## 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.

## 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.