Financial Transactions and Reports Analysis Centre of Canada

Centre d'analyse des opérations et déclarations financières du Canada

Canada

OPERATIONAL ALERT:

Laundering the proceeds of

ONLINE CHILD SEXUAL EXPLOITATION

Project Shadow partners

This Operational Alert was developed by FINTRAC in collaboration with members of Project Shadow, a public-private partnership on the money laundering of proceeds from online child sexual exploitation. Project Shadow includes, but is not limited to, the following members:

Scotiabank®

CANADIAN CENTRE for CHILD PROTECTION™
Helping families. Protecting children.

Royal Canadian Mounted Police / Gendarmerie royale du Canada

Canada Border Services Agency / Agence des services frontaliers du Canada

Financial Transactions and Reports Analysis Centre of Canada / Centre d'analyse des opérations et déclarations financières du Canada

Domestic partners

- Royal Canadian Mounted Police:
  - National Child Exploitation Crime Centre
  - Behavioural Sciences Investigative Services
- Public Safety Canada
- Statistics Canada
- Ontario Provincial Police
- Ottawa Police Service
- Toronto Police Service

International partners

- Australian Transaction Reports and Analysis Centre (AUSTRAC)
- United Kingdom Financial Intelligence Unit
- New Zealand Police Financial Intelligence Unit
- TRACFIN
- Financial Intelligence Unit – The Netherlands
- Anti-Money Laundering Council – Philippines
- International Centre for Missing & Exploited Children – Singapore
- International Justice Mission
- University of Nottingham's Rights Lab

OPERATIONAL ALERT:

Laundering the proceeds of

ONLINE CHILD SEXUAL EXPLOITATION

Purpose

The purpose of this Operational Alert is to support reporting entities in recognizing financial transactions suspected of being related to the laundering of funds associated to child sexual exploitation. Through financial transaction reports, FINTRAC is able to assist in the detection, prevention and deterrence of all stages of money laundering (placement, layering and integration), the financing of terrorist activities and sanctions evasion by providing actionable financial intelligence disclosures to law enforcement and national security agencies. This Operational Alert provides money laundering indicators as a result of analysis of suspicious transaction reports, other financial transactions and other sources of information related to online child sexual exploitation. It updates and replaces the previous Operational Alert on the laundering of proceeds from online child sexual exploitation published in December 2020.

Project Shadow

is a public-private partnership initiative co-led by Scotiabank and the Canadian Centre for Child Protection, supported by Canadian law enforcement agencies and FINTRAC to combat online child sexual exploitation. The objective of the project is to improve the collective understanding of the threat, and to improve the detection, prevention and deterrence of the facilitation and laundering of the proceeds from online child sexual exploitation.

Background

According to Public Safety Canada, online child sexual exploitation occurs when children are coerced into seeing or participating in online encounters of a sexual nature.[1] Online child sexual exploitation involves the use of technology or the internet to facilitate the sexual abuse and exploitation of a child. This includes child sexual abuse material, self-generated materials and sexting, artificial intelligence generated child sexual abuse material, sexual extortion (also known as "sextortion"), grooming and luring, live child sexual abuse streaming and made-to-order content. Online child sexual exploitation is a disturbing global crime targeting children that continues to rise year after year, not only in the number of confirmed reports showing child sexual abuse images, but also in the severity of the images and videos.[2] In recognition that Canadians have a responsibility to uphold Canadian laws and values even when they are outside of the country, Section 7(4.1) of the *Criminal Code* of Canada allows for the application of charges to Canadian citizens or permanent residents who commit these as well as other sexual offences or human trafficking crimes outside of Canada, as if they were deemed to have committed the offences in Canada.

The motivation for sexually exploiting children varies, and while most perpetrators commit child sexual exploitation for sexual gratification and not financial gain, there has been an increase in financially motivated offending,

[1] In Canada, children are defined as under 18 years of age.

[2] Internet Watch Foundation: "Internet Watch Foundation (IWF) Annual Report 2022"

including sexual extortion cases in recent years.[3] Sexual extortion is a form of online blackmail involving threats to distribute sexual images or videos (of a victim) if the victim doesn't pay the extorter or provide more sexual content. The Canadian Centre for Child Protection reports that many of the extorters have been reported using similar strategies involving prominent social media platforms, especially those targeting younger users, posing online as a young person where they build some rapport and entice the victim to send a nude image or video. Once the images are shared, the extorter will blackmail the victim, demanding money or commodities (i.e., gift cards) or additional images to keep the images from being shared publicly or with family and friends. Additionally, complying with the extorters' demands for the money often leads to further demands for money until the victim cuts contact. According to sources consulted by Cybertip, Canada's national tip line for reporting the online sexual of children, demands for money have been known to come from international organized criminal networks[4]. Cybertip further highlights that boys are often targets of financial sexual extortion while girls are more often extorted for more images.

Financial payments enable online child sexual exploitation to occur. There is a financial dimension involved with online child sexual exploitation including the payment, purchase and proceeds associated with the access, consumption, production and distribution of these illicit materials. Some perpetrators coerce or groom children to share sexual images or videos of themselves, including by way of sending them funds or tokens (e.g., gift cards and prepaid credit cards). Other perpetrators will send funds to facilitators of livestreamed online child sexual abuse. The financial footprint reveals the intent to commit a crime while facilitating it.

Virtual currencies are used to purchase child sexual exploitation material as they offer pseudo-anonymity, which is valued by both producers and consumers of content. The International Centre for Missing and Exploited Children reports that almost all darknet markets engaging in the sale of child sexual exploitation material exclusively accept cryptocurrencies for payment rather than traditional payment methods. According to Chainalysis, Bitcoin is the most widely used cryptocurrency for purchasing child sexual exploitation material, but there has been a rise in the use of Monero in recent years. Chainalysis further notes in their 2024 Crypto Crime Report that the sophistication of sellers of child sexual exploitation material, and their resilience to detection and law enforcement takedowns, has increased over time. Instant exchanges, mixers, tumblers, and privacy coins (e.g., Zcash, Monero, Dash) are commonly used in the purchase of child sexual exploitation material, to provide more layers of anonymity in the transactions.

Another emerging trend of concern is the increase in the importation of childlike sex dolls. These dolls have childlike dimensions and features, are designed predominately for sex and meet the legal threshold of child pornography under section 163.1 (1) of the Canadian *Criminal Code*. These dolls have been reported to range in value from CAD 2,000 to 8,000. The purchase of these dolls occurs online from manufacturers located frequently in China and Japan, are often shipped using Chinese-based shipping entities, and sometimes will come with children's clothing and accessories.[5] The Australian Institute of Criminology highlights in Exploring the implication of child sex dolls, that although it hasn't been empirically established, it is possible that use of child sex dolls may indicate a progression in child sex offences, from viewing online child exploitation material to contact sexual offending. According to the Royal Canadian Mounted Police Behavioural Sciences Investigative Services Criminal Intelligence Unit, from the perspective of criminally/sexually deviant behaviours, the use of a childlike sex doll represents a unique form of interaction, different than the consumption of other forms of child sexual abuse materials (videos, pictures, etc.) It likely represents psychologically meaningful behaviours related to the sexual attraction to children, however, the offender's behaviour as a whole, must be considered before assessing the full significance of its use.[6]

---

[3] ALERT: Sextortion- ALERT (alert-ab.ca)

[4] For example, https://networkcontagion.us/reports/yahoo-boys/

[5] ALERT: Sextortion- ALERT (alert-ab.ca)

[6] Behavioural Sciences Investigative Services Criminal Intelligence Unit, RCMP.

Overview of FINTRAC's analysis of financial transactions related to online child sexual exploitation

Based on FINTRAC's analysis of financial transactions related to online child sexual exploitation, perpetrators or suspected perpetrators were nearly all male. They were employed in a wide range of occupations or listed as retired, and the majority of these individuals were aged between their late 20s and 60s. Consumption of online child sexual exploitation (i.e. purchasing child sexual abuse material) was the most common perpetrator role observed in the reported transactions, followed by producer or seller of online child sexual exploitation materials.

Outgoing electronic fund transfers to another country, funded by cash deposits or incoming electronic fund transfers were the primary transactions relating to the suspected purchase of live online child sexual abuse. Most funds were sent through money services businesses using their digital platforms, in low dollar amounts (often below CAD 200), sent in high frequency (i.e. multiple times a week or sometimes multiple times within the same day), and usually sent in the evenings to younger recipients, often female. These funds were sent in multiple instances incurring fees for each transaction and often sent to the same beneficiary. The five most common receiving destinations of funds identified in transaction reporting to FINTRAC were the Philippines, Thailand, the Dominican Republic, Colombia and Mexico.

It was observed that some of the older males, often over the age of forty years old, sending outgoing electronic funds transfers to high-risk jurisdictions for child sexual exploitation also displayed a financial pattern consistent with travelling abroad to offend. This includes travel related expenses such as flight bookings, hotel charges, and taxi charges, occurring shortly before or after transfers to a high-risk jurisdiction for child sexual exploitation. Of note, these purchases might be conducted in a region that is not a typical tourist destination, or the perpetrators' stays may be longer or more frequent than expected for a typical Canadian traveller. Other suspicious activity includes excessive ATM cash withdrawals (often in lower values but high frequency) and gift-like purchases, such as jewellery, in the high-risk jurisdiction. Certain countries may be of interest to sex offenders due to their economic situations, their lack of legislation for protecting at-risk individuals and/or their relative proximity to Canada. These high-risk jurisdictions include the Philippines, Thailand, India, South Africa, Dominican Republic, Mexico and Cuba.

Online purchase of child sexual exploitation material using virtual currencies was increasingly reported, often conducted by males aged in their late 20s to 30s. These transactions would often start as a one-to-one pattern, where the virtual currency was sent from the purchaser to a unique address linked to the individual. This is followed by a many-to-one pattern, where the funds were sent from the unique address held by the purchaser to an address that is receiving many similar transactions. Funds were often further layered through mixers/tumblers and depleted through a virtual currency exchange. The value of the transactions were often between CAD 5.00 and CAD 50.00. Re-occurring payments to the same address receiving funds from many different addresses may indicate the funds are payments for a subscription to child sexual exploitation material. Additionally, younger males in their 20s to 30s were more frequently reported purchasing child sexual exploitation material using peer-to-peer transfers – email money transfers or payment processors. Most of these purchases were of low value, often below CAD 200, but high frequency and sent to multiple individuals. These transactions would sometimes include jargon or slang that advertise new content for sale and child sexual exploitation material, such as the use of terms "school girl" "tots", "cp" and the use of emojis depicting cheese and pizza slices, lollipops, and baby soothers.

Of note, excessive purchases and payments indicate that the perpetrators/suspected perpetrators likely spent a large portion of time on the internet – from online purchases, app purchases, online gaming, use of online video and communication technologies, use of online file storage and purchases towards upgrades, subscriptions and special features on social media platforms. Online adult entertainment purchases were frequently observed, often in conjunction with the use of payment processors known to serve the adult entertainment industry, along with purchases to achieve a level of online privacy and anonymity such as purchases for virtual private network services and forensic device cleaning services without a reasonable explanation. These purchases were often not in line with the stated occupation or expected income and/or appear to be excessive.

Transactions related to sexual extortion are often distinguished by the transaction notes/details. Transaction details would sometimes include pleading language, and references to explicit material taken including photos and videos (e.g. “delete the video”, “please stop”). Funds transfers typically range between CAD 10 and CAD 200 and are sent via peer-to-peer transfers or email money transfers. Money services businesses may be used to send aggregated funds, from multiple victims, and send the funds overseas. Sexual extortion payments from younger minors will typically be in smaller amounts whereas sexual extortion cases involving older individuals see larger funds transfers.

Childlike sex dolls are often purchased from manufacturers overseas, including from China and Japan. Individuals purchasing these dolls are often single males with no known dependants, and this purchase will be outside of typical purchases and/or not in line with expected expenses given their income. The purchase of these dolls is often seen in conjunction with other concerning purchases and financial activity such as excessive shipping charges, purchases at toy stores, youth clothing stores and sex toy stores. The purchase of these kinds of dolls occurs alongside other financial indicators of online child sexual exploitation material, such as purchases for online tools and services for online privacy and anonymity.

Reasonable grounds to suspect and how to use indicators

How reporting entities determine if they need to submit a suspicious transaction report to FINTRAC (for either a completed or attempted financial transaction) requires more than a "gut feel" or "hunch," although proof of money laundering, terrorist financing or sanctions evasion is not required. Reporting entities are to consider the facts, the context and money laundering indicators of a transaction. When these elements are viewed together, they create a picture that is essential to differentiate between what may be suspicious and what may be reasonable in a given scenario. Reporting entities must reach reasonable grounds to suspect that a transaction, or attempted transaction, is related to money laundering, terrorist financing or sanctions evasion before they can submit a suspicious transaction report to FINTRAC.

Indicators of money laundering can be thought of as red flags indicating that something may very well be wrong. Red flags typically stem from one or more characteristics, behaviours, patterns and other contextual factors related to financial transactions that make them appear inconsistent with what is expected or considered normal. On its own, an indicator may not initially appear suspicious. However, it could cause reporting entities to question the legitimacy of a transaction. This may prompt them to assess the transaction to determine whether there are further facts, contextual elements or additional money laundering, terrorist financing or sanctions evasion indicators that would raise their level of suspicion at which submitting a suspicious transaction report to FINTRAC would be required (see FINTRAC Guidance on Suspicious Transaction Reports).

Money laundering indicators

The following money laundering indicators related to online child sexual exploitation are based on an analysis of FINTRAC’s data holdings and other domestic and international sources of information. The identified types and patterns of transactions, along with contextual factors, emphasize the importance of knowing your client obligations under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*. These indicators should not be treated in isolation; on their own, these indicators may not be indicative of money laundering or other suspicious activity. They should be assessed by reporting entities in combination with what they know about their client and other factors surrounding the transactions to determine if there are reasonable grounds to suspect that a transaction or attempted transaction is related to the commission or attempted commission of a money laundering offence.

Several indicators may reveal otherwise unknown links that, taken together, could lead to reasonable grounds to suspect that the transaction or attempted transaction is related to the commission or attempted commission of a money laundering offence. It is a constellation of factors that strengthens the determination of suspicion. These indicators aim to help reporting entities in their analysis and assessment of suspicious financial transactions.

Reporting entities should also consider whether the listed transactional and contextual indicators play a role in maintaining a strong compliance program when considered as risk factors in a money laundering, terrorist financing and sanctions evasion risk assessment of potential and current clients. Understanding and applying these indicators can help mitigate against the money laundering, terrorist financing and sanctions evasion exploitation of a reporting entity's business. Business-client relationship risk factors dynamically evolve over time and fall into the following categories:

- products, services and delivery channels that create anonymity and obscure source or destination of funds;
- client transactions and geographical locations related to high-risk jurisdictions;
- new developments and technologies made available to clients; and
- client characteristics and the purpose of their relationship with a business that define expectations for what are normal or suspicious patterns of activity or transactions.

Please see FINTRAC's Risk assessment guidance and Compliance program requirements for more information.

Indicators related to suspected perpetrators who are consumers and/or facilitators of online child sexual exploitation

- Funds sent to/received from an individual charged with and/or mentioned in adverse media for child sexual exploitation-related offences.
- Frequent transfers of low-value funds by a male to one or a few recipients, often female, located in a jurisdiction(s) at high-risk for child sexual exploitation, in a short timeframe and who has no apparent familial or other legitimate connection to the recipient.
- Frequent transfers of low-value funds by a male (usually aged over 40), to younger recipients, often female, in a jurisdiction(s) at high-risk for child sexual exploitation through online banking or money services business, including digital platforms, often in the late evening/early morning hours.
- Receipt by an individual of numerous small credit transfers from third parties, often from other countries that are immediately transferred to another account or withdrawn in cash.
- Remittance information or transaction details that refer to expenses paid (such as school expenses, family support, medical bills, allowances, allotment) but does not align with the smaller amounts or frequency of the funds that were actually sent.
- Travel related expenses (e.g., flight bookings, hotel and taxi charges) that occur closely before or after transfers to a jurisdiction at high-risk for child sexual exploitation.
- Travel related expenses (e.g., flight bookings, hotel and taxi charges) occurring in a jurisdiction at high-risk for child sexual exploitation for periods longer or more frequent than expected for a typical Canadian traveller.
- Transactions conducted or account accessed in a jurisdiction at high-risk for child sexual exploitation (e.g., significant ATM cash withdrawals, purchases of jewellery or clothes that are atypical for account holder).
- Purchases at vendors that offer online encryption tools, virtual private network services, software to clear online tracking, or other tools or services for online privacy and anonymity, including encrypted email services.
- Excessive payments to online file sharing and hosting vendors/platforms.
- Frequent, low-value transfers, to or through peer-to-peer funds transfer platforms, often with sexually explicit references, references to social media platforms, and/or references to file sharing and creator-content streaming websites, including those hosting artificial intelligence generated material.

- Frequent, low-value transfers, to payment service providers, particularly those serving high-risk merchants in the adult entertainment industry or file sharing and hosting vendors/providers.
- Purchases on webcam/livestreaming platforms, dating platforms, and/or websites offering adult entertainment, particularly those that have chat functions and those suspected to host illegal content.
- Purchases at multiple vendors of electronics, computers, and cell phones and/or payments to cell phone service providers, particularly those specializing in international calling services.
- Frequent purchases at online gaming platforms that are known to be frequented by minors and have chat functions.
- Excessive purchases from online merchants providing gift cards.
- Frequent, low-value funds transfers with references related to child sexual exploitation and/or image and video-based social media platforms.
- Frequent, low-value amounts sent to entities that engage in virtual currency money service business activities (e.g., Instant exchanges).
- Frequent low-value purchases of cryptocurrencies, particularly privacy coins.
- Purchases or withdrawals of cryptocurrencies using prepaid and credit cards.
- Funds from a virtual currency wallet, often in low-value amounts, sent directly or indirectly to a wallet address or cluster identified as selling child sexual abuse material.
- Re-occurring, virtual currency payments to one address, or a group of addresses controlled by the same individual or entity, for the possible subscription of child sexual abuse material.

Indicators related to suspected perpetrators who are producers/sellers of online child sexual exploitation material

- Receiving peer-to-peer payments from predominantly male counterparts in low-value amounts, often located in other jurisdictions, with sexually explicit references, references to social media platforms and/or references to file sharing and creator-content streaming websites, including those hosting artificial intelligence generated material.
- Purchasing software for capturing video from websites and other online platforms from vendors.
- Purchasing domain registration/website hosting entities.
- Purchasing equipment or software for photography or video making from specialized vendors, not in line with stated occupation or expected business activity.
- Receiving funds from creator-content streaming websites (e.g., subscription payments from these sites) that may be associated with child sexual abuse material.
- Receiving funds from a payment processor while having a profile on a creator-content streaming website that includes adult entertainment content, especially with a subscription-based channel model.
- Receiving funds from a payment processor through a website that hosts child sexual exploitation material.
- Sending low-value (i.e. $0.01) peer-to-peer payments to counterparts with memos using jargon or slang that advertise new content for sale and child sexual exploitation material related references.

Indicators related to possible online child sexual exploitation in the form of luring[7]

- Multiple purchases for accommodations (e.g., hotel, motel, short-term rentals) within the individual's city of residence or a nearby city.
- Funds transfers sent in low, rounded dollar amounts to minors, especially with sexually explicit references.
- Funds transfers sent to minors with references to social media platforms or other communication platforms, particularly ones with restricted/closed channels.
- Purchases at youth-oriented stores or venues (e.g., gaming stores, children's clothing store, amusement parks).
- Purchases at youth-oriented live online chat rooms and/or social media platforms for upgrades, subscriptions, and special features.

Indicators related to possible online child sexual exploitation in the form of sexual extortion

- Referencing in transaction notes that suggest the funds were extorted from the senders, such as pleading language, and references to explicit material taken including photos and videos (e.g., "delete the video", "please stop").
- Receiving funds from young and underage counterparties, often funded by prepaid cards, using peer-to-peer funds transfer platforms.
- Receiving a pattern of funds from young and underage individuals in short succession in low-value amounts only once or twice with no clear purpose.
- Withdrawing funds, often by way of e-transfers to unrelated individuals, beyond transaction limit.
- Quickly depleting an account by way of email money transfers, online gift card purchases, and/or funds sent to peer-to-peer funds transfer platforms.

Indicators related to child-like sex dolls[8]

- High-value purchase(s) from sex doll manufacturer(s) that appears excessive or not in line with expected income.
- Frequent purchases from toy stores that are not in line with individual's personal status (single with no dependants) or expected account activity.
- Atypical or excessive payments to shipping companies.
- Purchases associated with dolls such as clothing, accessories and toys.

---

[7] Luring children to create child sexual abuse material may also constitute a human trafficking offense in Canada. Please see Updated Indicators: Laundering of proceeds from human trafficking for sexual exploitation for more information on human trafficking and the associated indicators.

[8] Indicators related the consumption of online child sexual exploitation material were always present when child like sex doll indicators were present in FINTRAC's Suspicious Transaction Reports.

Reporting to FINTRAC

To facilitate FINTRAC's disclosure process, please include the term **#Project SHADOW** or **#SHADOW** in the grounds for suspicion narrative of the Suspicious Transaction Report. See also, reporting suspicious transactions to FINTRAC.

Contact FINTRAC

Email: guidelines-lignesdirectrices@fintrac-canafe.gc.ca
Telephone: 1-866-346-8722 (toll-free)
Mail: FINTRAC, 24th Floor, 234 Laurier Avenue West, Ottawa ON K1P 1H7, Canada

Cat. No. FD4-24/2025E-PDF
ISBN 978-0-660-77732-0

Resources

For more information on child sexual exploitation as well as associated financial intelligence, please consult the following resources:

Canada

- ALERT: "Sextortion"
- Canadian Centre for Child Protection
- Cybertip.ca
- Public Safety Canada: "Child Sexual Exploitation on the Internet"

International

- Anti-Money Laundering Council (Philippines): "Online Sexual Abuse and Exploitation of Children in the Philippines: An Evaluation using STR Data"
- AUSTRAC: "Combating the sexual Exploitation of Children for Financial Gain"
- Australian Institute of Criminology: "Australians who view live streaming of child sexual abuse: An analysis of financial transactions"
- Chainalysis: "CSAM and Cryptocurrency: On-chain Analysis Suggests CSAM Vendors May Benefit from Privacy Coins like Monero and Other Obfuscation Measures"
- ECPAT: "Online Child Sexual Exploitation"
- Egmont: "Combatting Online Child Sexual Abuse and Exploitation Through Financial Intelligence – Public Bulletin"
- Europol: "Stop Child Abuse – Trace an Object"
- International Centre for Missing and Exploited Children: "Cryptocurrency and the Trade of Online Child Sexual Abuse Material"
- International Justice Mission: "Scale of Harm: Estimating the prevalence of Trafficking to Produce Child Sexual Exploitation Material in the Philippines"

- Internet Watch Foundation
- National Center for Missing & Exploited Children: Sextortion
- United Nations Office on Drugs and Crime (UNODC): Online child sexual exploitation and abuse
- University of Nottingham Rights Lab and Global Fund to End Modern Slavery: "Investigation into financial transactions used in the online sexual exploitation of children"
- Virtual Global Taskforce
- WeProtect Global Alliance: "Global Threat Assessment 2023"