RCMP·GRC
ROYAL CANADIAN MOUNTED POLICE • GENDARMERIE ROYALE DU CANADA

EMERGING TRENDS: Fraud Activity and Victimization in New Brunswick

Date: September 2, 2020

Background:
Criminal organizations are known to exploit victims in order to obtain their personal information and monetary instruments namely; gift cards, fiat currency and crypto currency. Threat actors continue to modify methods and tactics to exploit victims, utilizing local dynamics such as government assistance programs, and using methods to establish a sense of trust/authenticity. Threat actors are using cyber enabled methods to carry out the victimization and traditional methods such as telephone and pre-recorded messages. The Canadian Anti-Fraud Center released a report stating there was an increase in personal information reports using the name of Service Canada.

Summary:
In June and July 2020, over 260 occurrences of fraud and identity theft cases reported to the J Division RCMP resulted in monetary loss or the disclosure of personal information by the victims. The monetary losses for those two (2) months alone are estimated to total over $428,000, which include $88,000 attributed to loss by commercial businesses and $340,000 to monetary loss by individuals residing in New Brunswick.

Fraud activity involving threat actors claiming to be representatives of legitimate government agencies represented the greatest victimization against citizens of New Brunswick. This type of fraud along with social media related fraud, identity theft and banking fraud, represents 72% of fraud related victimization in the province.

Fraud Activities:
The top eight (8) reported frauds, representing 85% of the activity, can be categorized as follows:

- **Claims to be a representative from a legitimate Government agency** – A number of extortion related frauds involve actors asserting they are contacting the victim from a government agency, including; Service Canada, Canada Revenue Agency (CRA), Immigration Canada, Service New Brunswick, the Justice Department and other Law Enforcement entities. A number of reports involve call spoofing, where the local RCMP detachment phone number is displayed on the victim's phone, and they are told there is a warrant for their arrest. Actors attempt to obtain personal information from the victim including; social insurance numbers, date of birth and address. To conduct this fraud, the actors call the victim and inform them they will be receiving a call from the local RCMP detachment shortly. Then within minutes the victim receives a call from an actor impersonating an RCMP officer, and the local RCMP phone number displayed on the victim's phone. The actors then attempt to extort funds from the victim in the form of gift cards,

bitcoin or other monetary instruments. Threat actors are aware of the locations of bitcoin machines in the province, and have directed the victims to attend these locations to deposit the monies.
***Attempts**: 377, **Victims:** 112, **Amount extorted:** $73,714*

- **Social Media** – This type of fraud includes occurrences where actors use a number social media applications to extort money from victims. Their tactics include using fake websites, exploiting personal relationships, or compromising the personal social media account(s) of victims in order to ask their associates for money. In a number of instances, a social media platform is used to first build a relationship, then used to obtain money from the victim. Additionally, there are a number of occurrences where the actor will request that the victim deposit a cheque into the victim's bank account, then transfer the money to the actor. The cheque is later deemed fake by the bank.
  ***Attempts**: 56, **Victims:** 34, **Amount extorted:** $66,115*

- **Commercial Banking** – In this category, victims are identifying unusual activity involving their bank accounts, such as unauthorized e-transfers from their accounts. In a number of instances, the victims reported the transactions after clicking on links advising them of an e-transfer. Additionally, victims have reported received calls from persons claiming to be from the security department of the bank, advising them they need to withdraw money and purchase monetary instruments to protect their account or to assist police in their investigation.
  ***Attempts**: 34, **Victims:** 24, **Amount extorted:** $39,356*

- **Credit Card** – Victims are receiving calls from actors stating that are from the credit card company and that fraudulent charges have appeared on their credit card. The actors then attempt to obtain personal information from the victim as well as monetary instruments such a gift cards.
  ***Attempts**: 24, **Victims:** 7, **Amount extorted:** $1,251*

- **Identity Theft/Fraud** – In this category, victims report changes were made to their personal government accounts, such as the CRA, without their consent or knowledge. In a number of instances, the victim's information was changed so the actor is receiving government assistance, such as CERB or EI, under false pretences. In many of these cases, there was no monetary loss associated to the victim, however a breach of personal information would have occurred. The Government of Canada recently announced three (3) cyber attacks that resulted in over 9,000 accounts being compromised at CRA and other government agencies. The attacks were classified as "credential stuffing" where threat actors would use passwords obtained from previous breaches, knowing that users may reuse passwords across various websites. [i]
  ***Attempts**: 23, **Victims:** 20*

- **Lottery/Loans** – Actors inform the victim they are the winner of the lottery, however to receive their winnings they must pay an amount, usually described as a tax. A similar Modus Operandi is used when victims apply for loans online, requiring a prepayment using various monetary

instruments.
***Attempts**: 15, **Victims:** 6, **Amount extorted:** $24,225*

- **Business Fraud** – This fraud category includes instances where legitimate businesses are victims of credit card scams resulting in substantial losses to the companies. Another variant of this type of fraud includes cases where businesses are the victim of supply chain fraud, resulting in the non-delivery of goods.
  ***Attempts**: 14, **Victims:** 9, **Amount extorted:** $88,742*

- **Employment Fraud** – This fraud includes instances where victims receive a job offer and as part of their employment are directed to deposit cheques into their account and transfer the monies using monetary instruments including bitcoin, gift cards, or other bank accounts. In each instance the cheque is deemed fraudulent.
  ***Attempts**: 9, **Victims:** 5, **Amount extorted:** $35,734*

Repeat Victimization:
Fraud victims may experience repeat victimization, specifically in those instances where their personal information was obtained. This is often attributed to personal identifiers such as social insurance number and date of birth; however, the theft of email addresses and passwords can be equally as troubling. The recent cyber attack reported by the CRA is an example of repeat victimization. It is believed passwords were compromised in an unrelated cyber attack, then used to gain access to the CRA accounts. In a number of frauds reported to the J Division RCMP, the complainants indicated personal information had been breached months prior.

[i] CRA shuts down online services after thousands of accounts breached in cyberattacks, Aug 17, 2012, https://www.cbc.ca/news/politics/canada-revenue-agency-cra-cyberattack-1.5688163