect online fraud

- Scammers use email to “fish” or “phish” for your passwords and financial data they can use for identity theft
  - Also known as brand spoofing
- You can spot bogus email by placing your cursor or mouse over the link to see the URL or Web address
  - Don’t click, just hover
- Companies do NOT send you an email asking for personal information and telling you to open a link

The CRA extortion scam

"Dear Ellen, I am the next victim of the CRA scam," the man's email said. "If it is of your interest, we can talk. Maybe you will be able to protect others."

"Did you actually pay money to the fraudulent CRA people?" I asked.

"I have sent them over $60,000," the man replied.

Canadians are receiving a deluge of calls from fake Canada Revenue Agency collectors, warning that police would show up to arrest then after an audit showed they had a whopping tax bill to pay.

A recent story of a $5,000 loss

- **Tom Kane taught computer technology at Centennial College for 22 years.**
- **He was fooled by a phone scam, in which a menacing caller purported to be a member of the Canada Revenue Agency seeking back taxes.**
- **“I should be a smart guy. I wasn’t,” the 74-year-old told the Toronto Star.**
- **“It’s not just some frail, vulnerable people who fall for it. It’s also people who know better.”**

Warning signs of CRA scam

- **Calls typically originate from offshore, boiler-room operations in places such as India.**
  - **Check for accents, background noise**
- **Payment in Bitcoin has become more frequent, rather than previous payouts in iTunes cards and Western Union or MoneyGram.**
  - **No middleman with Bitcoin, very difficult to trace**
- **Kane received more than a dozen calls that day from 5 different people. All were excellent actors.**

The Canadian Anti-Fraud Centre

- **CAFC collects information on mass marketing fraud and gives it to law enforcement agencies**
- **Its phone number, 1-888-495-8501, has been spoofed by fraudsters**
- **If you are a victim of fraud, call the local police first. The CAFC's phone lines are jammed.**
- **Also, check the website to find information.**
  - **www.antifraudcentre.ca**

Emergency scam targets seniors

Roseman: Western Union ordered to repay 93-year-old scam victim

By **Ellen Roseman** Personal Finance Columnist
Fri., Sept. 21, 2012

Harry Zborowski is 93 years old. When he got a call from his granddaughter saying she had been in a car accident in Montreal, he agreed to send $4,200 to her right away.

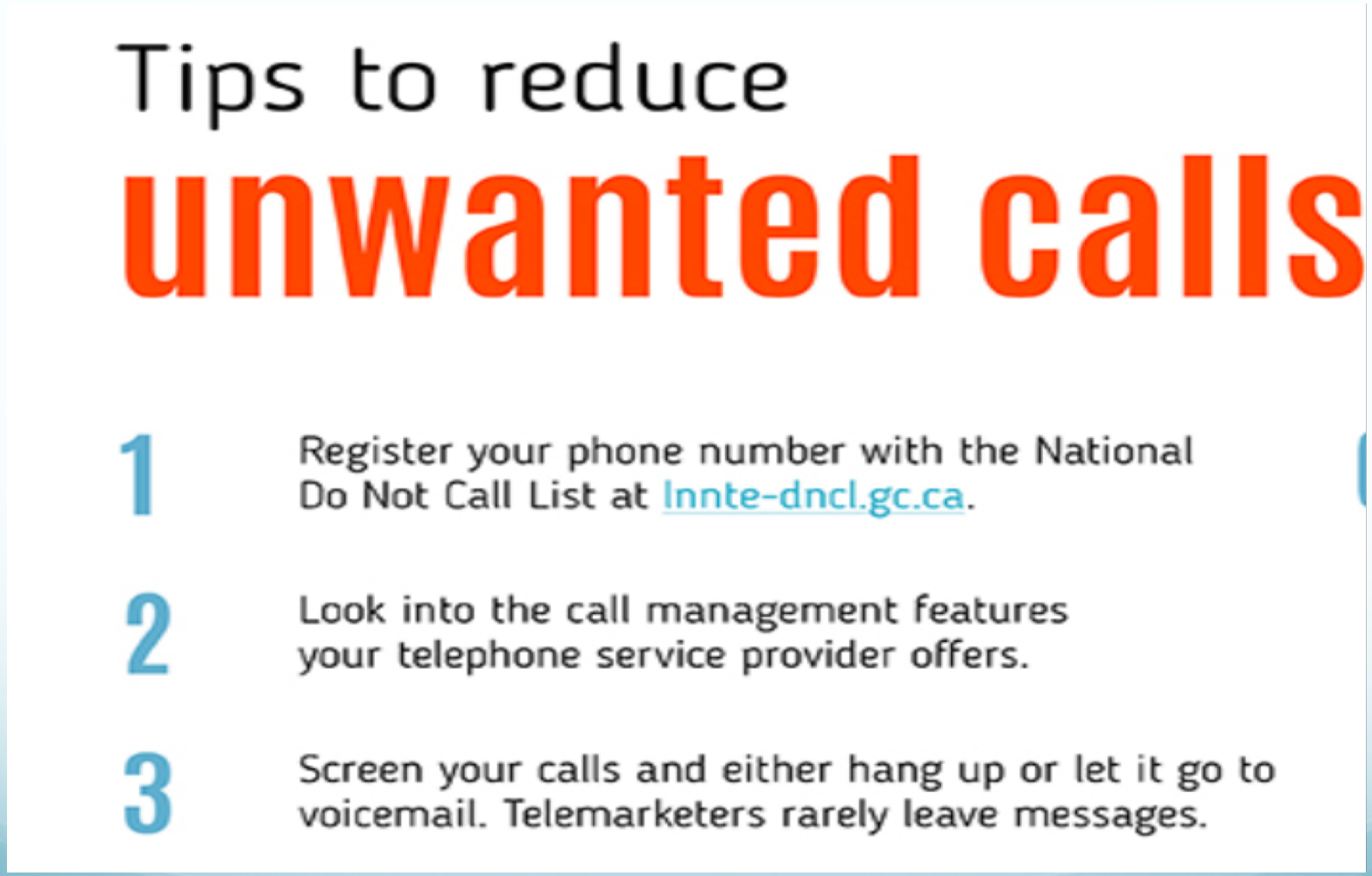
He went to Western Union, as instructed. But when his granddaughter called the next day to ask for more money to hire a lawyer, he became suspicious.

The Little Black Book of Scams from the Competition Bureau

Tips to protect yourself:

- Take time to verify the story. Scammers are counting on you wanting to quickly help your loved one in an emergency.
- Call the child's parents or friends to find out about their whereabouts.
- Ask the person on the phone questions that only your loved one would be able to answer and verify their identity before taking steps to help.
- Never send money to anyone you don't know and trust.
- Never give out any personal information to the caller.

CRTC infographic



More CRTC advice

4 Ask for your phone number to be added to the telemarketer's internal do not call list.

5 If you suspect a fraudulent call - DO NOT give out personal financial details or grant access to your computer. Best advice: HANG UP.

Door-to-door sales

- **Ontario banned unsolicited door-to-door sales of certain household appliances and services on March 1, 2018**
- **Rules apply to air cleaners, air conditioners, air purifiers, duct cleaning, furnaces, water filters, water heaters, water purifiers, water softeners**
- **These firms can only sell to you at home if you contact them ahead of time and invite them to your home for the purpose of making a sale**

Exemptions to Ontario's ban

- Telecom companies (federal jurisdiction)
- Some home maintenance services, such as burglar alarm systems, which receive fewer complaints
- Charities, which theoretically don't sell anything
- **What if you are pressured into buying without having contacted the business ahead of time?**
- **The contract is considered void and you can keep the goods and services with no obligations**

Help with door-to-door contracts

- **Cancel-It.ca** is a consulting company that provides non-legal consulting services to consumers stuck with home services equipment rentals
- Most contracts are for at least 10 years, it says
- At the end of the term, the equipment remains the property of the company and you will be forced to:
  - **Buy it out for "fair market value"**
  - **Continue paying the monthly rental rate indefinitely**
  - **Return the equipment to the company at your own expense**

Advice on investment fraud

- Learn about investing at GetSmarterAboutMoney.ca, sponsored by the Ontario Securities Commission
- Signs of investment fraud to look for
  - 1. You can make a lot of money with little or no risk
  - 2. You get a hot tip or insider information
  - 3. You feel pressured to buy
  - 4. They're not registered to sell investments
- Before you work with an advisor or dealer, check their registration.
  - Learn how at CheckBeforeYouInvest.ca

Please don't get scammed!

- **Here's how to contact me about deceptive tactics, and with complaints or questions:**

  - Website: www.ellenroseman.com
  - Blog: www.blog.ellenroseman.com
  - Email: ellen@ellenroseman.com
  - Facebook: www.facebook.com/ellenonyourside
  - Twitter: @ellenroseman