Gibraltar Financial Intelligence Unit

HM Government of Gibraltar

# Combating Online Child Sexual Abuse & Exploitation

Guidance Notes

Version 1.0

# Table of Contents

# Scope

This guidance is produced by the Gibraltar Financial Intelligence Unit (GFIU).[1] Terminology can vary across different countries, the use of child abuse or child sexual exploitation is often used. This document uses child sexual abuse and exploitation (CSAE) which is a more encompassing term.

CSAE is a serious crime that has life-long physical and psychological consequences for victims. The guidance provided in this document Online CSAE commonly includes sharing or possession of indecent images of children (still or video), grooming, coercing children into conducting sexual acts and live streaming. These guidance notes are intended to provide reporting entities with key indicators and red flags to be able to identify suspicious financial transactions related to the live streaming of sexual abuse over the internet and this profit-driven illicit activity. Raising awareness of the threats of online CSAE is a strategic priority for the GFIU and working in collaboration with our partners and reporting entities is crucially important to tackle CSAE.

The GFIU advises that you should always also refer to the relevant, up-to-date legislation. Neither the GFIU nor the Gibraltar competent authorities can issue definitive guidance on how the law might be applied in a particular case or how Gibraltar courts might interpret the law. **Finally, this guidance does not represent legal advice. If you are unsure about your obligations in a given case, you should take independent legal advice**.

# Background

Online streaming of CSAE is a significant threat, which has been exacerbated by the Covid-19 pandemic, restrictions in travel, and the improvement and accessibility of online streaming platforms. With perpetrators unable to travel, they have turned to new technology with faster global internet speeds that provide new opportunities for them to communicate in real time and exploit children for sexual gratification. The demand for child sexual abuse material has increased and has led to an increase in new abuses. Like other forms of sexual abuse, it can scar victims mentally, emotionally and physically for life. Consequently, this represents a real threat to the safety of children across the world and financial institutions can play an important role in combating this heinous crime. According to the findings of the Virtual Global Taskforce (VGT) Child Sexual Exploitation Environmental Scan, produced by Europol's European Cybercrime Centre, the online streaming of CSAE is no longer an emerging trend but rather an established reality. Awareness and understanding of this threat with an effective information sharing mechanism are paramount.

# 1 Overview of the problem

## 1.1 What is online streaming of child sexual abuse and exploitation?

Online streaming of CSAE involves children being coerced by facilitators at the request of an offender who may direct the abuse from a different jurisdiction. Facilitators may be the victim's own parents or extended family. Online streaming technology offers a more protective environment for the offender(s) who can direct the abuse of the victim(s) at the request of an

[1] This guidance document has been compiled from various sources including the Egmont Group project report on CSAE. Egmont's work is gratefully acknowledged.

offender(s) situated in a different location. The COVID-19 pandemic has triggered an increase in the use of online video applications, which reduces the risk to the offender.

## 1.2 What are the financial dimensions of CSAE?

In some countries, poverty amongst certain communities has created a profit-driven phenomenon using children that are vulnerable to sexual abuse and exploitation. Live streamed abuse can be monetised and therefore leaves a financial trail which may provide opportunities to identify perpetrators, their facilitators and most importantly protect the victims from further abuse. The financial transactions of online CSAE may include payments and purchases in order to access, produce and distribute the proceeds associated with the access, consumption, production, and distribution of child sexual abuse material. New methods of payment may include the use of pre-paid cards and cryptocurrencies. It must be noted that most perpetrators commit these crimes for sexual gratification and may not necessarily be making any profit. Financial gains will in most cases be made by the facilitators.

## 1.3 Enabling Factors

A number of factors have enabled perpetrators and facilitators to engage in online CSAE activities. The advances in technology and the global expansion of high internet speeds has created a new platform for child sex offenders to satisfy their sexual desires in a relatively risk free environment. Furthermore, research suggests that there is a perception in certain poorer communities that online streaming of CSAE is not conflicting with social norms. This can be attributed to limited understanding of technology and the wide reach of the internet but also that it provides a quick source of income to families.

Environmental factors such as the increase in social media platforms used by children is also a growing concern. Children are able to post self-generated indecent material for profit on popular platforms that have embedded streaming functions or webcam supported applications.

A 2013 study on child sexual abuse and exploitation, published by FIU The Philippines, found three main categories according to the scale of operation:

- **Individual operations** are run from private homes, internet cafes, or a 'Pisonet' (computers that will provide internet access for 5 minutes for every PhP1.00). Children involved in online sexual abuse are also commonly involved in street prostitution.

- **Family-run operations** are common in very crowded and poor neighbourhoods where children are coerced by parents and other family members.

- **Large-scale operations** may involve whole neighbourhoods where children are hired or trafficked. But many of the operations are family-run wherein the traffickers are mostly relatives and friends of the trafficked person. The study also noted that a facilitator may purchase online tools or software to support online streaming and/or enhance images and video creation.

## 1.4 Payment Patterns

Financial transactions are often of low values, ($15-$500) sent via a remittance provider. These payments usually occur through Money Service Businesses (MSBs) and banks using online platforms. Remittance payments can also be in cash via MSBs. Research shows that there are limited examples of the use of virtual assets. Payments may also be made using a combination

of remittance service providers to avoid raising suspicions. In most cases, payments are sent before the material is streamed, which demonstrates the financial incentive for facilitators.

## 1.5 Use of technology

Whilst technology may be a crime enabler for offenders, it also creates a digital footprint that may be useful for law enforcement agencies. Information such as IP addresses and network port numbers can assist to locate and identify perpetrators, facilitators or even victims. It is important to note that in order to disguise their illicit activity, offenders may use virtual private networks (VPNs). Payments for VPN services may also be an indicator.

# 2 The Red Flags

Red flags provide an overview of the types of activities that can be suspicious, and are not exhaustive. They are designed to assist reporting entities in conducting analysis and assessment of behaviours that indicate that a customer/client may be committing online CSAE related offences. [2]

The use of keywords may result in the identification of suspicious transactions related to CSAE. This may involve improving transaction monitoring rules with words that relate to CSAE.

These red flag indicators should be considered in context, as the mere presence of an indicator on its own is not necessarily indicative of online CSAE activity. Multiple red flags in transactions for which a customer/client is unable to provide a legitimate explanation raises the suspicion of potential criminal activity. The identification of multiple indicators that raises a suspicion should prompt further investigation, analysis and reporting where appropriate.

## 2.1 Client Behaviour – Perpetrators who are consumers/ facilitators

When conducting analysis and assessments of clients, there are some red flags that may raise suspicions related to online CSAE.

These include, but are not limited to, the following:

- An individual is the subject of adverse media involving CSAE related offences;
- Funds sent to or received from an individual (e.g., a convicted sex offender) charged with CSAE-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 person or multiple persons in a/many jurisdiction(s) of concern for CSAE (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 usually to a person in a jurisdiction of concern for CSAE usually between unusual hours that are not in line with the client's time zone;
- A male who transfers low-value funds usually to a person in a jurisdiction of concern for CSAE through online banking or an online money services business platform in the late evening/early morning hours (usually between 8:00pm and 1:00am, regardless of CET 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 CSAE;
- 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;
- 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;

[2] The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) recently conducted an analysis on CSAE and have kindly permitted the GFIU to use some of the red flags and key indicators in the preparation of this guidance. GFIU gratefully acknowledges FINTRAC's assistance.

- Purchases on dating platforms, particularly Asian dating websites or ones that also offer adult entertainment content;
- Purchases at adult entertainment venues and/or adult entertainment websites;
- Payments to or purchases through a payment processor that specialises 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 mobile phones and/or payments to multiple mobile 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;
- Payment link via 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.

## 2.2 Client Behaviour – Perpetrators who are producers of CSAE 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 VOIP communication services;
- Purchases at domain registration/website hosting entities;
- Purchases at vendors specialising 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).

## 2.3 Financial Indicators – Luring for CSAE

- 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;
- Payment link via email money transfers sent to multiple persons, including minors;
- Purchases at youth-oriented stores or venues (e.g., toy shop, children's clothing store, amusement park, play centre, sweets shop);
- Payments to an online classified ad website;
- Purchases at youth-oriented live online chat rooms.