# SYNTHETIC IDENTITY FRAUD: Costing Consumers Billions

## MINDS ON

Fraud is an act of deception that sees a person profit financially or personally at the expense of another person or a company. Fraudsters generally lure their victims with promises of monetary, material or personal gain, or they find a way to misrepresent themselves to steal people's money or assets without them knowing.


Here are some common examples of fraud:

- **Identity Fraud** – Using another person's identity to commit fraud. i.e. using the name of a person who has died to apply for a credit card.
- **Debit and Credit Card Fraud** – When a criminal steals the information from a debit or credit card to create a duplicate card. A thief would need a "skimming" machine to commit this type of fraud. The machine is often capable of saving the cardholders PIN.
- **Phishing** – Using e-mail, text messages or websites to persuade people to give up personal information (such as a credit card number) in order to receive an incredible deal.
- **Prize Pitch (Lottery) Fraud** – Making people think they have won a prize and telling them they can only collect it if they send money to cover the taxes or administrative fees of the person or group offering the prize.
- **Cash Transfer Fraud** – Providing a sad story to a person in order to get them to send money to help another person or group in need.

*Source: The RCMP Internet Scams and Fraud Factsheet.*
*rcmp-grc.gc.ca/cycp-cpcj/is-si/osf-efel-eng.htm*

Based on these examples, and the definition of fraud provided, how careful do you need to be when it comes to protecting your personal information and assets? Does social media pose a particular risk to you being a target of fraud? How much personal information do you give out when you are online? Do you worry that you could become a victim of fraud?

## SETTING THE STAGE

It's a new kind of crime and it is costing Canada at least a billion dollars a year. Criminals have found a way to exploit loopholes in the Canadian government and banking systems to create fictitious identities which allows them to apply for and receive bank loans and credit cards. Eventually they default on the loans and max out the credits cards, and once the police come looking for them, they are nowhere to be found because the people they are looking for never existed in the first place. Introducing the even more evil twin of identity fraud: synthetic identity fraud.

## Identity Fraud vs. Synthetic Identity Fraud

Traditional identity fraud happens when someone underhandedly obtains personal information and assumes the identity of their target victim. They use a variety of methods to do this but the bottom line is the fraudster is pretending to be someone else (maybe you!) to acquire goods and services. The main problem for the identity theft victim is that, if they don't pick up on the fraud early, they could be on the hook for some of the things the scam artist purchases. This is hardly fair but it is the current state of affairs in Canada. Equifax (one of Canada's two credit bureaus) estimates that fraud-related crime costs Canadians between fifteen and thirty billion dollars a year.

A rising chunk of this stolen money comes in the new variation of identity fraud known as synthetic identity fraud. In this case, criminals fraudulently create a fake identity and proceed to use that persona to build a credit score. While regular identity fraud tends to focus on a short-term cash grab, synthetic identity thieves are usually in it for the long haul. They apply for multiple credit cards, pay their bills on time, take out loans and follow the lenders payment plan, register businesses — all this with the goal of biding their time until they cash out. This sometimes take place years after the synthetic identity was created.

## A particularly disturbing crime

What makes this form of fraud particularly disturbing is that the authorities really don't have a clue where to find the perpetrators. Synthetic identity thieves will often create multiple personas and run multiple scams at the same time. When the police catch on to the fraud, they will follow the information like they would in any other investigation, only when they arrive at the home of a synthetic identity thief


they are not going to find anyone because the person never existed in the first place. It is extremely clever and diabolically sophisticated. In most cases, all the police are able to do is shut down isolated accounts that represent a fraction of the overall synthetic identity scheme.

John Russo, the vice president and legal counsel for the credit agency Equifax, explains the difference between traditional identity fraud and synthetic identity fraud this way, "The difference is, I exist. The fictitious identity doesn't. So I'm able to complain to the police. I'm able to look at my credit report and see something suspicious is on my credit report that doesn't belong to me."* Russo goes on to say that the perpetrators of synthetic identity fraud are able to profit more easily because there are no actual people to complain about suspicious activity surrounding their credit history.

## Infinite mischief

This is particularly concerning to Canadian law enforcement. Toronto Detective Constable Mike Kelly describes synthetic identity theft as a process of "infinite mischief." He says, "There's literally no limit to the types of things, the amounts of things, the amount of damage that can be caused to each sector that you can possibly think of — banks, government bureaucracies, police agencies, insurance, car

lenders. Everybody."* With this far reaching crime, comprising thousands of phony identities, law enforcement agencies are struggling to bring synthetic identity thieves to justice.

## Terrorist connections?

Financial crime expert Kalyani Munshani warns Canadian that they need to be worried about more than catching a few criminals who are looking to make a few bucks. She believes that synthetic identity schemes could be used by terrorist groups to advance their agendas. "Using synthetic identities, safe houses can be established, cars can be rented, heavy vehicles can be bought, international travel can be facilitated, restricted goods can be bought without any flags being raised. This is not a conventional crime."** In other words, both the Canadian economy and the nation's security may be subject to attack by synthetic identity thieves.

*Sources:*

**How 'synthetic' identity fraud costs Canada $1B a year. March 3, 2014. cbc.ca.*

***Suspected terrorist links to synthetic ID fraud are being 'ignored.' March 4, 2014. cbc.ca*

## To consider

1. What is the difference between traditional identity fraud and synthetic identity fraud?
2. Why is it so difficult to catch the people who are running synthetic identity theft schemes?
3. What does Detective Constable Mike Kelly mean when he refers to synthetic identity theft as a process of "infinite mischief"?
4. How might terrorists use synthetic identity theft to plot against Canada?

Synthetic identity fraud represents almost 90 per cent of all identity fraud events. (cbc.ca)

# VIDEO REVIEW

## Pre-viewing

Synthetic identity fraud involves the creation of a fictitious persona to be used to defraud Canadian financial institutions out of huge sums of money. They create these fake identities by exploiting loopholes in the system. For example, synthetic identity thieves somehow manage to obtain driver's licences under fake names. These licences are seen as a high value form of identification that gives the synthetic identity thieves the opportunity to apply for credit cards and open bank accounts. By some estimates, as many as 200 000 fake driver's licences are in circulation in the province of Ontario alone.

1. Why is the existence of as many as 200 000 phony driver's licences a serious problem for the province of Ontario?

2. What should the government of Ontario do to put a stop to distribution of fake driver's licences?

3. It there are 200 000 fraudulent driver's licences in existence in Ontario, how might they be used to advance the criminal operations of synthetic identity thieves?

## While Viewing

1. Why were police baffled by the million-dollar fraud involving the cement trucks?

2. How did the scene from *Shawshank Redemption* shed light on the crime?

3. What is the "new twist" on the old scam?

4. What role did the "handler" and the "face" play in defrauding the Bank of Montreal?

5. What did police find in "Mr. Ali's" wallet when they eventually caught up with him?

6. What does Detective Kelly mean when he refers to "infinite mischief'?

7. How can synthetic identities be used to create synthetic corporations? Why do many observers view this as dangerous?

8. How were credit card rejections used by the fraudsters to further their efforts to create synthetic identities?

9. How much money were fraud investigators able to keep from getting into the hands of criminals? How much do they figure the criminals still manage to make off with?

10. How many driver's licences did the man who took on the fake identity "Server Froze" manage to get?

11. How many bogus Ontario licences does Detective Kelly think are currently out there?

12. Why does the Canadian government need to be very concerned about the acquisition of passports by synthetic identity thieves?

13. What nefarious assets can synthetic passports garner for people who are involved in criminal, and perhaps even terrorist, activities?

14. How is synthetic identity fraud a game changer that Canadian authorities are not prepared for?

15. Why is it difficult for Canadian authorities to track potential terrorists who might turn to synthetic identity theft?

16. How can this new type of fraud be used to further other criminal acts?

## Post-viewing

Kalyani Munshani, a financial crime expert, worries that synthetic identity thieves could be setting their sights on obtaining Canadian passports. This would be particularly lucrative for terrorist cells hoping to travel undetected under phony names with the help of a Canadian passport. Why is the cause for serious concern? What should Canada do to thwart the advancement of synthetic identity fraud? Is synthetic identity fraud a threat to national security?

# OFFICER KELLY AND THE SYNTHETIC IDENTITY THIEVES

## Minds On

There's an old adage: If it sounds too good to be true, it probably is.

If someone offered you $5 000 to apply for a number of driver's licences under a variety of different names — none of which were yours — would you do it? What if the person told you the scheme was legal and the chances of you getting caught were next to nil?

## Murad/Fraz Ali

Detective Constable Mike Kelly didn't know synthetic identity theft existed prior to June 2009. That's when a Toronto bank teller contacted the police and told them about a suspicious customer who had opened up two different accounts under two different names in a little under a month. Kelly picked up the suspect, and brought him to the precinct for questioning. That's when he discovered that the man had 21 pieces of genuine identification under the names Murad Ali and Fraz Ali. The ID included a social insurance card, a driver's license, two debit cards and four credit cards. None of them were forged — all of them were issued by legitimate Canadian government and banking institutions.

## Eager to tell his story

So how did this happen? The man who Kelly arrested was eager to tell his story. He said he was working at a doughnut shop when a man came in and told him he had a way for him to make some easy money. Life at the doughnut shop was not very lucrative, so he agreed to accompany the person - who police refer to as the "handler" - to a number of driver's licence offices in the Toronto area where he would acquire licences under false names. Later he would go with the handler to various banks and open up accounts using the driver's licence as his main form of ID. The handler promised the man $5 000 for each account he opened.

## Tempting Fate

However, the scheme came to an abrupt end when the man and the handler tempted fate - and that quick thinking teller notified the police. In the end, Kelly and a colleague embarked on a five-month investigation called Operation Mouse that led to the break up of a fraud ring that had stolen $25 million through its synthetic identity network.

And for the record, the handler never did deliver on the promise to pay $5 000 per account to the one-time doughnut shop employee.

## To consider

1. How did Detective Constable Mike Kelly get drawn into the world of synthetic identity fraud?
2. What types of identification did Muraz/Fraz Ali have on him at the time of his arrest?
3. How was the man drawn into the synthetic identity fraud ring?
4. What was the outcome of Operation Mouse?

## YOU HAVE TO PROTECT YOUR IDENTITY

Over 30 000 Canadians were victims of identity fraud in 2013 - up 30 per cent from 2010. That number is expected to rise in the coming year as fraudsters find new ways to steal the personal information of Canadians, destroying credit rating, and damaging the nation's economy in the process.

Here are a few ways to protect your identity:

- **Guard your social insurance number** – Never give your SIN number out to anyone unless you trust them. You need a SIN number to get a job and pay your taxes but you don't need to provide your SIN number to anyone who asks for it. You also do not need to carry your SIN card in your wallet. Find a safe place at home to store it and know that your SIN number is a valuable asset for identity thieves.
- **Get a credit report from Equifax or TransUnion** – If you are worried that someone may have stolen your identity, contact one of Canada's credit bureaus and ask for a credit report. This should show you if someone has been doing things like taking loans out in your name.
- **Check for suspicious mail** – If you start getting collection or overdue payment notices for things you didn't purchase, someone has probably stolen your identity. Suspicious mail is often the first clue that you are an identity fraud victim.
- **Look into credit denial notices** – If you are rejected when you apply for a credit card or loan, find out why. This may be a sign that identity thieves have been abusing your good credit rating and have started defaulting on payments.
- **Use an identity theft protection service** – Canada's credit bureaus (Equifax and TransUnion) provide monthly services that look for signs of identity theft. In 80 per cent of cases, these services can spot suspicious activity that may point to identity fraud.
- **Protect your personal documents** – You should store your old tax returns, bills, credit card statements and other personal information in a safe place. When you decide to throw them away, shred them. Identity thieves often steal personal information from the family trashcan on garbage day.

In the spring of 2014, the Canada Revenue Agency (CRA) shut down its website due to threats brought on by the "heartbleed" computer bug. It was eventually revealed that at least 900 Canadians had their SIN numbers stolen from the CRA as a result of vulnerabilities brought on by the "heartbleed" bug.

### Note to the wise

Many of you may be too young to worry about identity theft. Keep one important thing in mind: if an identity thief gets a hold of your SIN number, they can probably get your birthday off your Facebook page and your address off any number of online sources. With this information, they can assume your identity and start applying for credit cards. Guard your personal information while you are young!

## To consider

1. Are you concerned about identity fraud?

2. How do you think you can protect yourself against identity theft?

## Follow up

While some of this information may not apply to you because you are too young to have a credit rating, it certainly would apply to your parent or guardian. Review the different ways to protect your identity with your parent or guardian and see if they were aware of how vulnerable we all are to the devious ways of identity thieves.