Description and Associated Definitions of Canadian Anti-Fraud Centre (CAFC) Statistics

Fraud and Cybercrime Thematic Categories

- Bank Investigator Fraud: Fraudster calls you to ask for help to catch a bank employee who has been stealing money; or, alternatively claims to be helping you to solve suspicious transactions on your bank account.
- Charity/Donation Fraud: Fraudster contacts you to ask for a donation to a charity, association, federation or religious cause. Frequently, the fraudster uses high-pressure tactics to motivate you to donate immediately.
- Collection Agency Fraud: Fraudster contacts to demand a payment for a non-existent debt.
- Counterfeit Merchandise: Fraudster uses websites that have the same look and feel as a legitimate manufacturer to sell knockoff products at large discounts. Products are inferior and can pose significant health risks.
- Directory Fraud (Subsection of False Billing Fraud): Fraudster calls a business to confirm details such as the company's address and telephone number. After this is confirmed, the fraudster sends an invoice asking for payment for a directory listing or listing renewal.
- Emergency Fraud: Fraudster claims to be someone you know or knows someone you know, and tells you that they need money immediately.
- Extortion: When someone unlawfully obtains money, property or services from a person, entity, or institution through coercion.
- False Billing: Receipt of an unsolicited invoice and demand for payment, where no product or service was requested.
- Foreign Money Offer: Fraudster contacts you asking for help to transfer a large sum of money from one country to another. The requests often appear to come from a lawyer or legal entity. This fraud is also known as an inheritance scam or fake business proposal.
- Fraudulent Cheque: Fraudster sends a cheque, with a request to help cash the cheque. Prior to cashing the cheque, the fraudster requests that you return a portion of the funds.
- Grant and Loan: Fraudster uses websites that look like official sites to attract people from looking for grants or loans. This includes government grants, weight loss grants and loans.
- Health: A now-disused fraud pitch previously used by the CAFC to define fraud with a nexus to health-related themes. This category has now been divided into more appropriate pitches.
- Identity Theft and Fraud:
    - Identity Theft: Fraudster steals someone's personal information for criminal purposes;

    - Identity Fraud: Fraudster or criminal uses previously stolen personal information, usually to commit another crime.
- Incomplete (Report) / Unknown: When an individual files a report with the CAFC, but does not classify the type of fraud or give sufficient detail to classify the type of fraud.
- Investment Fraud: Any solicitation for investments into false or deceptive investment opportunities.
- Job: A generic category of fraud targeting individuals looking for a job. This may be through the recruitment of a nonexistent job, and is frequently connected to fraudulent cheque fraud.
- Merchandise: Fraudster create fake ads and post them on classifieds sites, resale sites, website pop-ups, and fake company websites.
- Modem-Hijacking: When a cybercriminal remotely accesses an individual's computer for the purposes of committing additional cybercrime or the theft of money.
- Office Supplies: Related to false billing fraud, a fraudster may pretend to be the usual office supplier or offer supplies at a discounted price. Once the business confirms an address, they may send unsolicited business supplies, along with an invoice.
- Other: When reporting a fraud occurrence, this category is for any other form of fraud that may not be accurately described by any other category of fraud.
- Personal Information: Fraudster, while impersonating a business, government agency, bank or utility company, urgently requests personal information. Once this information is acquired, the fraudster uses said information to commit identity fraud.
- Phishing: Fraudster uses techniques to convince someone to give personal information or clicking on links.
- Prize: Fraudster notifies you that you have won, or have a chance at winning, a prize or lottery. If you respond, the fraudster will state that before receiving any winnings, you must pay an advance fee or buy something.
- Psychics: Deceptive offer received through mail, email or online offering psychic services.
- Pyramid: Fraud that focuses primarily on generating profits by recruiting other investors. The fraud may offer products, but they usually have very little value.
- Recovery Pitch: After an individual is victimized by fraud, a fraudster may target the individual again with the promise that they can recover the previously lost funds.
- Romance: A fraudster convinces an individual to enter a virtual, online relationship so that the fraudster can gain trust and affection. Once this relationship is created over a span of time, the fraudster may ask for money, to join a business venture, or invest in a company or cryptocurrency.
- Service: Fraudster contacts individuals and offers unsolicited and nonexistent services for a fee or to obtain personal information.

- Spear Phishing: Fraudster pretends to be from a legitimate source, to convince individuals or businesses to send them money or provide personal information.
- Spoofing: Subsection within spear phishing.
- Survey: Fraudster contacts individual to participate in a fraudulent survey, for the purpose of obtaining personal information.
- Timeshare: Fraudster lures an individual with free stays at a timeshare in exchange for agreeing to sit through a presentation about the timeshare. If a timeshare is purchased, fraud can include hidden booking or maintenance fees, or the company disappearing once they secure a deposit.
- Unauthorized Charge: When a legitimate or fraudulent business obtains the banking or credit card information of an individual, and applies a fraudulent or unauthorized charge to the individual's account without the exchange for a product or service.
- Vacation: Fraudster uses an automated call to tell that the individual has won a free or discounted vacation. If the individual tries to claim the vacation, the scammers ask for personal information or a deposit prior to booking the trip.
- Vendor: Connected to merchandise fraud, a fraudster will claim to be out of town or unable to pick up the product, requesting that the individual mail the item instead prior to paying for the product.

Additional Definitions and Descriptions of Dataset Abbreviations

- **CAFC**: Canadian Anti-Fraud Centre
- **NCFRS**: National Cybercrime and Fraud Reporting System
- **Solicitation Method**: The initial method of contact between the fraudster and victim.
- **Cases**: Number of instances that the fraud has occurred against the reporting victim/complainant
- **Complaint Number**: The catalogued and unique number given to each CAFC report for the purposes of maintaining the report database.
- **Complaint Received Type – CAFC Website**: A report received through the CAFC's Online Reporting System.
- **Complaint Received Type – Phone**: A report received by the CAFC through the victim reporting by telephone at 1-888-495-8501.
- **Complaint Received Type** – Email: A report received by the CAFC by email.
- **Dollar Loss**: Total amount of money lost to the instance(s) of fraud.
- **Fraud and Cybercrime Thematic Category**: Type of fraud experienced by the reporting victim, selected through a drop-down list on the CAFC Online Reporting System, or by submitting a description of the fraud to a CAFC intake analyst in a telephone report.
- **Victims**: Total number of victims associated to the reported instance(s) of fraud.

Additional Questions

- **Why do so many reports have a dollar loss of $0?**
    - Reports concerning identity fraud, personal information theft and fraud, and phishing have a universal dollar loss of 0, because the dollar loss is inaccurate or impossible to accurately determine. For these forms of fraud, the losses are either absorbed by an identity other than the reporting victim (e.g. a financial institution), or actually occur at a later date from the initial fraud. For example, the information stolen in a personal information theft may be used in additional forms of fraud or sold to commit additional fraud and cybercrime.

- **Why does the category "not specified" have many reports and losses?**
    - When reporting to the CAFC, individuals have the option of offering as many or as few details as they choose, and the CAFC also receives anonymous reports. However, the CAFC only validates reports that have a nexus to Canada, and the majority of reports are filed by Canadian victims.

- **What form of currency is reflected in the dollar loss?**
    - Prior to inputting into the system, all dollar valuations are converted into CAD.

- **How is this dataset obtained?**
    - All CAFC fraud and identity crime reports are contained within the CAFC Fraud Reporting System database after a review by CAFC analysts, which produces data exportable to spreadsheets.

- **How accurate is this data?**
    - As data is acquired from total public reports, online reports are created by the public entering information to populate their individual reports. The accuracy of a fraud report is largely dependent on the individual submitting the information. Individuals submitting reports can choose to include as much or as little information as they deem necessary. Nonetheless, CAFC intake analysts review all submitted reports to determine accuracy of submitted information.

- **How can I request more data from the CAFC?**

- The CAFC is currently working on new methods of producing publicly-available fraud and identity crime reporting data, in addition to working with the RCMP's Open Government Office. Initiatives to make this possible are ongoing.

- **What is the National Cybercrime and Fraud Reporting System (NCFRS)?**
  - The NCFRS is the new cybercrime and fraud reporting repository being developed by the CAFC and National Cybercrime Coordination Centre (NC3). A prototype, the NCFRS currently receives a small number of reports diverted from the CAFC Fraud Reporting System (FRS) as an ongoing and daily test sample. The public can also access the NCFRS by following this link: National Cybercrime and Fraud Reporting System