Reference number: FINTRAC-2019-OA001
April 2019

Laundering of the proceeds of romance fraud

Issued in partnership with the Canadian Anti-Fraud Centre

Romance fraud involves perpetrators expressing false romantic intentions toward victims to gain and then take advantage of their trust and affection in order to access their cash, bank accounts and credit cards. The Canadian Anti-Fraud Centre has found that romance fraud victims account for some of the highest dollar losses per year from mass marketing frauds in Canada. However, romance fraud is one of the lowest reported types of mass marketing fraud, because victims can be ashamed to come forward, or may be unaware or unwilling to accept that they are a victim.

The laundering of the proceeds of romance fraud largely resembles that of other types of mass marketing fraud. However, reporting entities—front-line employees, in particular—must be aware of contextual factors that both suggest clients are victims of romance fraud and might not be apparent from reviewing transactions alone. To that end, reporting entities, particularly financial entities and money services businesses, should consider the indicators set out below that relate to both victims and the transactions perpetrators of romance fraud carry out in combination with the indicators of mass marketing fraud listed at the end of this document. FINTRAC uses these indicators, along with other context and facts, to assess reporting entities' compliance with their suspicious transaction reporting obligations.

Victims

Generally, perpetrators use fake profiles on social media or online dating sites—set up with stolen photos, and fictitious names and occupations—to contact possible victims. Once trust is established, perpetrators request financial assistance. Although the specific reasons perpetrators give for needing funds vary, they tend to focus on life-or-death medical emergencies, being unable to access their own money in a foreign jurisdiction (e.g., their bank account is frozen or their wallet lost or stolen), fees imposed by an international authority (e.g., taxes, customs or legal fees) and/or money needed to obtain more money (e.g., investments, inheritance fees, work equipment, wages). Reporting entities should be particularly attuned to clients telling hard-to-believe stories about why they are conducting certain transactions.

Indicators relating to romance fraud victims

- Client met the individual they are transacting with on a social media platform, via email or on a dating website.
- Client always, or almost always, communicates with the individual they met online by email or text.
- Client has never met or has never seen the individual they are in the relationship with, and is often older than that individual.
- Client relays a confusing, conflicting or non-believable story about why the funds are needed or the transaction is taking place.
- Client is at a potentially more vulnerable stage of life (i.e., a senior or widowed, separated or divorced).
- Client provides minimal or inconsistent information and/or avoids answering questions about the purpose of the transaction.

Transactions

Romance fraud generally involves victims carrying out transactions that do not fit their profile, including sending funds directly to individuals to whom they have no apparent connection. This type of fraud may also feature sudden increases in wires/email money transfers (EMTs). In some instances, victims sell or pool assets to fund transfers to perpetrators and/or third parties, sending increasing amounts over time as perpetrators gain their trust. These funds are generally sent domestically through wires/EMTs, and internationally by wire transfer through banks and money services businesses. Common international destinations for these transfers are the United States, Ivory Coast, Nigeria, Ghana, Burkina Faso, South Africa, Mali, the United Kingdom, Malaysia, Turkey, Philippines and Benin. Returned or cancelled transfers may indicate either that perpetrators have been caught or victims have realized they are being defrauded.

In many cases, perpetrators attempt to have victims act, unknowingly, as *money mules* to move proceeds of crime to other victims, perpetrators and/or third parties. As a *money mule*, victims serve as intermediaries to distance the funds from the perpetrators and make transactions more difficult to track. The transactions conducted by *money mules* may resemble in-and-out activity, which could, for example, include multiple third-party transfers into the victim's account followed by cash withdrawals. These transactions could also take the form of outgoing wires/EMTs or purchases of money orders/bank drafts. Reporting entities should be mindful of individuals conducting transactions at the direction of others (who may or may not be present at the time) or who do not have the expected information related to the transactions. In addition, victims may give perpetrators direct access to their bank accounts by disclosing online login information or sharing bank cards.

> A *MONEY MULE* IS AN INDIVIDUAL WHO, WITTINGLY OR UNWITTINGLY, TRANSFERS OR TRANSPORTS FUNDS ON BEHALF OF THE PERPETRATOR OF A CRIME, OR A MONEY LAUNDERER.

Indicators associated with transactions related to romance fraud

- Client appears to be pooling all financial resources from various sources (e.g., credit cards, loans, retirement savings, insurance policies) and depleting assets (e.g., home, vehicle, investments and retirement savings) to fund transfers to individuals/entities.
- Client sends funds to another individual, and the amount or frequency of funds sent increases over time.
- Client is transacting with one or more individuals suspected of being either a victim or perpetrator of romance fraud.
- Client is identified as a victim and is transacting with one or more individuals who are also identified as victims of romance fraud.
- Client either cancels transaction for no apparent reason or transaction is refused due to questionable rationale for it.
- Client makes payments to online dating services or social media websites.
- Client conducts large volume and/or excessive number of transactions involving foreign jurisdictions over a short period.
- Client receives funds from numerous individuals in multiple jurisdictions. The funds are then depleted by cash withdrawals conducted in Canada or abroad, or by wires to the benefit of individuals/entities in Canada or abroad.

Indicators of mass marketing fraud

- Client conducts financial activity or holds accounts at multiple financial entities without adequate rationale.
- Non-account holders or apparently unrelated individuals make deposits or payments to client's account.
- Client does not appear to know the sender of a wire transfer from whom the wire transfer was received, or the recipient to whom they are sending a wire transfer.
- Client conducts transactions at different physical locations or with different representatives in an apparent attempt to avoid detection.
- Account is used for pass-through activities (e.g. to receive and subsequently send funds to beneficiaries).

- Client becomes defensive when asked about the rationale for a transaction and may take steps to close account or conduct transaction elsewhere.
- Client orders wire transfers that are frequently returned or cancelled.
- Client frequently deposits fraudulent cheques or bank drafts that are later returned by the financial institution.
- Client appears to be directed by a third party to deposit funds into accounts or to wire funds to individuals domestically or in foreign jurisdictions.
- Client sends and/or receives an increasing amount of wires/EMTs.
- Client's wire transfers involve amounts or jurisdictions that are inconsistent with their profile.
- Client receives multiple incoming wires into a business account in a manner inconsistent with day-to-day business.
- Client makes numerous third-party cash deposits followed by outgoing draft/wire transfers to or cash withdrawals in high-risk jurisdictions.
- Client receives payments from payment processors that are inconsistent with the client's profile.

Reporting entities may wish to advise victims of romance fraud to contact the Canadian Anti-Fraud Centre at 1-888-495-8501 and their local police.

Reporting to FINTRAC

To facilitate FINTRAC's disclosure process, please include the term **Project CHAMELEON** or **#CHAMELEON** in Part G—Description of suspicious activity on the Suspicious Transaction Report.

(See also, Reporting suspicious transactions to FINTRAC.)

Contact FINTRAC

- **Email:** guidelines-lignesdirectrices@fintrac-canafe.gc.ca (include Operational Alert FINTRAC-2019-OA001 in the subject line)
- **Telephone:** 1-866-346-8722 (toll free)
- **Facsimile:** 613-943-7931
- **Mail:** FINTRAC, 24th Floor, 234 Laurier Avenue west, Ottawa, ON, K1P 1H7, Canada

Cat. No. FD4-19/2019E-PDF
ISBN 978-0-660-30150-1

FINTRAC operational alerts provide up-to-date indicators of suspicious financial transactions and high-risk factors related to new, re-emerging or particularly topical methods of money laundering and terrorist activity financing.