DATA BREACH/BANK FRAUD

In light of the National Public Database breach, in which the personal information of nearly every person in Canada and the United States was deeply compromised, I am offering this document to help people determine 1) if they were compromised, 2) how to react, and 3) action they can take to reduce future exposure.

1. Was I compromised?

a. Go to npd.pentester.com and enter your first name, last name, year of birth and the state(s) in which you have lived. The site will present a list of all the records that match the data you supply.

b. You may also go to www.haveibeenpwned.com to check but also sign up for emails about future breaches.

c. There will likely be scam artists who offer other websites in which you can allegedly check the breach data. To avoid those sites, use the URLs provided in the two paragraphs above.

2. How do I react to being compromised?

a. Contact Experian, Equifax, and Transunion (the three credit reporting agencies) and FREEZE your credit account. All of them will allow you to do it online and for free. DO NOT pay someone else to do it for you or pay for freezing your credit report. Remember to unfreeze your credit report if you need to apply for a loan or credit card.

b. Go to annualcreditreport.com to get a free copy of your credit report from each of the three agencies. Typically, you would not get all three at once (because you only get one free one per year) but instead reach out to a different agency every four months so you can keep a recurring eye on your credit report.

c. Contact your telephone provider (ATT, Verizon, T-Mobile) to prevent someone from calling to change your mobile phone number to their phone (called SIM jacking). Each has a different procedure…for more info, go to https://www.wired.com/story/sim-swap-attack-defend-phone/

d. Ensure all of your accounts have Two-Factor Authentication enabled. Ideally, you will use an authenticator app on your phone instead of SMS texts (to prevent the issue of SIM jacking) but any protection is better than none.

e. Change passwords to your online accounts, making them complex and random. Use a password manager like 1Password (that's what I use) to create and store your passwords for you. Apple is releasing a password manager with the next version of macOS that promises to be very good (and free).

3. How do I prevent/reduce the chance of this happening again?

a. Do not ever provide more data than you must for any accounts. Your doctor's office, for example, will ask for your SSN. Don't give it. They don't need it.

b. Never give account info to anyone over the phone UNLESS YOU CALLED THEM YOURSELF. If you believe it's a legitimate call, tell them you will hang up and call them back at the phone number listed on their company's website.

c. Consider signing up for a service like www.incogni.com which will, on your behalf and for a fee, reach out to all the companies recording this kind of data and use a legal power of attorney to have you removed from their databases.

These are only recommendations and do not represent a specific endorsement of any product or service. If you follow all these tips, you will reduce your exposure but in a digital world there is no guarantee. This is neither legal nor financial advice and you should consult a lawyer or financial adviser before you take action.

Bank fraud is out of control

The scams don't stop — and here's another one you need to know about. Your phone rings. It's a rep from your bank, and they're warning your account has been compromised. You're smart, so you immediately suspect it's a scam.

Then, the guy on the other end reads off your Social Security number and account info. Only your bank could know that, right?

Some 300,000 people in the U.S. thought the same last year. People lost their life savings; one Virginia woman had a whopping $700,000 wired out of her Wells Fargo account, and another in Los Angeles lost $100,000 in minutes.

📈 Why banking scams are rising

Bank scams used to be a niche operation. Now, anyone can buy the tools to con you for a few bucks on the Dark Web. There are even guides to make a phone number look like it's from *your* bank, including phony customer service reps to answer all your questions.

Pro scammers rely on social engineering, too. That's the fancy name for mind games to gain your trust. They love jumping on video calls because seeing a face makes you more trusting. They'll keep chatting with you so you miss the security alerts warning you to stop.

The big banks lost interest

Last year, the banks reimbursed scam victims at pitiful rates. JPMorgan Chase reimbursed 2% of transactions disputed as scams, while Wells Fargo reimbursed 4% of scam claims. Bank of America, meanwhile, reimbursed 24% of its scam dispute transactions.

Federal law requires banks to reimburse you only under certain circumstances, like if someone steals your phone and accesses your account. But if you're the one to sign a wire form or agree to an online transfer and you find out it's a scam, you're screwed.

💰 Keep your money safe

- **Slow down:** If a caller claims to be from your bank or asks for your account details, hang up. Call the bank yourself. Do *not* Google your bank's number; find it on their official website or the back of your card.
- **Beware of transfer scams:** Never send money via wire transfer, crypto or gift cards in response to unsolicited calls or emails. Your bank or the government will never ask you to transfer funds to a "safe" account.
- **Don't follow links:** If you're told to visit a website, download an app or click a link, it's a phishing site or malware installation.
- **Set up alerts:** In your banking app, you can turn on alerts for transactions over a certain amount or made in a foreign country, as well as notifications about suspicious activity like attempted logins from a new browser. I have all this set up. Some banks let you set transaction limits on withdrawals or purchases, too.