STOPPING AN EMPLOYMENT SCAM

"This story begins when one of our members brought in two cheques for a few thousand dollars from financial institutions in (another province).

The member wanted cash for nearly five thousand dollars. This member who works in the service industry receives the majority of incoming funds through direct deposit, so bringing in two unfamiliar cheques for this amount was not within the members normal account activity. One cheque was from a well-known financial trust company, and looked like it could have been legitimate. When asked from whom she had received the cheques, the member explained that they were from a new employer, and that the member was hired over Skype for a nanny job in Montreal, which was to start the following week.

The member said the cheques were sent from someone in Montreal, whose family would soon be arriving in Canada from Mexico. The member was instructed to buy furnishings for their house, and ship them to an address in Montreal. The MSR told her gently that she thought it was a scam, by leading with the fact that it logically doesn't make sense that she would be getting paid for any work that she had not yet done.

The MSR explained how this scam worked, and the member agreed that had the cheques been cashed, the member would have lost thousands of dollars! The MSR made photocopies of the cheques as the member wanted the originals to take to the police.

What's interesting about this case is that this member was going to be moving to Montreal the following week regardless of this fraud. The MSR asked if the member had mentioned the relocation over social media, and the member said yes. These fraudsters thought that the member would be an easy target for this scam, because they already knew about the move. Luckily this fraud attempt was thwarted and the member was saved a lot of grief and money."

STOPPING FRAUDULENT WIRE TRANSFER

"We have a commercial member who regularly sends large wire transfers to suppliers in China & Hong Kong.

He generally initiates these wires via e-mail and includes a copy of the PO order which contains the total amount and banking info for the supplier.

One day I received an e-mail from him requesting a wire for $75,000 to a new supplier in Hong Kong - this is not a usual amount for our member to send.

The email was worded very similar to the emails I generally get from my member and even included a PO that looked very similar to those my member usually sends.

Luckily our credit union has implemented a policy where all wires must be signed by the member and verified by phone if initiated remotely. When I sent the wire form back to my member for him to sign, he called to ask what this was for, as he had not sent the email.

When he looked back into his sent history, he saw the outgoing email to me, but he had not done it. He had been hacked. He then had to have all his computers wiped clean and changed his email address. Thanks to our credit union's verification policy, this wire was stopped from going out."

STOPPING A LOTTERY SCAM

"In December of last year, a long time member of mine made an appointment to see me for a loan. It was just before Christmas and she was very excited about an opportunity that had recently presented itself.

When I asked her the purpose of the loan, she said it was to pay for courier fees to have her lottery winnings delivered to her, approximately $7,000.00. Right away I told her that I felt this was a scam, that you never have to pay to collect winnings, but she persisted. She said that she had won through Facebook and that her cousin had also won so she knew it was legit.

I asked her if she recalled entering any lottery, she didn't, but was still optimistic that this was for real. I told her that I couldn't give her the loan and convinced her to dig a little deeper. She finally admitted that she hadn't actually spoken to her cousin, that she had only had contact through Facebook.

I suggested that she contact her cousin via telephone and also contact the RCMP to get their take on it. I also advised her to stop communicating with this person and to change her privacy settings on her Facebook.

About a week later she came into the branch together with her husband to thank me for talking her out of borrowing the money.

She had really wanted to believe it was a legitimate winning because she and her husband have a very large family and they wanted to get everyone a nice present for Christmas, but she could now see that it was a scam.

As bad as I felt bursting her balloon during that first meeting, I was ultimately glad that I could prevent them from losing money."

For More Tips On Protecting Your Money Visit www.svcu.mb.ca

FRAUD Prevention

Credit Union Success Stories

swan VALLEY CREDIT UNION

Falling victim to fraud can have a devastating effect on a member and on their family.

Many frauds are designed to steal money by emotionally abusing people.

Fraudsters create fictitious scenarios where people believe that a family member has been hurt or has been arrested and placed in jail.

Other schemes will lure a person into a fraudulent romance.

As a credit union, we have a unique opportunity to protect our membership from having to endure the hardships that these frauds can cause.

Take a closer look at the many types of fraud that Credit Unions have prevented.

Thank you CUMIS *for compiling these stories.*

STOPPING AN IDENTITY THIEF

"Last year, I was reviewing one of our Conditional Sales Agreements and came across a fraud warning on the client's credit bureau. I followed the instructions and called the number indicated in the warning and left a message for them to call me back.

Since the warning had been registered the month before, I took it very seriously. I advised our broker of the situation, as it would take longer for us to provide an answer as we needed to clarify this warning.

Not long after, I received a call from a gentleman claiming to be the loan applicant. I started asking him very simple questions about his personal information which he gave without hesitation. Then I simply asked that he confirm the telephone number where I had left the message for him to call me; this is when the person started saying that it was an old number and he didn't remember what it was.

I found this very strange so I asked him how he knew to call me; he replied that when he called the dealer for an update on his file they told him that we were waiting for his call in order to confirm some more information.

While talking to this gentleman, my co-worker came in saying that another gentleman was on the other line claiming to be the same loan applicant. I proceeded by putting the current gentleman on hold and spoke with the new entleman. I asked him the same questions, which he replied without hesitation and even added additional information about his credit bureau that I didn`t ask. He was even able to provide me with the telephone number that was left in the fraudulent warning on his credit bureau. He then informed me that someone had stolen his information and was going around applying for loans in his name. I advised the gentleman to contact the police immediately.

During this conversation, the first caller had hung up the phone. That gave me time to contact our local police to see if we could do anything. Unfortunately they advised us that it's not their jurisdiction however they strongly recommend not approving the loan! Not long after, the fraudulent person called again to see what was happening with the application. I proceeded to tell him that I didn't believe he was who he said he was. This ended up with a lot of rude comments on his part and him telling me that I was not doing my job properly and that he could prove that the social insurance number belonged to him. I asked him to fax me a copy of his most recent tax return and he responded 'No problem, I'll have it faxed to you within 30 minutes' and ended the call.

Long story short, I never received a fax or heard from him again."

STOPPING A ROMANCE SCAM

"A well-known member of ours had recently lost his wife to cancer. About 3 months after she passed away, he was wanting to send a WIRE for around $8,000 after depositing funds from a recent cattle sale. He had never sent a WIRE before and the name of the company he wanted to send it to seemed suspicious.

At first I asked him if he could leave the info with me and I would do up the transfer and then he could come back in about a half-hour to complete the transaction. Once he left I searched the company name on the internet and found out that it was a dating site. I immediately knew this was probably some sort of scam.

I called the member to get some more info on the purpose of the WIRE. He told me it was a dating site and he was told that when he sends these funds they had a match for him that would contact him. I told him I was not able to do the WIRE that day and that I felt that a dating site should never be asking for anyone to send money in order to match you up with a mate.

He was not convinced and was still focused on meeting a mate. I asked him to think on it and maybe talk to someone he trusted about their thoughts before completing this transaction.

He came back to me the next week after talking to his sons and a lawyer and agreed that it was a scam. He thanked me for looking after him and saving him from losing his money. He also came back about 6 months later to introduce me to his new girlfriend whom he met on a safe dating program his sons had helped him find."

STOPPING VULNERABLE PERSON ABUSE

"One of our members is legally blind and has a home care aide help her when she comes into the branch.

One day the member came into the branch alone and the MSR (Member Service Rep) thought that was strange. They asked her where her aide was and she told the MSR she had a new one and he was waiting outside.

The member proceeded to ask for five thousand dollars in cash and when the MSR questioned why she needed that much cash, the member told the MSR her aide told her she needed new furniture. The MSR suggested she talk to me first and brought her to my office. I suggested to the member to bring in the aide so I could talk to him before we release any funds.

The member went outside and asked him to come in and see me but he refused and took off. The member came back in to let me know so I told her that that individual was a fraud. We called the agency and told them what happened."

STOPPING AN EMERGENCY SCAM

"(Our credit union employee) had a member inquire about sending a wire to their son. He told her he preferred Western Union, so he was withdrawing the funds in cash to go offer to a local Western Union location. (The credit union employee) knew this was not typical of our member, so she suggested that she do the wire here at our branch, all she needed was some additional information.

The member said that it was a very personal matter and he didn't want to reveal any details. (The employee) could tell that the member was very distressed, so she pressed him again to explain what the issue was.

The member admitted that he had gotten a call from his son and that his son had been involved in a car accident. His son was injured and had broken his nose, and that is why he sounded so different. The son explained that he was arrested and needed money wired to his lawyer to get him out of jail. The son further explained that he didn't want his Dad to call his wife, or tell Mom as he was embarrassed and didn't want to worry them.

(The credit union employee) was aware that this sounded very much like a scam that had been circulating in our area. She explained to our member that she thought he might be a victim of an impersonation scam. The member is a senior (but a very savvy senior - on line banking, well recognized in the community and very active) and he told her that he was aware of these type of scams, but he was very worried that it might be true.

(The credit union employee) suggested that she make a call to the son's home, and ask for the son. No one needed to know why she was calling and they could move on from there if they needed to. The member was relieved for the suggestion and gave (the credit union employee) the number for the son's home. (The credit union employee) placed the call and you can guess who answered the phone! The son was at home – unhurt - and quite happy to let his Dad know that all was well.

So thanks to several actions by (the employee), noticing a non-typical transaction of our members, keeping up to date on potential frauds circulating and some persistence in resolving member's concerns, even though it meant asking some personal questions, she prevented the member from giving his money to the criminal enterprise."

Credit Union Employees, annually receive training on how to identify all types of fraud, money laundering & privacy breaches to protect our members & their investments.