Credit card fraud comes knocking in Bancroft

By Bill Kilpatrick

When most people think of credit card fraud, they often think of some key board warrior with a head set in another country stealing your information and using it to make online purchases or purchases in another country. People also often conjure up the phone fraudster who calls impersonating your bank trying to get personal information, but for one Bancroft resident, who wishes to remain anonymous due to safety concerns, credit card fraud landed right on their doorstep, literally.

Back in March they tried to place an online order at a business in town and received what they referred to as a ?weird error? and when they got home they started to receive emails, text, messages, and phone calls from people who claimed to be their bank. Instead of answering them, they instead called their bank's fraud line and sure enough their card had been compromised. The bank listed all the transactions that were attempted, went through all the security protocols, and informed them that the calls and text messages were indeed their bank attempting to get a hold of them.

?I don't answer those calls? the person told Bancroft This Week, ?I always call the number on the back of the card. I'm not gullible. I don't do this [get manipulated]. I don't save numbers online. I don't use Apple wallet. I don't trust anyone.? Until those phone calls from their bank, all of the previous calls, text messages, and/or email they have received regarding ?suspicious activity? on their card were fraudulent according to their banks fraud department. ?This was the only time that they were legitimate,? they said.

The bank canceled their card and they were sent a new card. No problem, crisis averted, and most importantly no money was lost. They received their new card about one week later and after completing three transactions at three different local Bancroft business their phone started blowing up again. ?I was like, ?What the hell?'? they said. The number on their phone was listed as their financial institution so they answered. The person on the other end was able to perfectly mimic the same lines and transactions that their bank had used only a week before. ?The reason I didn't hang up was because the conversation was the same as the one a week ago,? they said. ?All the little details lined up perfectly? and they were lulled into a what they called a ?false sense of security.? While they were skeptical at first, after 45 minutes the fraudster managed to convince them that things were legitimate, but they were not.

This false sense of security led the person to go to an online portal they were given by the fraudster where they changed their banking password, which was then changed again by the people posing as their bank. They were now locked out of their own account. ?Within 30 seconds they reset my password,? they said. The person posing as their bank also informed them that the RCMP was now involved because their card had been compromised twice in such a short time. The impersonator was able to put a so-called supervisor on the phone to confirm it. It was at this point that things took an unusual turn.

The fraudster told them that the RCMP needed proof that they were in possession of their card at the time of the unusual activity. They were told to cut the card in half, only once, and that a UPS person would be dispatched to pick it up. They said the UPS person would have a postage paid, pre-addressed, sealed envelope and that they were to place the cut card in it, sign it, and write a reference number on it and seal it. ?I was not given a reference number,? they told Bancroft This Week ?and looking back there were a number of red flags that I missed.? Three and a half hours later there was a knock at their door and they were confronted by a person that simply said they were there for a pickup.

The pick-up person appeared to not know what they were picking up, they were not dressed as a UPS driver, nor did they have an envelope, nor were they able to present credentials. They attempted multiple times to have the homeowner write their signature on their cell phone, but they refused. At this point the victim knew that something was up. ?I asked them where their envelope was? and when they went back to their vehicle they returned with a greeting card envelope.? The person then laughed at them and told them to leave. They then promptly called their bank, and called the police.

At this point the full gravity of the situation hit them ?I went into full panic mode,? they said ?This is on my doorstep. I don't know if he's got a gun. I don't know if he's got a knife.? The person was just glad that they had a partner and some large dogs, that they

believe helped pursued the person to leave when asked. ?What if I was a senior or a single person with no pets? Where might that have gone? they pondered, obviously still upset by the whole situation.

When contacted regarding the incident, the Bancroft detachment of the OPP's media officer Daniel Cook said that there was not an update on the incident as of yet, but he did have some suggestions for people. Cook said that the OPP ?recommend not giving out personal information to anyone who calls you or reply to emails from unknown parties. If people are ever suspicious of an email or phone call we recommend them hanging up the phone and calling a known phone number for the business they are claiming to be. Also trust your gut, if something doesn't feel right and they believe it to be a scam stop what they are doing and report it to the Canadian Anti Fraud Centre.? Cook also pointed out that the Canadian Anti Fraud Centre has multiple resources that can help people recognize current and past scams.

This credit card fraud case speaks to the increased sophistication and organization that fraudsters are using to try and steal your information and money. The reason? Fraud continues to be a lucrative business that cost Canadians some $638 million in 2024 up from $578 million in 2023 according to the Canadian Anti-fraud Centre. Despite the Bancroft resident's due diligence to avoid fraud, circumstances made the fraud more likely and they let their guard down, but thankfully the worst thing that happened was that their accounts were inaccessible for about a week.

Jeff Horncastle, a fraud expert and spokesperson for the Canadian Anti Fraud Centre pointed out that ?We've seen deep impacts [beyond just monetary loss] on victims across the board with all types of fraud now because of how sophisticated scams are getting? adding that ?scams of any kind can lead victims to experience feelings of betrayal, anger, and sadness, especially if the scam involved an emotional connection such as what happens during a romance scam. For some, this can lead to feelings of mistrust and hopelessness, anxiety, depression, or post-traumatic stress.?

While the Bancroft resident mentioned lingering feelings of insecurity, they did not feel any shame and said that ?people needed to know? so that they might be able to avoid the same scam. Their advice for people who might suspect that they are being scammed was to hang up the phone, and use a different phone to call their banks fraud line, keep a small amount of cash on hand, and utilize anti fraud and identity theft services such as Equifax or Transunion. Their main message: don't let your guard down because if it can happen to me, it can happen to anyone.

The Canadian Anti Fraud Services can be reached online at https://antifraudcentre-centreantifraude.ca/index-eng.htm