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

Canada

**OPERATIONAL ALERT**

Reference: FINTRAC-2020-OA001
December 2020

# Laundering of Proceeds from 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, particularly online child sexual exploitation. Through financial transaction reports, FINTRAC is able to facilitate the detection, prevention and deterrence of all stages of money laundering (placement, layering and integration) and the financing of terrorist activities by providing actionable financial intelligence disclosures to law enforcement and national security agencies. This Operational Alert provides money laundering indicators as a result of the analysis of FINTRAC disclosures and Suspicious Transaction Reports (STRs) related to online child sexual exploitation.

### 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 of the facilitation and laundering of the proceeds from online child sexual exploitation.*

## Background

Online child sexual exploitation is defined by the Virtual Global Taskforce as "offences related to possessing, distributing, producing and accessing child pornography [or, more accurately, child sexual abuse material or child sexual exploitation material], online grooming and luring".[1] It is a disturbing global crime targeting children.

### The Virtual Global Taskforce

*is an international collaboration of law enforcement agencies and private sector partners. Co-founded and currently chaired by the Royal Canadian Mounted Police (RCMP), this taskforce aims to protect children from online and offline sexual exploitation.*

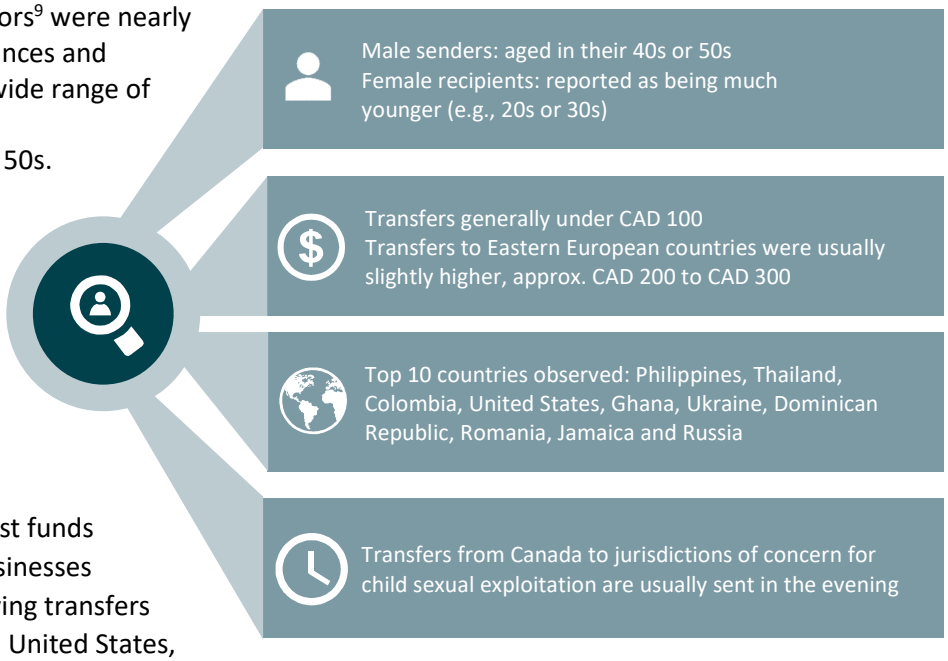
The ease of Internet accessibility as a result of a growing number of affordable Internet-enabled devices, along with a growing number of children using the Internet at a younger age have given perpetrators increased access to children for sexual purposes.[2] Further, technological advancements have increased the production and consumption of child sexual exploitation material for a very low cost.[3] Perpetrators have also increased their use of encryption services, anonymization technologies, the dark web, online file hosting and file sharing to avoid detection. They also solicit children online for sexual purposes on many online platforms children use[4], and distribute[5] child sexual exploitation material mostly through online peer-to-peer sharing platforms and increasingly through social media. As well, the COVID-19 pandemic since early

2020 has served as an accelerator of and has contributed to an increase in the consumption and production of child sexual exploitation material, while also pushing offenders to adapt their online environment to avoid detection.[6] The financial dimension of online child sexual exploitation includes payments, purchases and proceeds associated to the access, consumption, production, and distribution of the illicit material. There is also increased risk of virtual currencies being used as payment for online child sexual exploitation material. Furthermore, some perpetrators coerce or groom tween (children between 8 and 12 years old) and teen victims to share sexual images or videos of themselves then threaten and extort their victims for money or additional sexual material. This is known as "sextortion".[7] However, most perpetrators commit child sexual exploitation offences for sexual gratification and not for financial gain.

## Overview of FINTRAC's analysis of disclosures and STRs related to online child sexual exploitation

Based on FINTRAC's analysis of disclosures and assessment of STRs related to online child sexual exploitation[8], perpetrators and suspected perpetrators[9] were nearly all males, located in all Canadian provinces and territories. They were employed in a wide range of occupations and the majority of these individuals were aged in their 40s and 50s. Consumers of online child sexual exploitation were the most common perpetrator role observed.

Figure 1. Characteristics of perpetrators'/ suspected perpetrators' international funds transfers




Transactions were primarily outgoing funds transfers to another country —particularly to jurisdictions of concern for child sexual exploitation (see Figure 1 for characteristics of those transfers). Most funds were sent through money services businesses (MSBs). The top 10 jurisdictions receiving transfers were: Philippines, Thailand, Colombia, United States, Ghana, Ukraine, Dominican Republic, Romania, Jamaica and Russia. In the Philippines, transfers were primarily received through MSBs and pawn shops. Transfers were usually sent in the evening hours (mostly between 6 p.m. and 9 p.m., regardless of Canadian time zone), mostly on Thursdays and Fridays and least on Sundays.

FINTRAC assesses that numerous other purchases and payments indicate that the perpetrators/suspected perpetrators likely spent a large portion of time on the Internet (e.g., online purchases, app purchases, online gaming and gambling, use of online video and communication technologies, use of online file storage), often consumed material on online adult entertainment platforms (which may include imbedded child sexual exploitation material) and were likely concerned about their online privacy and anonymity. Transactions also heavily involved payment processors.

## Reasonable grounds to suspect and how to use indicators

Reporting entities' decision 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 is not required. Reporting entities are to consider the facts related to a transaction and its context that can, when taken together, give rise to reasonable grounds to suspect that the transaction is related to the laundering or attempted laundering of proceeds of crime.

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. Reporting entities' review of the trail of indicators may follow various scenarios and lead to different conclusions depending on whether the level of suspicion is strengthened or weakened (see FINTRAC Guidance on Suspicious Transaction Reports).

## Money laundering indicators

Below are money laundering indicators related to online child sexual exploitation derived from FINTRAC's analysis and reflect the types and patterns of transactions, contextual factors and those that emphasize the importance of knowing your client. 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 is related to online child sexual exploitation offences and/or the laundering of proceeds derived from those crimes. It is a constellation of factors that strengthen the determination of suspicion. These indicators aim to help reporting entities in their analysis and assessment of suspicious activity.

### Money laundering indicators related to possible perpetrators who are consumers and/or facilitators* of online child sexual exploitation

- ⊗ An individual is the subject of adverse media involving child sexual exploitation-related offences.
- ⊗ Funds sent to or received from an individual (e.g., a convicted sex offender) charged with child sexual exploitation-related offences (including any luring offences) and/or funds to or from a common counterparty shared with such an individual.
- ⊗ A male who frequently transfers low-value funds to the same female or multiple females in a/many jurisdiction(s) of concern for child sexual exploitation (e.g., Philippines) in a short timeframe and has no apparent familial or other legitimate connection to the country or recipient.
- ⊗ A male (usually aged over 50) who transfers low-value funds from an in-branch/in-store location usually to a female in a jurisdiction of concern for child sexual exploitation usually between 1 p.m. and 8 p.m., regardless of Canadian time zone.
- ⊗ A male who transfers low-value funds usually to a female in a jurisdiction of concern for child sexual exploitation through online banking or an online money services business platform in the late evening/early morning hours (usually between 8 p.m. and 1 a.m., regardless of Canadian time zone).
- ⊗ Travel-related expenses (e.g., passport purchase, flight bookings, airline baggage fees) that occur closely before or after transfers to a jurisdiction of concern for child sexual exploitation.
- ⊗ Transactions conducted or accounts accessed in a jurisdiction of concern for child sexual exploitation (e.g., ATM cash withdrawals, account logins through IP address in a jurisdiction of concern).
- ⊗ Purchases at vendors that offer online encryption tools, virtual private network (VPNs) services, software to clear online tracking, or other tools or services for online privacy and anonymity.
- ⊗ Payments to online file hosting vendors/platforms.

* Facilitators are those who share, distribute, make available, and/or sell child sexual exploitation material online. Nearly all facilitators in FINTRAC's analysis were also consumers of online child sexual exploitation material and some were also producers.

- ⊗ Transfers to peer-to-peer financing websites or through peer-to-peer funds transfer platforms.
- ⊗ Payments to or funds received through or from payment processors, including ones that deal in virtual currencies.
- ⊗ Purchases on webcam/livestreaming platforms, including those for adult entertainment.
- ⊗ Purchases on dating platforms, particularly Asian dating websites or ones that also offer adult entertainment content (dating websites observed in FINTRAC's analysis were: www.filipinocupid.com, www.asianbeauties.com, www.asiandating.com, www.asiandatingspace.com, www.asiandate.com, www.arabmatching.com, www.amolatina.com, www.lovetoria.com, www.naughtydate.com, www.mingle2.com, Tinder, Grindr).
- ⊗ Purchases at adult entertainment venues and/or adult entertainment websites.
- ⊗ Payments to or purchases through a payment processor that specializes in serving high-risk merchants such as those in the adult entertainment industry—some of which appear able to conceal the merchant's name.
- ⊗ Payments to a self-storage facility and/or for office rentals.
- ⊗ Purchases at multiple vendors of electronics, computers, and cell phones and/or payments to multiple cell phone service providers.
- ⊗ Purchases at a vendor that rents or leases computers and/or computer equipment.
- ⊗ Purchases at online gaming platforms and/or gaming stores.
- ⊗ Transactions to reload prepaid credit cards (particularly ones that deal with virtual currencies).
- ⊗ Purchases at online merchants.
- ⊗ Purchases of gift cards and/or payments made using gift cards.
- ⊗ Payments to or purchases through social media platforms, including ones that enable payment services through a payment processor.
- ⊗ Email money transfers that include a partial email address or reference with terms possibly related to child sexual exploitation.
- ⊗ Use of virtual currencies to fund a virtual currency account, convert funds and/or transfer funds to another virtual currency wallet, obtain a cryptocurrency loan or withdraw funds in cash.

## Money laundering indicators related to possible perpetrators who are producers of online child sexual exploitation material

- ⊗ Purchases at vendors that offer software for peer-to-peer (P2P) sharing platforms for P2P sharing of videos and images, including software to share hard drive content directly over the Internet.
- ⊗ Purchases at vendors that offer software for capturing video from websites or other online platforms.
- ⊗ Purchases at vendors that offer Voice-Over-IP communication services.
- ⊗ Purchases at domain registration/website hosting entities.
- ⊗ Purchases at vendors specializing in equipment or software for photography or video-making.
- ⊗ Purchases at creator-content streaming websites (e.g., membership fees or subscriptions to these sites or payment of funds to other streamers on these sites).

- ⊗ Receiving funds from a payment processor and having a profile on a creator-content streaming website (particularly a creator-content website that includes adult entertainment content with a subscription-based channel model).

### Financial indicators possibly related to online child sexual exploitation in the form of luring

- ⊗ Multiple purchases for accommodations (hotel/motel/peer-to-peer accommodation rentals), particularly at venues in the individual's own city or in a nearby city.
- ⊗ Purchases made for long-distance travel (e.g., air travel, city-to-city bus).
- ⊗ Use of separate email accounts to send or receive email money transfers.
- ⊗ Email money transfers sent to multiple females, including minors.
- ⊗ Purchases at youth-oriented stores or venues (e.g., toy store, children's clothing store, amusement park, playcentre, candy shop).
- ⊗ Purchases at vendors for cannabis/cannabis-related products and equipment and/or at pharmacies.
- ⊗ Payments to an online classified ad website.
- ⊗ Purchases at youth-oriented live online chat rooms.

## Reporting to FINTRAC

To facilitate FINTRAC's disclosure process, please include the term **#Project SHADOW** or **#SHADOW** 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
**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. FD4-24/2020E-PDF
ISBN 978-0-660-36454-4

## Resources

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

### *Canada*

- Canadian Centre for Child Protection
- Cybertip.ca
- Public Safety Canada: "*Child Sexual Exploitation on the Internet*"
- Virtual Global Taskforce: "*Online Child Sexual Exploitation: Environmental Scan Unclassified Version 2019*"

### *International*

- AUSTRAC: "*Combating the sexual exploitation of children for financial gain: Activity indicators*"
- ECPAT International: "*Trends in Online Child Sexual Abuse Material*"
- Egmont Group: "*Combatting Online Child Sexual Abuse and Exploitation Through Financial Intelligence – Public Bulletin*"
- Europol: "*Internet Organized Crime Threat Assessment 2019*"
- Internet Watch Foundation

[1] Virtual Global Taskforce: "*Online Child Sexual Exploitation: Environmental Scan Unclassified Version 2019*"
[2] *Ibid.*
[3] *Ibid.*
[4] Canadian Centre for Child Protection, Cybertip.ca: "*What are "cappers" and why do parents need to know?*"
[5] Europol: "*Internet Organized Crime Threat Assessment 2019*"
[6] Interpol: "*COVID19 Impact: Threats and Trends Child Sexual Exploitation and Abuse 2020*"
[7] Cybertip.ca: "*Sextortion*"
[8] Disclosures and STRs were from 2018 to late 2020.
[9] FINTRAC considers perpetrators to include offenders charged with child sexual exploitation-related offences or individuals under investigation by law enforcement for such offences. Suspected perpetrators include individuals in the same financial network as perpetrators and/or who exhibited similar financial activity as perpetrators.