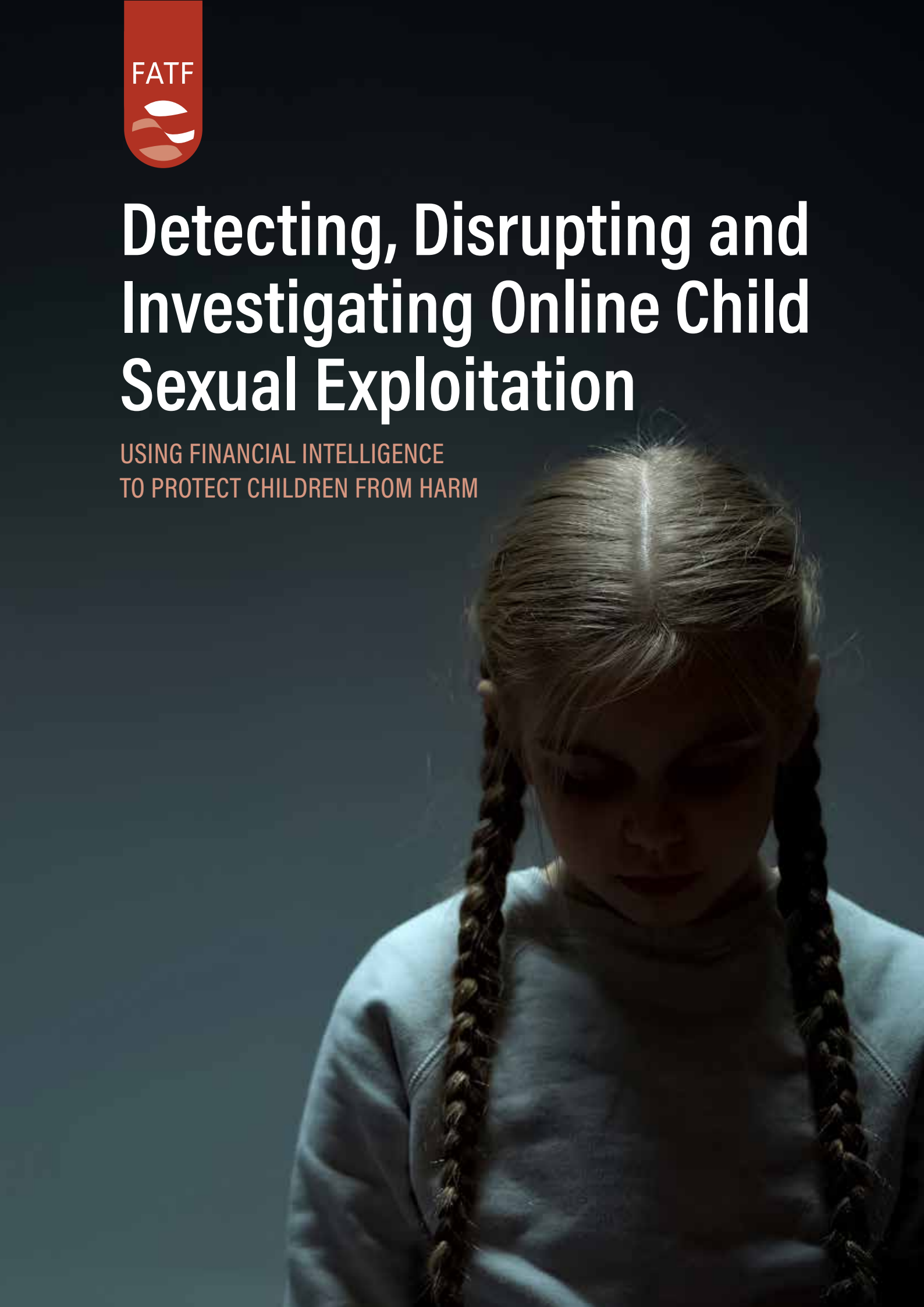
FATF

Detecting, Disrupting and Investigating Online Child Sexual Exploitation

USING FINANCIAL INTELLIGENCE TO PROTECT CHILDREN FROM HARM



The Financial Action Task Force (FATF) is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. It sets international standards that aim to prevent these illegal activities and the harm they cause to society. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CFT) standard.

For more information about the FATF, please visit
www.fatf-gafi.org

Detecting, Disrupting and Investigating Online Child Sexual Exploitation

USING FINANCIAL INTELLIGENCE TO PROTECT CHILDREN FROM HARM

Acronyms

CSAM	Child Sexual Abuse Material
EUR	Euro
FATF	Financial Action Task Force
FSEC	Financial Sexual Extortion of Children
LSAC	Live-streamed Sexual Abuse of Children
ML	Money Laundering
MVTS	Money or Value Transfer Services
OCSE	Online Child Sexual Exploitation
P2P	Peer-to-Peer
VASP	Virtual Asset Service Provider
VPN	Virtual Private Network

Definitions

Abuser	An individual separate to the facilitator who commits the live-streamed sexual abuse of children.
Catfishing	The process of attracting someone into a relationship by means of a fictional online persona. In the context of sexual extortion, catfishing is used to attract potential victims into online relationships for a specific purpose.
Capping	The recording of live-streamed child sexual abuse material, including material generated for financial gain or material generated by children themselves under coercion, which is then disseminated online.
Child	A person under the age of 18 years.
Consumer	An individual who issues a payment to a facilitator to view the live-streamed sexual abuse of children, at times directing the nature of the sexual abuse. Generally based in a separate location to where the contact abuse takes place.
Destination Country	The country where the OCSE-related financial transactions, made by a consumer or by a victim of sexual extortion, are ultimately received.
Facilitator	An individual who arranges the live-streamed sexual abuse of children. In some cases, they also act as the abuser.
Perpetrator	The individual, or groups of individuals, conducting financial sexual extortion of children.
Ransom	An amount requested to stop a perpetrator of sexual extortion from releasing, or threatening to release, the sexually explicit material of a victim.
Source Country	The country where an OCSE-related financial transaction originates from. These are the transactions made by consumers or victims of sexual extortion.
Teenager	A person between the age of 13-17 years, inclusive.
Victim	The child subjected to the online sexual exploitation.

Table of contents

Executive Summary

At a global level, researchers estimate that 300 million children around the world, or 1-in-8 of all children, are affected by online sexual abuse and exploitation annually.

Online child sexual exploitation, or the use of the internet to carry out or facilitate the sexual exploitation of a child, is rapidly becoming a dominant, complex cyber-enabled victim-based crime trend. These offences have a devastating, severe and long-lasting consequence on victims and their families. This report examines two distinct types of online child sexual exploitation:

BOX 1 – **Types of Online Child Sexual Exploitation**

Live-streamed Sexual Abuse of Children (LSAC) – the broadcasting of sexual abuse of children for financial gain. Specifically, the real time transmission or sharing of any material depicting a child in sexual activity, either alone or with other persons, that consumers pay to watch remotely.

Financial Sexual Extortion of Children (FSEC) – the threat of exposing sexually explicit images or video of a child unless they meet financial demands.

The scale, scope and trajectory of these crimes is alarming. At a global level, researchers from the University of Edinburgh estimate that 300 million children around the world, or 1-in-8 of all children, are affected by online sexual abuse and exploitation annually. This estimate goes beyond the crime types profiled in this report but gives a good understanding of the scale of the threat children are facing today. The 2022 INTERPOL Global Crime Trend Summary report found that online child sexual exploitation and abuse was ranked among the top ten crime trends perceived to pose a "high" or "very high" threat by member countries. Not only is this a significant threat to children today, but the trajectory of instances is increasing dramatically. That same INTERPOL report found that 62 per cent of member countries strongly expected these crimes to "increase" or "significantly increase" in the future. In 2024, these crimes remained in the high threat category for member countries, aggravated in particular, since the last reporting period by the increased utilisation and proliferation of technology of encrypted communications.

This report aims to provide an updated and more precise understanding of the financial flows related to online child sexual exploitation through exploring the live-streamed sexual abuse of children and financial sexual extortion of children. This improved understanding will offer opportunities to connect financial transactions to offenders, and earlier detect and intercede in online child sexual exploitation situations.

This report provides good practices in detecting and disrupting online child sexual exploitation. Given the high level of harm present, it is critical that the investigatory techniques used cater to the needs of children at risk and victim-centric investigative strategies are developed and applied. Countries are encouraged to develop investigative strategies that reduce reliance on victim testimony to secure operational outcomes. By putting the victim at the centre of the investigative strategy, authorities can minimise harm, the ultimate aim of crime prevention.

Live-streamed sexual abuse of children and financial sexual extortion of children are in a period of alarming escalation. This report concludes by identifying challenges in detecting, disrupting and investigating online child sexual exploitation, and provides recommendations to stakeholders, including FATF Global Network members, on how they can improve their understanding and ability to combat these crimes in the future.

Introduction

Scope

This report aims to provide an updated and more precise understanding of the financial flows related to online child sexual exploitation through exploring the live-streamed sexual abuse of children and financial sexual extortion of children. This report provides information on detecting, disrupting and investigating online child sexual exploitation. This report uses the following key terms when referring to this activity:

BOX 2 – **Definitions of Key Terms**

Online Child Sexual Exploitation (OCSE) – the many uses of information and communication technology ('the internet') to carry out or facilitate the sexual exploitation of a child. For the purposes of this report, this definition can be used to refer to the totality of OCSE crime types, but it is also used at times to refer to the live-streamed sexual abuse of children and the financial sexual extortion of children collectively.

Live-streamed Sexual Abuse of Children (LSAC) – the broadcasting of sexual abuse of children for financial gain. Specifically, the real time transmission or sharing of any material depicting a child in sexual activity, either alone or with other persons, that consumers pay to watch remotely.

Financial Sexual Extortion of Children (FSEC) – the threat of exposing sexually explicit images or video of a child unless they meet financial demands.

OCSE crimes are part of the FATF Glossary definition of 'designated categories of offences' as they include sexual exploitation of children and can also in some cases involve participation in an organised criminal group, fraud, human trafficking and extortion. Inclusion under this definition means consideration of such crime is within FATF's purview, and a jurisdiction's response to the financial flows and proceeds associated with OCSE could be considered under a jurisdiction's Mutual Evaluation Report where pertinent to their ML/TF risk context.

This report will look at the various components of OCSE, building on the wide body of work from various national and international sources to provide an up-to-date resource for stakeholders to assist them in tackling these financially motivated crimes. It is designed to be used by FATF Global Network members, competent authorities, practitioners, policymakers, financial institutions, designated non-financial businesses and professions, virtual asset service providers, non-profit organisations and any other individuals or bodies with an interest in better understanding the financial flows related to OCSE and detecting, disrupting, investigating, prosecuting and recovering assets linked to OCSE. This report contextualises these crimes, provides indicators of financial transactions and other detection techniques, and identifies good practices and challenges in detecting, disrupting and investigating OCSE.

This report deliberately does not cover similar offences which are not financially motivated.

Methodology

This FATF project was co-led by delegations from Australia and the United Kingdom. The project team consisted of delegations from Brazil, Canada, Côte d'Ivoire, the European Commission, India, Indonesia, Ireland, Luxembourg, Mexico, the Netherlands, Singapore and Spain. The project team also comprised members from the Asia Pacific Group on Money Laundering (APG), the Egmont Group and INTERPOL.

The methodology consisted of a review and refinement of existing available material on OCSE, which included:

- A literature review to identify recent trends in the nature and scope of OCSE. This review focused on LSAC and FSEC, and the financial flows surrounding these crimes, including information from the private sector and civil society submitted by FATF Global Network members.

- Two requests to members of the FATF Global Network to provide relevant material to the project team. These requests included strategic intelligence products, reports and/or case studies that provided information on the characteristics, methods, tendencies or indicators of LSAC and FSEC, as well as examples of current best practices, and innovations to detect, disrupt and investigate OCSE.

There is no reliable figure estimating the proceeds generated by live-streamed sexual abuse of children globally, however, there is clear evidence that this crime type is large in scale and becoming increasingly more prevalent.

Section 1:

The Scale, Demographics and Proceeds of Online Child Sexual Exploitation

Global Context

OCSE is a heinous crime that preys on some of society's most vulnerable people, our children. The emergence of this trend has been fuelled by societal developments – children's access to the internet, social media and gaming platforms and the mobility that modern technology allows for access points to virtually limitless content. These developments have led the children of today to face different risks than children at any other time in our history. OCSE is one such risk, and a risk that has become dramatically more pronounced over recent years.

Although this cyber-enabled victim-based crime type continues to evolve and there is some body of work describing it, its prevalence, and impact, there is not yet a globally codified definition for this crime type. Accordingly, various actors in national governments, international organisations, academia and civil society have made estimates for the prevalence of this activity using slightly different definitions and scopes. Given the different definitions and scopes used for these estimates, there is no globally accepted understanding of the scope and scale of OCSE.

There are however, two striking features of all estimates and research; firstly, that the crime types are highly prevalent and affect a significant number of children in the world today, and secondly, that the trajectory of instances of this cyber-enabled victim-based crime type is rising at an alarming rate.

Scale – At a global level, researchers from the University of Edinburgh estimate that 300 million children globally, or 1-in-8 of all children, are affected by online sexual abuse and exploitation annually[1]. This estimate goes beyond the crime types profiled in this report but gives a good understanding of the scale of the threat children are facing today. The 2022 INTERPOL Global Crime Trend Summary report found that online child sexual exploitation and abuse was ranked among the top ten crime trends perceived to pose a "high" or "very high" threat by member countries[2]. Interpol's 2024 strategic findings show these crimes remained in the "high" threat category for member countries, aggravated in particular since 2022 by the increased utilisation and proliferation of technology of encrypted communications.

Trajectory – The 2022 INTERPOL Global Crime Trend Summary report found that 62 per cent of member countries strongly expected these crimes to "increase" or "significantly increase" in the future[3]. Global law enforcement perceives that the evolution of criminal *modi operandi* to develop child abuse materials, draw in audiences and profits, distribute content at scale, and evade detection has intensified. In addition, Interpol's 2024 strategic findings have underscored the growing number of cases of sexual extortion of children, involving both the coercion of sexual content and financial gain, and European law enforcement agencies report that this threat is becoming increasingly prominent.

These concerning features of the scale and trajectory of this crime type were echoed by the project team of global operational experts who worked on this present report.

These findings of the global scale and trajectory are alarming in and of themselves. However, they become much more concerning when considering this crime type. OCSE has devastating consequences on victims and their families. These consequences impact victims and their families throughout their lives, are often severe and long-lasting, and in some cases have led children to take their own lives. One child facing such consequences of having their life dramatically altered is too many and all stakeholders must bring all available tools to bear to mitigate this risk to children. While it's important, particularly for the FATF, to understand the financial dynamic of this crime type, stakeholders must remember that this is a crime against the dignity of children and there can be no monetary value placed on the damage caused to victims.

1. https://www.ed.ac.uk/news/2024/scale-of-online-harm-to-children-revealed-in-globa
2. 2022 INTERPOL Global Crime Trend Summary Report
3. 2022 INTERPOL Global Crime Trend Summary Report

For the purpose of this report, OCSE has been broken into two very distinctive sub-crimes: LSAC and FSEC. These crimes are different in nature, both in the way that offenders carry them out, and the financial flows of the crime. The following section of this report sets out the characteristics of these two crime types, and the methodologies in which they are conducted.

Live-streamed Sexual Abuse of Children

Methodologies of Live-streamed Sexual Abuse of Children

LSAC is a cyber-enabled crime that covers a range of offences, including sexual exploitation and human trafficking, both of which are considered designated categories of offences in the FATF Glossary. The crime involves individuals performing the following roles to arrange the sexual abuse of the child victim, including forcing them to engage in sexual activity in front of a webcam or camera device:

- **Abuser** – An individual separate to the facilitator who commits the live-streamed sexual abuse of children.
- **Consumer** – An individual who issues a payment to a facilitator to view the live-streamed sexual abuse of children, at times directing the nature of the sexual abuse. Generally based in a separate location to where the contact abuse takes place.
- **Facilitator** – An individual who arranges the live-streamed sexual abuse of children. In some cases, they also act as the abuser.

This abuse is live-streamed to a remote consumer who is paying to view and potentially direct the activities. The consumer that is paying to view the abuse gains access through those people who arrange the abuse and may also be an abuser themselves (the "facilitator" and "abuser" when conducting the abuse). Evidence suggests there are different classes of consumers. Some are habitual consumers while others may be situational consumers, meaning that they were not originally seeking to watch child abuse material.

Consumers and facilitators communicate via messaging applications, including well-known applications such as Skype, WhatsApp, Facebook and Telegram, to arrange a time and date in advance, and to negotiate the price. When the abuse takes place, the abuser subjects the victim to sexual acts and/or forces them to perform such acts and/or incentivises them into participating in these acts, sometimes directed by the consumer in advance of the abuse and/or during the livestream. In some cases, live-streamed abuse is recorded and disseminated online to a broader audience. This practice is sometimes colloquially referred to as "capping". This can be driven by various motives, including that new or unseen child sexual abuse material is a valuable currency within the offending community or to generate further profit, by uploading the capped material to the dark web or cyberlocker sites where the content can be downloaded for a fee. This capping represents further criminality and re-exploitation and abuse of the victim.

Detection of LSAC is difficult since most social interaction platforms have live-streaming capabilities, and content moderators have limited capacities to review massive volumes of real time interactions and chats that are temporary within a volume of millions or hundreds of millions of instances.

LSAC is primarily motivated by financial gain. While the sums involved tend to appear small, the seller may be subjecting the child to repeated online sexual abuse, which may generate substantial profits over time.

Profile of Victims, Consumers, Abusers and Facilitators of Live-streamed Sexual Abuse of Children

Victims

Victims of LSAC are generally not involved in the financial transactions enabling their abuse. They are vulnerable individuals subject to violence that is likely to have a long-term impact on their lives. Victims have not been further profiled, as it is not necessary for the purpose of this paper in supporting stakeholders to use their tools to target consumers, facilitators and abusers.

Consumers

Consumers that pay for LSAC are believed to be typically, male, and while they vary in age, the typical consumers tend to be older men. However, this may not accurately represent the demographics of consumers, as younger consumers may be more adept at concealing their online activity or payments.

Detected consumers who pay for LSAC are predominantly from Australia, Europe and North America[4]. These offenders seek out live-streamed abuse by targeting regions of the world with limited domestic child protection measures and easy access to children. Unlike the abusers and facilitators of LSAC, consumers are sexually, not financially, motivated.

Abusers and Facilitators

Both men and women are abusers and facilitators of LSAC. These roles overlap in some cases and, thus, can share some common characteristics. In cases where the abuser(s) and facilitator(s) are known to the victim (i.e., a parent or relative), they are more likely to be a young woman (mid-20s). In many cases where they are a woman, she has underage children of her own, as well as other children that she may have access to. Where more than one individual is involved in the abuse, offenders may be assigned different roles in the crime, with distinct roles being (1) communicating with the consumer, (2) carrying out the abuse and (3) collecting payments.

The abusers and facilitators of live-streamed sexual abuse are usually based in the same location as the child victim, due to the required proximity to the victim to commit the offence. Based on concluded investigations, a large proportion of abusers and facilitators are found in Southeast Asia. This continues to be a perceived threat in this region[5]. While a large number of victims, abusers and facilitators are concentrated in Southeast Asia, there are cases where the facilitator, abuser and their victim(s) are based in other regions such as North America, Europe and the Middle East and North Africa region. This demonstrates the importance of avoiding limiting the framing of LSAC as a crime that only affects children in certain regions or countries.

Proceeds derived and laundered from Live-streamed Sexual Abuse of Children

There is no reliable figure estimating the proceeds generated by LSAC globally, however, there is clear evidence that this crime type is large in scale and becoming increasingly more prevalent. Concluded cases and victim reporting provide some idea of the proceeds generated through LSAC and how they are laundered.

Transactions relating to instances of this crime are typically characterised by small amounts that are paid from consumers primarily in Australia, Europe and North America to high-risk jurisdictions for child sexual exploitation. The amounts of individual transactions may be considered low to the consumer (normally between 10-200 EUR per instance), but the amounts can be substantial to the abuser and facilitator, who are often based in a developing country. The facilitator may also maximise the proceeds generated from this crime by developing a relationship with the consumer, ensuring that they become a repeat consumer. In some cases, the facilitator may succeed in persuading the consumer to send money for other expenses, such as medical bills.

4. Technical and Financial Sector Indicators of Livestreaming (International Justice Mission, 2020)
5. 2024 INTERPOL Global Crime Trend Summary Report

Payments for these services are typically made to facilitators via popular Money or Value Transfer Services (MVTS), predominantly online peer-to-peer (P2P) payment systems such as PayPal, or sometimes through direct bank transfers or transfers of virtual assets (VAs) through virtual asset service providers (VASPs). The latter can provide even greater perceived anonymity for the consumer.

While organised crime groups are not often involved in these crimes due to the lack of large profits there is some evidence of criminal business structures in developing countries exploiting the commercial opportunities presented by paid LSAC. This includes sharing methodologies for payments.

Facilitators and abusers generally use unsophisticated laundering mechanisms because there is a lack of large profits and a slow trickle of small denomination payments. They include simple conversion of international transactions to cash or bank deposits for day-to-day spending. More significant facilitators and abusers have been observed as purchasing lifestyle goods with their ill-gotten gains, including properties, electronics and cars.

While the financial component may be small compared to other major crime types, uncovering and understanding the financial component of this crime can help operational authorities identify and safeguard victims as well as identify, disrupt and prosecute offenders. It is vital to remember the devastating impact of this crime on its victims throughout their lives, which is often severe and long-lasting, rather than define this crime by the money it generates.

Financial Sexual Extortion of Children

Methodologies of Financial Sexual Extortion of Children

FSEC is a cyber-enabled victim-based crime that combines fraud, extortion and sexual exploitation. Children are not necessarily intentionally targeted but caught by perpetrators seeking to target any and all victims they can. The crime generally involves a victim being initially contacted by an unknown perpetrator over social media. Victim testimony points to victims and perpetrators initially making contact primarily over Snapchat, Instagram and Facebook, but other social media platforms may be more prominent in particular regions around the world.

This unknown perpetrator generally deceives the victim, taking on a false persona, normally that of a teenager or a person in their 20's (also known as catfishing). Perpetrators may create their own false profiles or use existing hacked or purchased profiles. When creating new profiles, they may use bots and scripts, or engagement with other hacked accounts to manufacture evidence of account usage and engagement, leading victims to believe the perpetrator is an authentic user. The perpetrators generally use publicly available images that have been sourced from across the internet.

This perpetrator communicates with the victim using a variety of techniques to pique their interest in the false persona that the perpetrator has taken. The techniques to manipulate the victim are generally deployed very quickly, in minutes or a few hours, rather than much longer-term grooming techniques that are observed in some other child sexual abuse crime types. Once the victims' interest has reached an appropriate level, often encouraged by receiving sexually explicit content from the perpetrator's false persona, they are invited to exchange sexually explicit photographs or footage, or to join a sexually explicit video call that is recorded, or screen captured. This sometimes happens on the same platform where the relationship began, but there is emerging typology that indicates perpetrators attempt to get the victim off the original platform and onto end-to-end encrypted platforms. These attempts are sophisticated, target individuals at a vulnerable time, and have a reasonably high success rate.

Once the perpetrator has the sexually explicit material of the victim, they use this material to threaten or coerce victims to send money (a ransom). Having access to their social media presence, they are able to blackmail victims

with threats of sending the explicit material to their peers, family or others within the online community. These threats are generally aggressive and can involve multiple social media accounts bombarding the victim at once. This quickly applied pressure through social engineering techniques is designed to take advantage of a victim, and quickly convince them to pay a ransom for the images.

This *modus operandi* has proven attractive for perpetrators for several reasons. Firstly, it can be committed from anywhere in the world and can be replicated from any location with internet access and a suitable device. It also generally requires minimal investment of time in any one potential victim. Secondly, the incongruence of investment by perpetrators versus potential threat perceived by victims (i.e., low investment versus the feeling of existential threat) can yield a high return on investment for perpetrators. Thirdly, the perceived anonymity of activities and/or disconnection from the perpetrator's real life allows them to distance themselves from the crimes, including by being generally physically distant from their victim(s). Lastly, the almost unlimited number of potential victims makes this a crime type where perpetrators will always have another opportunity for potential illicit gains in the future.

Profile of Victims and Perpetrators of Financial Sexual Extortion of Children

Victims

Victims of FSEC are mostly teenage males, rather than women or girls as is typical with sex-related crimes more generally, although there is an increasing number of females targeted[6]. Perpetrators may target any victim but are best able to conduct their activities on victims with significant social media connections, such as those that are connected to sports teams, clubs or other social groups so as to identify friends or contacts to whom they can threaten to release the images.

Victims are from all over the world, and as the reporting on this activity accumulates, there is more and more victim representation from all countries. To date, in the international context, most perpetrators have mostly targeted native English speakers as the perpetrators conducting this activity have not reached the sophistication to operate in many languages all over the world. This sophistication may develop over time with the use of emerging technologies, and there are some indications that demonstrate a gradual increase in such sophistication. Cases where perpetrators operate domestically have also occurred all over the world and not only within English-speaking populations, as language barriers do not apply.

Perpetrators

The profile of perpetrators of FSEC varies considerably from that of sexually motivated sexual extortion.
Perpetrators of FSEC generally work alone but groups or teams have been observed using common methodologies. These groups or teams generally involve both males and females though with a very significant proportion of members being male. These organisations act both domestically and internationally, and generally target speakers of their native language and English speakers wherever they may reside. The perpetrators come from varied age groups.

The geographical locations of perpetrators have varied over time with the emergence of this crime type. Perpetrators can conduct this crime from wherever they are in the world. Some of the most affected countries by these perpetrators, such as the United States, Canada and Australia, have conducted analyses of victim complaints. These complaints generally show that Nigeria, the Philippines and Cote d'Ivoire are the most common locations of identified perpetrators.

Some perpetrators use a very basic toolset to commit this crime. Most perpetrators, however, generally have a level of technical proficiency. They can deploy technologies and techniques that provide a degree of anonymity such as VPNs, blockchain technology, screen capture technology, peer-to-peer payment networks and end-to-end encrypted chats.

6. https://www.iwf.org.uk/news-media/news/exponential-increase-in-cruelty-as-sextortion-scams-hit-younger-victims/

Proceeds Derived and Laundered from Financial Sexual Extortion of Children

As with LSAC, there is no reliable figure estimating the proceeds generated by FSEC globally. However, reporting from FATF delegations and open sources[7] show that this crime type is large in scope and it is becoming increasingly more prevalent. Concluded cases and victim reporting provide some idea of the proceeds generated through FSEC and how the proceeds are laundered.

Individual ransoms from victims to perpetrators are perceived to be relatively low value (50-1500 EUR) with initial ransoms generally less than 250 EUR. This may be due to the targeted victims generally being teenagers who do not have significant financial means and are not able to provide high value ransoms, even if demanded by the perpetrators. Perpetrators will sometimes seek further ransom payments from victims after the initial payment, preying on their embarrassment to lock them into indefinite payments. However, such arrangements are generally short lived as disposable cash is quickly depleted, though it is common for victims to thereafter be forced to become money mules for perpetrators.

BOX 3 – **Financial Sexual Extortion of Children Methodology in the Netherlands**

Two Children (B.T. and S.Q.) both received a WhatsApp message from someone they did not know with different numbers. B.T. directly received a message containing a photo with a picture of a woman in lingerie. After he sent back a half-naked picture, he received a Tikkie[8] of €15, which he paid. Quickly a message followed, which made it clear that the person behind the other number figured out who he was (his name and pictures of his Facebook page), based on the name connected to the bank account with which he paid the Tikkie. A Tikkie of €150 followed, including a threat that his picture would be sent to his friends and family if he did not pay. B.T. paid this Tikkie as well. Quickly he would receive even more Tikkies from different phone numbers. The amounts ranged from €20 to hundreds of euros. In total, B.T. paid €3500 worth of Tikkies. B.T. then sent a message saying he was running out of money, after which he was asked to send a screenshot of his bank account overview, for proof. This showed that he had €300 left on his bank account. He was asked to buy gift cards with the money he had left. He had to send the corresponding code of the cards via WhatsApp, so the cards could be used.

The girl (S.Q.) received a picture of a naked man after she had been chatting with the person for a while. S.Q. sent back naked pictures of herself, after which she directly received a message with a screenshot of her pictures, telling her to pay money. If she would not pay, the pictures would be sent to her friends and family. She received a Tikkie of €50, which she directly paid. The person sending the Tikkies found out her name based on the name connected to the bank account tied to the Tikkie payments. More Tikkies followed, which S.Q. paid as well. After a while, she ran out of money, which she needed to prove using screenshots of her transaction overview. These showed that she was lying, so more Tikkies followed. In total, she paid €470 to three different bank accounts within a timeframe of 71 minutes.

Source: The Netherlands

7. https://www.missingkids.org/theissues/sextortion#bythenumbers
8. https://dutchreview.com/expat/tikkie-netherlands/ - Tikkie is an online payment app that allows you to forward payment requests to people via WhatsApp or pay through a QR code. Once you open the request or scan the code, you'll be asked to forward the money through your online banking.

The means of sending ransom payments are generally direct but unsophisticated, reflecting a teenage cohort with limited financial literacy, but who are technologically more fluent and proficient at adopting new payment methods than adults. As with LSAC, ransoms are also paid using MVTS, predominantly online P2P payment systems such as PayPal, or sometimes through direct bank transfers or transfers of VAs through VASPs. The latter can provide even greater perceived anonymity for the consumer. For FSEC, there is a much higher proportion of funds paid to perpetrators in prepaid cards, credits to gaming platforms and gift cards, through which the highest proportion of ransoms are sent. Ransom transactions can be very difficult to detect because the amounts and details of the transactions are generally unremarkable – one large payment service provider found that only a small percentage of payments linked to OCSE had any notes attached, and only a fraction of these notes would raise suspicion.

In addition to payments made directly from victims to perpetrators, there is also evidence of the use of proxies or mules receiving payment on their behalf. In some cases, previous victims act as mules where they were not able to make sufficient payments of ransom.

While the individual ransom payments may be perceived as small, the overall proceeds to perpetrators can be significant given the minimal time investment that is made into each potential victim. Overall proceeds to perpetrators are generally laundered through simple mechanisms such as conversion of the ransom to day-to-day spending. There have been a few cases where third parties have either (1) redeemed gift cards in the country of the victim and sent the value to perpetrators overseas or (2) assisted in the conversion of VAs to fiat to enable perpetrators' access.

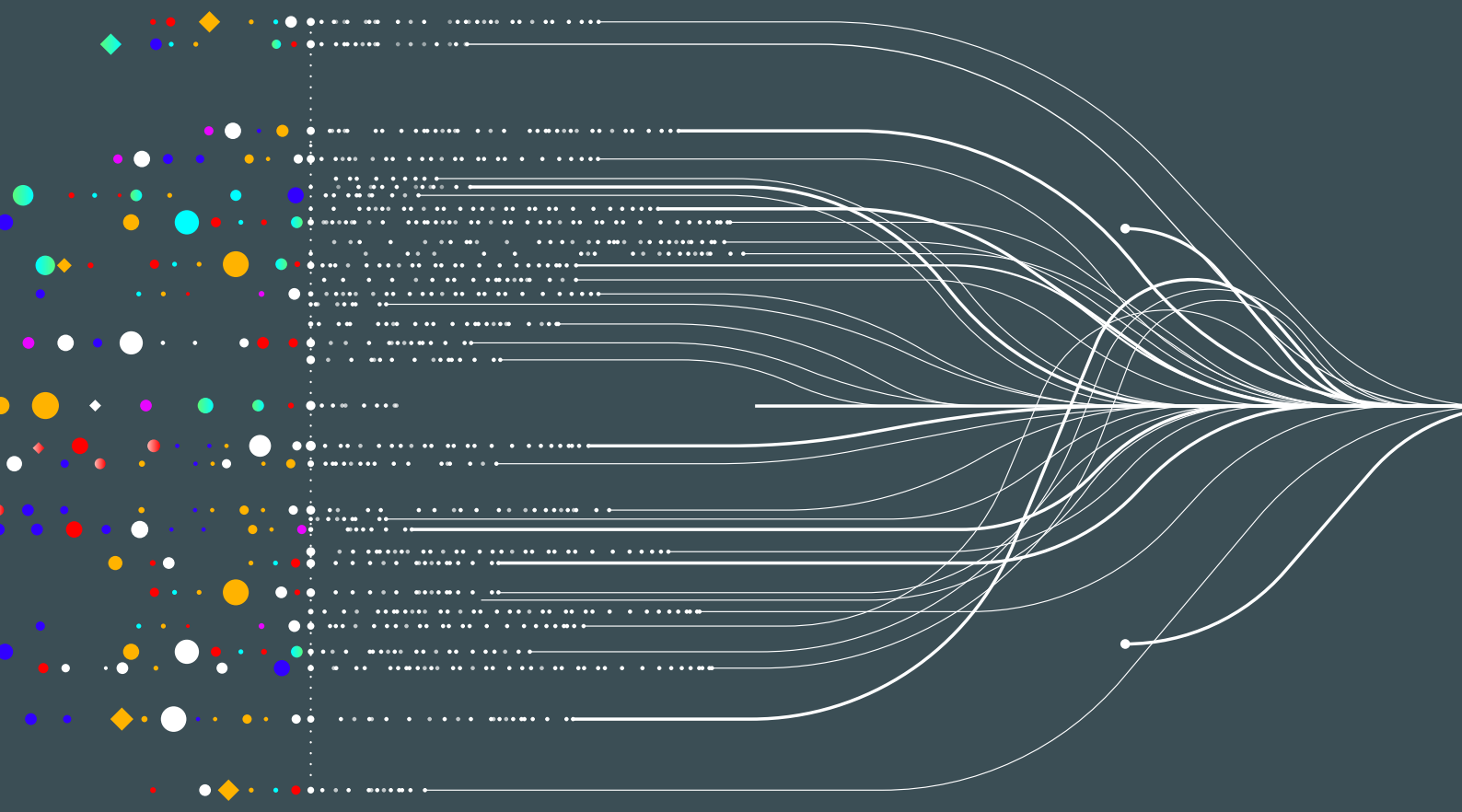
Perpetrators' transaction patterns show that perpetrators spend a higher percentage of funds online than the general population, including general online purchases, application purchases, online gaming and gambling, use of online video and communications technologies and online file storage. Perpetrators obtaining more significant proceeds have been observed as purchasing lifestyle goods with their ill-gotten gains including properties, electronics and cars.

While the financial component may be small compared to other major crime types, uncovering and understanding the financial component of FSEC can help operational authorities identify perpetrators. Financial information can also be critical in identifying instances of such extortion early enough that interventions of support can have a material impact, including saving lives.

It is vital to remember the devastating impact of this crime on its victims throughout their lives, which is often severe and long-lasting, rather than define this crime by the money it generates.

Section 2:

Detection of Online Child Sexual Exploitation



Detection of Online Child Sexual Exploitation through Financial Indicators

This list of indicators is also available in Annex A for ease of use. It should be appreciated that indicators linked to the detection of OCSE are constantly evolving, and jurisdictions should continue to inform and strengthen these indicators through continued collaboration between their FIUs, reporting entities, law enforcement, and other stakeholders.

Identifying Financial Transactions Linked to Live-streamed Sexual Abuse of Children

As outlined above, consumers who pay to view LSAC typically use popular MVTS, predominantly online P2P payment systems such as PayPal. While less common, some consumers make direct bank deposits or transfer VAs through VASPs, and there is evidence of the increasing use of other applications to make payments, such as the all-purpose Grab app available in some regions, or through OnlyFans. The obliged entities providing or facilitating these financial services can detect transactions that may be linked to cases of LSAC by using a combination of the indicators outlined below:

General Indicators of Transactions Related to Live-streamed Sexual Abuse of Children

- Transactions from developed countries to high-risk jurisdictions for child sexual exploitation.
- Significant age differences between remitters and receivers.
- Transactions of low (i.e., 10-200 EUR per instance), even-denominated amounts either in source or destination country currency, or in the virtual asset equivalent of even-denominated fiat amounts (i.e., a virtual asset amount that is equivalent to an even amount of fiat currency).
- Payments being made to receivers in another jurisdiction, with whom the remitter has no apparent legitimate connection.
- Transactions made at irregular intervals but made repeatedly to accounts on the same day or on successive days.
- Transactions made late at night or early in the morning (signalling that the consumer may be in a different time zone).
- Transaction purpose refers to social media or social media usernames, sexual or pornographic terms, or date/time that material was received.
- Extended financial history characterised by payments over a long period, signalling a long-term relationship has formed between the consumer and facilitator.
- Transaction may be described as being for medical or subsistence costs or refer to relationships between the remitter and receiver. For example, descriptors such as "family support", "school fees", "assistance", "support", "medical bills", "accommodation", "education", "financial assistance", "gift", "purchase of clothes", "purchase of toys", "uniform", "friend", "boyfriend", "girlfriend", or "sponsor".
- Purchases at vendors that offer online encryption tools, VPN services, software to clear online tracking, or other tools or services for online privacy and anonymity.
- Accounts or customers that have a high volume of transactions to Facebook, Microsoft, Google Play, OnlyFans, TikTok, Instagram or other social media sites (such as Micous).
- Transaction linked to an individual on a public registry of sex offenders.

Transactions Conducted by Consumers

- Transactions conducted to accounts in, or accessed in, high-risk jurisdictions for LSAC (e.g., accounts accessed via ATM cash withdrawals, or account logins through IP address in a jurisdiction of concern).
- Purchases on dating platforms or platforms that offer adult entertainment content.
- Purchases on webcam/livestreaming platforms, including those providing adult entertainment.
- Purchases on online gaming platforms or gaming stores.
- Purchases of video capture software.
- Funds sent to or received from an individual 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.
- Transactions linked to an individual who is the subject of adverse media involving child sexual exploitation-related offences.

Transactions Conducted by Facilitators/Abusers

- Money remittances are usually withdrawn immediately.
- Receivers are under investigation by law enforcement for the suspicion of being part of facilitating online child sexual exploitation.
- Payments for premium features or services on social media platforms.
- Purchases of video capture software for use on websites or social media.
- Transactions on online gaming platforms or gaming stores.
- Acquisition of spyware or surveillance applications.
- Multiple deposits of similar amounts traced to foreign sources, particularly from high-risk LSAC consumer countries, including deposits from these foreign sources at the same or similar time.
- Payments to online file hosting vendors/platforms.
- 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).

While one of the above indicators in isolation may not necessarily signify payments relating to potential cases of LSAC, using a combination of indicators and other relevant factors regarding transactions and clients can help obliged entities to observe patterns that may signal suspicious activity.

Identifying the Financial Sexual Extortion of Children through financial transactions

As detailed above, the majority of victims report having paid ransoms to facilitators via MVTS (predominantly online P2P payment systems such as PayPal), bank transfers, VAs through VASPs or gift cards. The obliged entities providing these services have the capability to spot transactions that may be indicative of FSEC by using a combination of the indicators listed below:

General Indicators of Transactions Related to Financial Sexual Extortion of Children

- Transactions conducted between two individuals where there is no apparent relationship (i.e., no common surname, no clear business purpose).
- Transactions generally of less than 500 EUR, but sometimes ranging up to 1500 EUR in even-dominated amounts.
- Initial transaction between remitter (victim) and receiver (perpetrator) generally less than 250 EUR.
- Multiple transactions from a remitter to a receiver over a short period of time and then stopping entirely.
- Transactions conducted to a common country of operation of perpetrators of FSEC (i.e., Cote d'Ivoire, Nigeria, Philippines etc.). Obliged entities should take note of the shifting trend of countries where this is predominantly taking place over time.
- Transaction purpose refers to social media or social media usernames, sexual or pornographic terms, threatening/pleading language or date/time that material was received.
- The transaction recipient is not local to the remitter.
- Payment details appear like a charitable donation.
- Transaction linked to an individual on a public registry of sex offenders.

Transactions Conducted by Victims

- Transactions that are conducted by a teenage or young adult male and to a lesser degree teenage or young adult female.
- Transactions originating in primarily English-speaking countries, if international. Obliged entities should note that this will become less of a marker over time as facilitators become more sophisticated.
- Receipt of complaints from individuals about transaction links to sexual extortion.
- Payments typically occurring between 7pm and 7am (usually as the sexual extortion is happening in real time).
- The remitter (victim) does not enter a payee name (i.e., only enters a general label for recipient) or enters a payee name that does not match the actual account holder.
- Diminishment of funds in the remitter's accounts within a matter of hours (usually less than 24 hours).

- Uncharacteristic purchase of digital gift cards or gaming credits.
- Uncharacteristic uses of individuals' P2P platform accounts.
- Uncharacteristic purchase of VAs.
- When questioned by bank staff, the remitter is evasive or offers an implausible explanation for the activity.
- Customer purchasing multiple gift cards (for example, Amazon, PlayStation or other gaming providers).

Transactions Conducted by Perpetrators

- An account receiving multiple apparently unlinked transactions.
- Receiving account having multiple unlinked rationales identified for the transactions being received by the account.
- Amounts received quickly removed from account.
- Payments to online services offering privacy and/or anonymity (i.e., encryption, VPN, virtual phone numbers, etc.).
- Payments associated with multiple pre-paid credit cards or gift cards.
- Receipt of funds from multiple online file hosting marketing services (e.g., pay-per-download models) across different jurisdictions.
- Purchase of goods (vehicles, real estate, household appliances) in a short period of time, subsequent to receiving money, without justification for the means used.
- Persons with a lifestyle and consumption that is not consistent with the income earned from their work activity.

It is important to note that any one of the indicators listed above is insufficient to raise suspicion of a potential financially motivated sexual extortion attempt, but that obliged entities should consider all factors surrounding a transaction and whether the transaction meets a number of the indicators described above.

Section 3:

Investigating Online Child Sexual Exploitation

Detecting and Identifying Live-streamed Sexual Abuse and Financial Sexual Extortion of Children

Reporting by victims is a key avenue for detection of many crimes, but this is not the case for OCSE. For FSEC, while reporting by victims can be a means of detection, victims often feel embarrassed and are vulnerable to extortion because they want to prevent others from knowing they have shared explicit images. This can extend to them not wanting to report the extortion taking place, and intelligence has demonstrated that FSEC is a vastly underreported crime.

Victim reporting is an even less common means of detecting LSAC. This is due to barriers related to the profile of the victims, for example their age, vulnerability, access to means of reporting, but also due to factors such as coercion or familial relationships being present in the abuse environment.

The barriers to detecting LSAC and FSEC through victims reporting mean financial transactions and information are a critical resource in detecting OCSE. However, this is not the only means of detection. Delegations also highlighted the role of referrals from the private sector and online undercover work, among other methods of detection. In the case of LSAC, the overwhelming method of detection, of either consumer or facilitator activity, is the receipt of intelligence from other countries.

Using Financial Information

Section 2 sets out the indicators that can be used to identify transactions related to LSAC or FSEC. Reporting these identified transactions to Financial Intelligence Units (FIUs) and law enforcement is a critical means of detecting OCSE.

Financial intelligence obtained during investigations or via FIUs also plays a key role in detecting and disrupting offenders who travel internationally to commit sexual offences offshore. The Australian Federal Police's experience shows that a large proportion of LSAC consumers will go on to contact offend offshore. When overlayed with other data sources, such as CyberTipline reports from the United States' National Center for Missing and Exploited Children (NCMEC), financial intelligence can assist to build more accurate profiles of possible offenders, which can in turn be shared with domestic border security agencies – to potentially prevent possible offenders from leaving the country or to identify travellers for closer scrutiny upon their return – or shared with international law enforcement partners for consideration and potential action in local jurisdictions.

For financial institutions, there are further opportunities to detect LSAC and FSEC. A leading Southern Hemisphere VASP is an example of going beyond just strict transaction monitoring rules in their commitment to tackling OCSE, deploying expansive risk indicators, staff education and engagement with key industry partners, law enforcement and government as key mitigation strategies.

What sets this VASP apart, however, is the high level of customer engagement as a key mitigation strategy. Employees conduct engagement throughout the lifespan of an account and have a large workforce dedicated to verbal and online customer engagement. This human touch approach allows for increased understanding of how a customer intends to use the VASP's platform and better oversight when their trading patterns change, enhancing their ability to detect high risk behaviours or circumstances that may otherwise go undetected, such as when their customers, or potential future customers, are being sexually extorted. Once extortion is suspected or detected, this VASP works closely with their relevant FIU to submit a suspicious activity or transaction report and refer the concern to safeguarding authorities. These authorities arrange for local law enforcement to undertake a welfare check at the home of the customer, who is also encouraged by the VASP to report the matter to the police.

BOX 4 – **Using Financial Information to Investigate OCSE**

Indonesian FIU (PPATK) Leveraging Financial Information

Based on information received by PPATK, a New Zealand citizen, Mr. X was shown to have sent funds to the Philippines, Vietnam, the United Arab Emirates, and Indonesia since 2021. The transactions are suspected to be for payment of images related to child sexual exploitation. The transaction descriptions include "gift," "photos and fun", and "test transfer". PPATK's database found that Mr. X actively made transactions to female individuals in Indonesia with small amounts of recurrent frequency. One of the recipients of funds, named Ms. A, often used suspicious transaction descriptions such as "byr amer" and "bayar room" and transacted with those with profiles of owners and employees in the hotel, karaoke, and entertainment sectors. Ms. A also lives in a tourist area, Bali, which is prone to cases of OCSE. Ms. A received funds from male individuals in several countries through money remittances totalling IDR 173 million (approximately €10,000).

Source: Indonesia

Canada's Project Shadow

Project SHADOW is a Canadian public-private partnership co-led by Scotiabank and the Canadian Centre for Child Protection, supported by Canadian law enforcement agencies and FINTRAC, Canada's FIU, to combat online child sexual exploitation. Through this public-private partnership, FINTRAC was able to identify and share financial indicators to support reporting entities in recognizing financial transactions suspected of being related to the laundering of funds linked to OCSE.

FINTRAC's financial indicators were used in a case of FSEC, where a victim sent a sexually explicit video of themselves to an individual they met online. The individual (perpetrator) then threatened to circulate the video if they did not send the perpetrator $400.00 CAD. The victim sent the money, and the incident was also reported to law enforcement, who then submitted information of the offending to FINTRAC.

In parallel, the transactions were also flagged by a reporting entity as a result of the OCSE indicators developed by FINTRAC. Through this public-private collaboration, FINTRAC was able to determine the flow of related illicit funds and provide law enforcement with account numbers at various Canadian banks and other personal identifiers, which have been used by law enforcement to support the investigation against the perpetrator.

Source: Canada

Another example is the partnership between the National Australia Bank (NAB) and the Australian Federal Police led Australian Centre to Counter Child Exploitation (ACCCE) to develop means to proactively detect suspected child sexual extortion payments in near real time.

NAB created daily alerts for potential child victims of sexual extortion, primarily targeting victims that have not reported the incident, but where the financial indicators of FSEC are present. Alerts are triaged each business day, and where potential victims are identified, they are disclosed to the ACCCE, who make outbound calls to the victims. One such victim was identified, by indicators such as payments to new payees late at night, and exhaustion of funds in a single night. This led NAB to refer this information to the ACCCE within a few hours of the transfers being made. The direct feedback from the ACCCE to NAB demonstrates the impact of near real time identification:

> *"I can confirm that [victim] was indeed the victim of sexual extortion, having spoken to him and his mother in [location].*

We greatly appreciate your [NAB's] alerting feature as [victim] had not reported to the authorities and was still being pressured by the scammers – even during our telephone conversation. I am pleased that he now has the appropriate support and will no longer be engaging with the scammer/s.

I have reported the offending social media account for take down.

[victim] said that he had spoken with a representative from National Australia Bank about the payments."

These are not isolated cases or successes, but proven methods for successfully disrupting this criminality and enabling the provision of support to the victims.

Referrals from the Private Sector

Both LSAC and FSEC fundamentally depend on online infrastructure to facilitate the offences. Relevant infrastructure for OCSE includes social media platforms, internet services providers, mobile network operators, messaging applications, cloud services, content distribution networks, browsers, and app stores, among others. This private sector infrastructure, or as categorised by the United States' NCMEC, electronic service providers, is in a particular position to detect OCSE directly, and in some cases, in real time.

In most jurisdictions, private sector entities are obligated by law to cooperate with law enforcement and report where suspicion or instances of criminal activity is identified. However, efforts to proactively detect OCSE or related material is generally less explicitly required. In cooperation with the private sector, authorities should ensure appropriate protection of information, particularly where of a confidential or sensitive nature.

Many providers of this infrastructure are taking seriously the need to address the use of their services to conduct OCSE and identify behaviour reportable to law enforcement where it is occurring.

NCMEC's CyberTipline is a US-based non-profit organisation that can serve as a channel for electronic service providers to file reports of suspected OCSE in the United States as well as other jurisdictions, which are then made available to law enforcement around the world. These reports can be critical to detecting and investigating OCSE.

Though nearly 36 million CyberTipline reports of suspected online sexual exploitation of children were made to NCMEC in 2023, these were from only 245 companies, with 5 of these companies accounting for more than 91% of the reports. In addition, not all reports received were of sufficient depth or quality to provide utility to law enforcement. Only those where the reporting company provides sufficient information, such as details of the user, including, if possible, their location, can lead to a referral to law enforcement and result in action to identify and safeguard the victims involved. Poor quality reporting has the additional detriment of adding to the volume of reports to be analysed, burdening NCMEC or other equivalent bodies, but without contributing to meaningful detection. Despite these opportunities for improvement, the CyberTipline reports provide investigators with tangible, timely and actionable leads. Countries outside of the United States regularly use NCMEC information and have taken steps to better use this in combination with other domestically sourced information to great effect.

BOX 5 – **Detection and Investigation using CyberTipline Reports**

NCMEC's CyberTipline Reports

NCMEC's CyberTipline is a centralised reporting system for reporting the suspected online exploitation of children. The public and electronic service providers can make reports of suspected online enticement of children for sexual acts, child sexual molestation, child sexual abuse material, child sex tourism, child sex trafficking, unsolicited obscene materials sent to a child, misleading domain names, and misleading words or digital images on the internet.

NCMEC staff review each tip and work to find a potential location for the incident reported so that it can be made available to the appropriate law enforcement agency for possible investigation. NCMEC also use the information from its CyberTipline reports to help shape its prevention and safety messages.

Source: National Center for Missing and Exploited Children

Norway's Use of CyberTipline Reports

NCMEC reported Person A to the Øst police district and Norway's National Criminal Investigation Service on suspicion of the payment for live-streamed sexual abuse of children under the age of 14 years from the Philippines. Norway's competent authorities developed adequate rationale to review the electronic devices of Person A. During the review of his mobile phone and computers, several chats were found that showed that Person A was indeed paying to watch live-streamed sexual abuse of children under the age of 14 years from the Philippines.

As a result of this investigation, Norway shared information with the Philippine authorities about the facilitators from whom Person A had streamed the abuse. As a result, the Philippine National Police arrested at least five facilitators and safeguarded several children from further sexual abuse.

Person A was sentenced to 14 years in prison and had to pay compensation for damages to two of the victims, totalling NOK 500,000 (approx. 42,000 EUR). He was also sentenced to forfeit four USB drives, an Apple iPhone X, an iPhone 5s, and a Dell desktop computer to the national treasury.

Source: Norway

Many private sector entities take the approach of screening for Child Sexual Abuse Material (CSAM), which can be created through the capping of LSAC or sexually explicit images extorted via FSEC. A key tool for this is hash-based detection technology. A hash is a digital fingerprint that is unique to individual content. Hashes of known CSAM can therefore be stored in secure databases, for companies to compare content against and quickly identify previously identified CSAM material. Machine learning can also be utilised to flag suspected but previously undetected material, which after being confirmed by human reviewers, can be reported to law enforcement and fed into the secure hash databases that underpin the hash detection technology. User or third-party reporting of content is another means of detecting CSAM material.

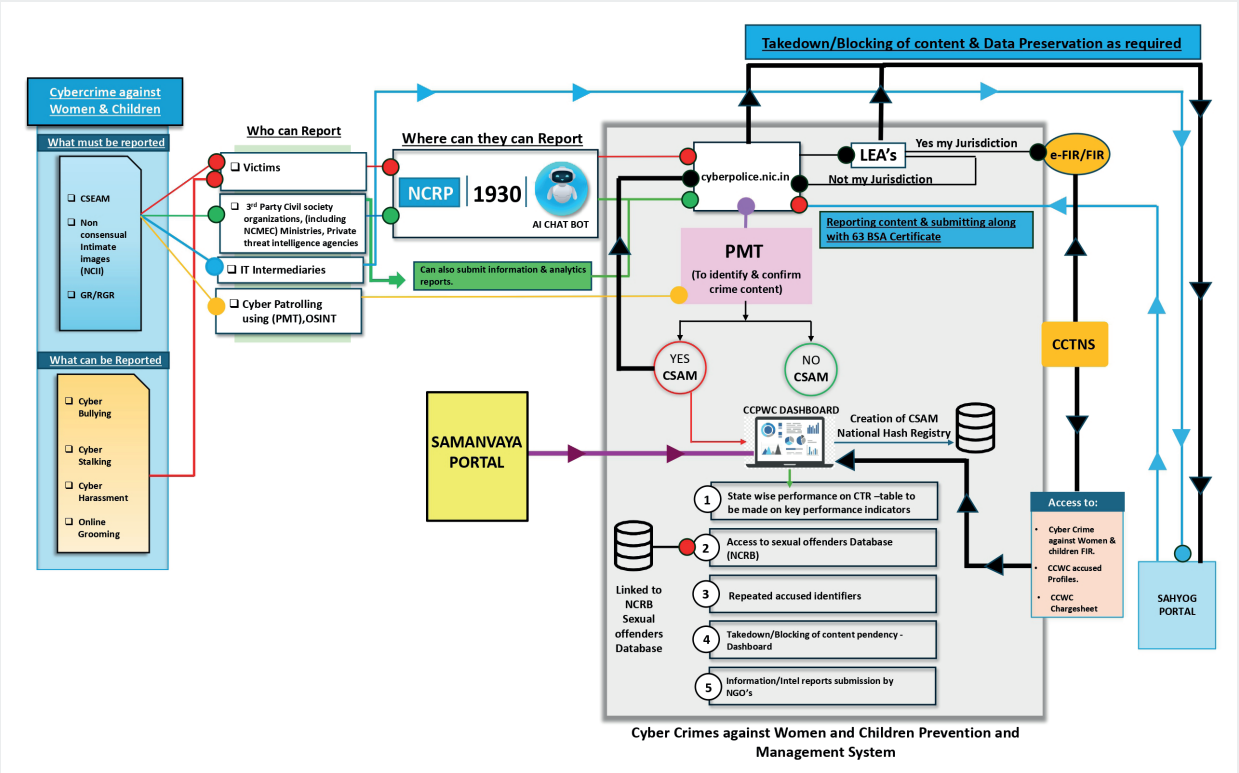
Though hash-based detection, user/third party reporting and machine learning to detect new CSAM material could be effective in limiting re-exploitation via the sharing of capped or extorted child sexual abuse content, they have limited effectiveness in detecting LSAC or FSEC. The nature of LSAC, which disappears with little, or no trace left behind, means it is not captured by many of the screening mechanisms used by online infrastructure providers. Images related to FSEC are often contained within the privacy of direct person to person conversations or messaging and so are also less vulnerable to such screening. The increasing rollout of end-to-end encryption of video communication channels, and communication channels more widely, will make detection of LSAC and FSEC even more difficult.

BOX 6 – **India's 1930 Take Down System**

India's "1930 Take Down System" is a structured framework and platform for addressing various cyber-enabled crimes, including OCSE. Victims can report these offences through the cybercrime portal (www. cybercrime.gov. in) or the dedicated 1930 helpline, after which the reports are processed through the portal. All reports are sent to cyberpolice.nic.in, which connects to the law enforcement agencies (LEAs) dashboard for further investigation and action. India's LEAs, using this dashboard, coordinate take-down requests of harmful content, reported by specially focused bots on social media and other online platforms.

Tips from other sources, like NCMEC, are added and analysed through AI-based filtering tools, helping LEAs identify pertinent cases. These cases are then stored in the Cybersexual Offender Database, which assists in tracking known offenders and preventing recurrences. This data is also integrated into a broader dashboard for real-time monitoring, mapping, and managing cases across regions, enhancing the efficiency of response and coordination by LEAs.

Proposed Architecture



Source: India

Closer public-private partnership, and private-private partnership is one means to support detection in light of these challenges and detect not only individual cases but networks of offenders.

The Lantern Coalition[1] is an example of such partnership, where an alliance of global technology companies works together to combat online child sexual exploitation. As OCSE activity frequently occurs across multiple online platforms, the initiative facilitates companies working together to uncover the full picture. It provides a means for

1. https://www.technologycoalition.org/newsroom/announcing-lantern

companies to securely share signals about activity and accounts that violate policies against child sexual abuse and exploitation, allowing other platforms to then conduct their own screening for these signals, and, where appropriate, lead to reporting of suspected criminal activity to NCMEC. While the signals are not proof of abuse or extortion of children, they aid, and can be crucial pieces of the puzzle, in uncovering real-time threats and harm to victims.

Online Undercover Work

The high level of harm present in many cases of OCSE and the nature of these crimes means that, in certain cases, it can be proportionate and appropriate to use covert means to detect and identify the commission of OCSE crimes. In some cases, law enforcement may pose as children themselves, or as potential consumers in cases of seeking to detect LSAC, to build relationships with facilitators, abusers, consumers, and perpetrators to collect information, evidence, and identify victims.

The actions performed by law enforcement during online undercover operations should be in accordance with the basic principles of existing laws, policies and procedures, and all undercover officers should be screened and highly trained before engaging in such operations.

Best practices in Investigating and Disrupting the Live-streamed Sexual Abuse of Children and Financial Sexual Extortion of Children

There is a mixed level of understanding and prioritisation internationally in investigating and disrupting OCSE, in part reflecting its geographic dispersion. The increasing scale and spread of these crimes, however, make it highly relevant to develop and share best practice on how to investigate these crimes and proactively disrupt where possible.

The good practices in both investigation and disruption are based on country examples contributed to this project by jurisdictions and on information available in the public domain. Both demonstrate the need to take a multi-faceted approach that focuses on domestic and international partnerships, specialist expertise, innovation, and technological and financial developments. As previously stated, it is critical that investigatory and disruption techniques cater first and foremost to victims in trauma-informed systematic responses.

Investigating

Victim-centric investigative strategy

Given the high level of harm present, it is critical that the investigatory techniques used cater to the needs of victims through a trauma-informed response and a victim centric investigative strategy is applied. The priority in investigations must always be the safeguarding of children, even if there is potential to disadvantage evidence gathering opportunities for potential criminal investigation and, as such, mechanisms to manage risk should always be in place.

In taking this victim-centric strategy, countries are encouraged to develop investigative strategies that reduce reliance on victim testimony to secure operational outcomes. Approaches based on financial intelligence, and payment interception, can hold potential in providing less distressing routes of investigation and reducing reliance on often re-traumatising victim testimony.

The high level of harm related to this crime means it is also imperative that law enforcement have intelligence development processes that minimise potential time delays, to enable swift victim identification and victim safeguarding as quickly as possible.

Given the need for specific approaches to investigating these crimes, there is benefit in having dedicated investigative expertise to facilitate this. In the UK, there is a specialist police programme, the Hydrant Program, that exists to support police forces across all child protection and abuse investigation issues. The Hydrant Program acts as a hub for specialised knowledge and expertise, providing guidance and support on investigating contact and online sexual abuse and exploitation. Their practical guidance on investigating OCSE, updated yearly, provides for a standardised and consistent law enforcement response to the investigation of these complex crimes, including financial aspects such as the use of Suspicious Activity Reports (SARs) or Suspicious Transaction Reports (STRs).

Using information and evidence sources unique to this crime type

Standard use of information and sources of evidence apply to investigating these crimes, for example, a broad range of domestic data can be used in victim and offender identification, such as immigration and tax data, information on national welfare payments systems, locally held crime and intelligence data, health and social care data and criminal records data.

However, there are specificities to the evidence and information relevant to investigating LSAC and FSEC. For example, the generally international nature of these crimes, means that information often needs to be deployed across borders and the evidence is often inherently cross-border, i.e., communications between LSAC consumers and facilitators/abusers, or between perpetrators of FSEC and their victims. However, these crimes can also take place wholly domestically.

Another specificity is the critical role of communications data, in both LSAC and FSEC. Feedback from law enforcement agencies indicated that initial referrals regularly only identified usernames, IP addresses and email addresses suspected to be linked to OCSE. Therefore, to translate these referrals into identification of victims, and offenders, it is imperative that LEAs engage with authorities responsible for access to communications data.

Such engagement is also key given the frequent role of online chat correspondence as a form of evidence in cases of OCSE. Skype or Facebook, for example, are common sources of evidence in demonstrating engagement between consumer and facilitators and tying financial flows to the commission of LSAC.

In the case of Operation O by the UK's National Crime Agency, the investigation was triggered by an intelligence package including not only financial transactions and child sexual abuse material video/images, but also Skype chat. However, given the delays experienced in accessing communications data, authorities should be mindful of developing intelligence that is not solely reliant on communications data.

Investigations of these crimes can be difficult to navigate due to their nature as enabled by continually advancing technologies. Movement, for example, towards broader end-to-end encryption of communications, including video streams will further shield livestreams from screening. However, technological advancements also offer an opportunity for law enforcement in investigating. The National Special Crime Unit in Denmark experimented with the use of facial recognition technology by police to compare images of victims with images from a database of previously identified victims. This technology has now been implemented as a permanent tool to increase the speed of victim identification in child sexual abuse and link together cases. This increases the chances of stopping ongoing abuse and further distribution of material, in cases where capping has occurred, for example.

Initiating multi-agency task forces

Where large, and particularly international, investigations are undertaken, use of multi-agency task forces should be considered to ensure the effective handling of the investigation. These should take a strategic approach to intra-agency and inter-agency cooperation to support information and intelligence sharing, particularly with international

counterparts, where strong working relationships were demonstrated through case studies to be critical in uncovering wider networks of OCSE offenders and victims.

Task forces should seek to ensure they have appropriate expertise, and therefore include representatives experienced in, for example, digital forensic investigation, financial investigations, investigating the specific type of OCSE, and, where dealing with victims directly, child safeguarding. In some cases, country law enforcement work closely with non-profit organisations to benefit from their experience and to directly connect victims with support services, for example the Danish police collaborates with Save the Children, while Hong Kong, China has undertaken a joint investigative operation with a non-profit organisation that led to the successful apprehension of a suspect.

There are also examples of multi-agency task forces stretching internationally in aid of investigating, and identifying victims, of OSCE. Since 2020, the ACCCE, has hosted Victim ID Taskforces of domestic and international law enforcement to analyse material to identify victims of child sexual abuse. Specifically, in 2022, one such task force, was created to target the most active capping criminals on dark web forums. Capped material from these targets was analysed through the task force, with participants from Australia, Canada, New Zealand, Norway, United States, Europol, and Interpol, among others, working together to identify victims in the capped material. As a result of this, 77 victims were referred to 12 different countries as well as 10 offenders being referred. As of October 2024, 4 of these offenders have been arrested as a result of the analysis conducted.

In addition to these task forces, countries could consider developing a strategy to enhance co-operation between the public and private sectors beyond their reporting obligations. The private sector as the owner of financial, communication, or other data, with the ability and the expertise to process it, may often have better visibility of OCSE activity occurring than law enforcement. Information exchange should always be undertaken within legal parameters and with adequate protection of information and rights to privacy. Within these caveats, information exchange should be enhanced between the sectors to better and more effectively identify activity that may assist law enforcement in conducting investigations of OCSE.

International cooperation

Enduring across both investigation of LSAC and FSEC is the fundamental importance of strong and effective international law enforcement and FIU cooperation. Though both crimes can occur entirely domestically, more frequently they are not bound by physical borders and can flourish in the economic disparities between countries. In the case of LSAC, international cooperation is the foundation of most investigations, and critical in this specific crime where criminality occurs at both ends of the financial flows, and investigation is required of both the consumption and facilitation of abuse.

As such, sharing of referrals and intelligence among agencies on the consumer and facilitator, or victim and perpetrator, sides is especially effective. The abovementioned Operation O in the UK initially led to identification of a consumer of LSAC in the UK, but close collaboration and exchange of intelligence with authorities in the Philippines is what was crucial in identifying further facilitators and victims, several of which were able to be safeguarded as a direct result of this investigation. Law enforcement leads involved noted that key to the success of the investigation was the strong relationships built with their international partners. In another example provided earlier, information shared with the Philippines, following an investigation in Norway into a suspect making payments to a known facilitator in the Philippines, lead to the arrest of at least five facilitators and safeguarded several children from further abuse. The disruption, investigation and potential arrest of facilitators also frequently results in intelligence that identifies other consumers that have been sending them payments, which often otherwise would have gone undetected.

BOX 7 – **Operation Cyber Guardian**

Between 26 February 2024 and 29 March 2024, the Singapore Police Force, Hong Kong Police Force and Korean National Police Agency commenced an international joint operation, Operation Cyber Guardian, and collectively arrested 272 persons from 236 locations across the three jurisdictions for OCSE-related offences. During this month-long operation, these international partners detected cases of OCSE and safeguarded several children held in captivity. Operations Cyber Guardian illustrates the importance of international cooperation, and for law enforcement agencies to continue taking tough, decisive, coordinated and transnational enforcement actions against OCSE activities.

Source: Singapore, Korea and Hong Kong, China

BOX 8 – **Acting on Proactive Dissemination of Intelligence**

Police in Jersey received an intelligence package from a third country following the disruption of a Philippines based child trafficking network. The investigation identified a male suspect from Jersey who had made contact with the network and made payments for online child sexual abuse images. The male suspect was also discovered to have travelled to the Philippines to abuse children in person.

Skype video conferencing software was found to have been used and examinations of Skype text chat conversations indicated that the male suspect had been communicating with female children and paying them to perform sexually explicit shows. Conversations were also located suggesting the suspect viewed sexually explicit live shows involving children. The suspect sent payments via PayPal to the network for viewing the live abuse.

Chat logs showed that the suspect sent money in the Philippine Peso to various individuals. Many payment references were identified along with details of how the facilitator could collect the payment. Other Skype text chat conversations showed that the suspect had made payments to add credit to various mobile phone numbers. The phone numbers and mobile operator details were provided to him by the network. These payments appear to be payment for consuming sexually explicit live shows on Skype and for the receipt of child sexual abuse material.

Further electronic evidence was located indicating that the suspect was arranging or attempting to arrange to meet females whilst in the Philippines, including children. The suspect offered to pay for the transport costs for the females to get to his hotel. He indicated that he would pay cash to the females on meeting them in person.

Upon seizing the suspect's electronic devices, the details of the suspect's internet searches were examined. The searches included terms indicating searches for child sexual abuse material. Other internet searches were also located relating to money transfer services and money collection services in the Philippines. Evidence was located showing the suspect paid for VPN services which provided online anonymity.

The suspect was subsequently convicted of being in possession of indecent images of children. He died in prison.

Source: UK Crown Dependency of Jersey

The critical nature of effective international cooperation is further demonstrated by the impact of its absence. In some cases, information is provided to other jurisdictions but with restrictions or limitations in how it can be utilised. This can prevent authorities acting on the information which can allow consumption and commission of child sexual abuse material to continue for years. In one case, financial intelligence demonstrating a consumer was making payments to livestreaming facilitators was provided to the suspect's country of origin but with restrictions on how it could be used. Despite repeated attempts to secure release of this intelligence for use, because this was not provided the suspect was able to continue to commission the sexual abuse of children for a further four years.

In other cases, restriction around the use of material provided by international partners, such as limitations on its use in court, meant that although suspicious activity was reported and intelligence disseminated, investigative measures could not be initiated, again potentially allowing OCSE to persist by preventing disruption.

It is imperative that countries proactively develop contacts and networks that support sharing of intelligence, both financial and otherwise, where links arise with other jurisdictions and do so in a manner that ensures the receiving country can assess the extent of criminal activity and use the information to its full extent. The FATF Standards already set out characteristics of effective international cooperation, to ensure this delivers appropriate information, financial intelligence, and evidence to facilitate action against criminals. These Standards serve as a useful guide for effective cooperation related to OCSE financial activity.

Parallel investigations

This report has found that proceeds and flows involved in LSAC and FSEC are often modest, particularly in comparison to other proceed generating crimes, however, investigations should still look for opportunities to investigate money laundering (ML) offences in addition to focusing on the OCSE primary offence. Particularly given there is some evidence of criminal business structures in developing countries increasingly exploiting the commercial opportunities presented by paid LSAC, and the presence of organised scam networks and groups.

Parallel investigations focus on the investigation of the OCSE predicate offence and the ML offence simultaneously[2]. The concept of having parallel investigations brings together expertise from both investigative backgrounds which is complementary and ensures offences are fully investigated.

Conducting parallel financial investigation of the OCSE offence can allow identification of the proceeds of crimes (i.e., criminal assets). Most critically, though, in the case of OCSE, the financial investigation can provide the link between the source of money, who receives it, when it is received, and where it is stored or deposited, as proof of criminal activity. They can also aid competent authorities in uncovering and identifying all the participants in a criminal enterprise, for example, the facilitators and abusers linked to an identified consumer, or the networks that can be involved in FSEC.

Countries can consider including in their standard operating procedures for investigative agencies a form of checklist or outline of the essential elements for conducting investigations of the financial elements of OCSE crimes, and where relevant, related ML offences. This can help structure each financial investigation and be used as a guideline for investigators.

The FIUs should also be utilised as the subject matter experts where appropriate in investigations. The UK's Hydrant Program as mentioned above, plays a key role in directing policing teams to bring in FIU support in investigating complex OCSE cases. Countries should also consider whether there is benefit in training investigators focused on OCSE offences on relevant aspects of ML and financial investigations.

The level of the proceeds of OCSE and how they are used, often to meet basic needs, means investigating related ML can be inherently difficult. However, parallel financial investigations should still be undertaken, including as there could be involvement of organised criminality, and there are examples where proceeds have been used to purchase luxury goods and other assets, not just to fund basic needs. These parallel investigations are also important in facilitating use of asset recovery laws, which as discussed in Section 4, should be considered as part of the investigation and litigation strategy taken in cases of OCSE offences.

2. Operational Issues - Financial investigations Guidance

Disruption

Both the high level of harm generated by OCSE, and the challenges in it being detected, reported, and hence investigated, mean there is a central role for systematic initiatives to disrupt OCSE, not just initiatives which disrupt individual cases. Two avenues for disruption of OSCE are financial disruption and infrastructure disruption.

The financial motivation for LSAC and FSEC mean their commission is fundamentally driven by their ability to generate proceeds for offenders. Offenders are therefore highly reliant on services that facilitate the movement of funds and access to their proceeds of crime. This reliance offers an avenue to disrupt OCSE, by disrupting the financial vehicles and flows that underpin and drive it. In the case of LSAC, where the receipt of a payment is a trigger for an act of sexual abuse, even the disruption of a single transaction can have a monumental impact.

Operation Huntsman in Australia, led jointly by AUSTRAC (FIU), and the ACCCE, is an exemplar of successful disruption of the financial infrastructure underpinning FSEC, with a secondary impact on organised crime more widely, for whom FSEC is only one of their streams of criminal income. The design of Australia's financial system requires the involvement of an adult to move funds offshore. Whilst victims attempted an array of methods to obscure payments, the operation found that each payment was being primarily redeemed by an adult in Australia, who converted the domestic transfer from the victim into a direct bank transfer offshore to the perpetrator.

The operation identified thousands of these domestic "bank mules", who often were proven to be vulnerable persons and victims themselves, in some cases of long-standing romance scams. Most of these mules were also identified as enablers of a breadth of high-monetary value fraud crimes. Action against their involvement in the FSEC, which results in relatively small value sums for the perpetrator, compromised their utility for enabling perpetrators' higher value crime, diminishing their domestic mule network and access to efficient, low-cost means to receive extorted or fraudulent funds. This has helped create a hostile online environment for perpetrators targeting children in Australia and forcing them to rely on more expensive "finance-as-a-service" vendors or, more inconveniently, gift cards which limit the return of this relatively low value crime type.

Of note, in addition to the specific tactics deployed in Operation Huntsman, there has also been considerable efforts to convey to the Australian community how to avoid becoming a victim of FSEC. This includes innovative prevention and education initiatives, targeted directly at the key FSEC demographic, both at the grass roots community level as well as via engagement with social media companies and trusted social media influencers. Furthermore, as part of an international effort, the ACCCE has engaged directly with local law enforcement partners in countries where perpetrators are based to share information obtained about FSEC perpetrators and contribute to effective local enforcement action. This multifaceted law enforcement and prevention and education approach to tackling FSEC is critical, with its success demonstrated by the fact that the ACCCE is now seeing a decrease in reports and instances of FSEC in Australia.

OCSE is also dependent on other online infrastructure to prevail. In the case of FSEC, popular social media and messaging applications are primary vectors for perpetrator's initial contact with victims and their subsequent exploitation. Such platforms and other forms of online infrastructure are also utilised for LSAC to enable communication, identification of consumers/facilitators, and the streaming itself. Relevant infrastructure for OCSE includes social media platforms, internet services providers, mobile network operators, cloud services, content distribution networks, browsers, and app stores, among others.

Infrastructure providers are implementing measures to detect and then disrupt these crime types. Meta, for example, reported[3] in July 2024, they had removed around 63,000 Instagram accounts in Nigeria attempting to target

3. Combating Financial Sextortion Scams From Nigeria | Meta

individuals for FSEC but also thousands of other pages or accounts that were providing guidance on how to conduct online scams.

However, the rapid evolution of technology and the tactics used by OCSE offenders necessitates ongoing innovation and for companies to mitigate their specific vulnerabilities. In addition to proactive measures by providers, there is increasing requirements from national governments for "safety by design".

The UK Government's Voluntary Guidance for internet infrastructure providers on tackling online child sexual exploitation and abuse[4], provides cross-cutting actions for infrastructure providers, such as embedding safety by design, receiving and acting on reports of abuse material, and being transparent about efforts taken to disrupt. However, it also critically provides service-specific actions that are tailored to different types of infrastructure provision.

INTERPOL's Operation Narsil sought to target the infrastructure enabling OCSE, aiming to identify and bring to justice individuals responsible for creating websites providing and profiting from CSAM, some of which could have been created through capping of livestreamed material. One outcome of the Operation's monitoring and seizing of offending domains was a plethora of debit and credit card information using pseudonyms and/or stolen identities, as well as evidence of the use of payments processors, peer-to-peer platforms, and cryptocurrency exchanges. In turn, this resulted in the location of confirmed identifiers and account information linked to financial institutions, and the related offenders.

Like financial disruption, disruption of the infrastructure that facilitates OCSE can be effective in preventing instances of abuse. A concerted effort across the available infrastructure is, though, key in preventing the criminal actors from simply relocating to infrastructure where barriers are weaker.

4. Voluntary guidance for internet infrastructure providers – GOV.UK

Section 4:

Recovering Assets Linked to Online Child Sexual Exploitation

Recovering Assets Linked to Online Child Sexual Exploitation

One of the most effective means of combatting financially motivated crime is to go after the assets of those that have committed the crimes. Asset recovery laws are frequently employed in cases of drug trafficking, ML, fraud and corruption matters. While the pursuit of asset recovery may be more typical in these areas, opportunities to use asset recovery laws to target the proceeds, instruments and benefits relating to OCSE, including FSEC and LSAC, can also be considered as part of the investigative and litigation strategy to deliver maximum accountability against those committing these offences.

BOX 9 – Pursuit of Home Linked to Online Child Sexual Exploitation

Example 1

In recent years, the Australian Federal Police (AFP) led Criminal Assets Confiscation Taskforce (CACT), working alongside the AFP-led Australian Centre to Counter Child Exploitation (ACCCE), AUSTRAC's Child Sexual Exploitation Response Team (CSERT) and Australian law enforcement's Joint Anti Child Exploitation Teams (JACETs), has taken targeted measures to pursue the assets of offenders involved in OCSE. Utilising the Commonwealth of Australia's *Proceeds of Crime Act 2002*, the CACT has adopted a targeted strategy to punish and deter offenders who create and/or consume child exploitation material, whether motivated by profit or otherwise, by confiscating the proceeds, instruments and benefits of their offending. This has included, for example, considering the physical features of the location where the relevant conduct occurred and whether any arguments regarding instrumentality can be made.

A significant and complex child exploitation matter in 2022 resulted in an Australian man being sentenced to 15 years' imprisonment for a range of child abuse offences. This included LSAC and resulted in the safeguarding of 15 young victims in the Philippines. The man, who paid for children in the Philippines to be sexually abused while he watched and instructed on webcam from his home in Australia, pleaded guilty in 2021 to 50 offences, which included charges relating to viewing, remotely instructing and recording the sexual abuse of children.

In late 2020, the CACT obtained restraining orders over the man's home, from where some of his internet-based offending was believed to have taken place. The CACT's asset recovery proceedings against the man's home were finalised in 2022 with the man making a financial payment, equivalent to half the value of the home, to the Commonwealth's Confiscated Assets Account. This case was the first time that the CACT sought to confiscate the home of a person charged with child sex offences.

Example 2

In 2023, a 34-year-old man was convicted in Australia of accessing and possessing child sexual exploitation material and sentenced to 3 years' imprisonment. More than 6000 child sexual exploitation images and videos were located on the man's electronic and storage devices, found at his home. A restraining order was sought and obtained by the CACT over the home in March 2024, and it was successfully forfeited to the Commonwealth in June 2024. The home, which has a value of approximately $375,000, will now be sold, and the net proceeds of sale will be paid into the Commonwealth's Confiscated Assets Account. This account is used by the Australian Government to fund various crime prevention, law enforcement and community safety related initiatives, including the ThinkUKnow Australia online child safety education program aimed at preventing OCSE.

This was the second time the CACT successfully used proceeds of crime laws to target a home in Australia linked to online child sexual abuse offences, and the first time a forfeiture outcome has been obtained in such circumstances.

Source: Australia

The FATF project team for this report found very limited examples of the application of asset recovery laws to OCSE cases. This could be due to potential difficulties in some jurisdictions with applying asset recovery laws to OCSE offending, but this could also be because jurisdictions have not yet considered the ways in which their asset recovery laws could be so applied.

Two successful asset recovery strategies that countries can consider include those of Australia and the United States. Australia has taken targeted measures to pursue the assets of offenders involved in OCSE as part of their enforcement approach, and to deter potential offenders from committing OCSE in the first place. The United States have also demonstrated the use of restitution to assist victims in recovering from being party to exploitative acts.

BOX 10 – **Ordering Restitution**

In April 2024, Samuel Ogoshi and Samson Ogoshi, both of whom were extradited from Nigeria to the United States in August 2023, pled guilty to conspiring to sexually exploit teenage boys.

The plea agreements describe the integrated roles played by Samuel and Samson Ogoshi in creating fake profiles, luring, and extorting victims. They devised a fraudulent scheme where they pretended to be a young woman in social media profiles and encouraged teenage boys and young men to engage in sexually explicit conduct and produce images of that conduct. Once the victims produced and sent those images, the Ogoshis used those images to blackmail their victims for money, threatening to send the images to others, including families, friends, and classmates of the victims. The Ogoshis instructed their victims to send money to designated financial accounts through various cash applications.

The Ogoshis targeted over 100 teenage boys and young men, at least one of whom committed suicide as a result of the devastating impact that sexual extortion can have on victims.

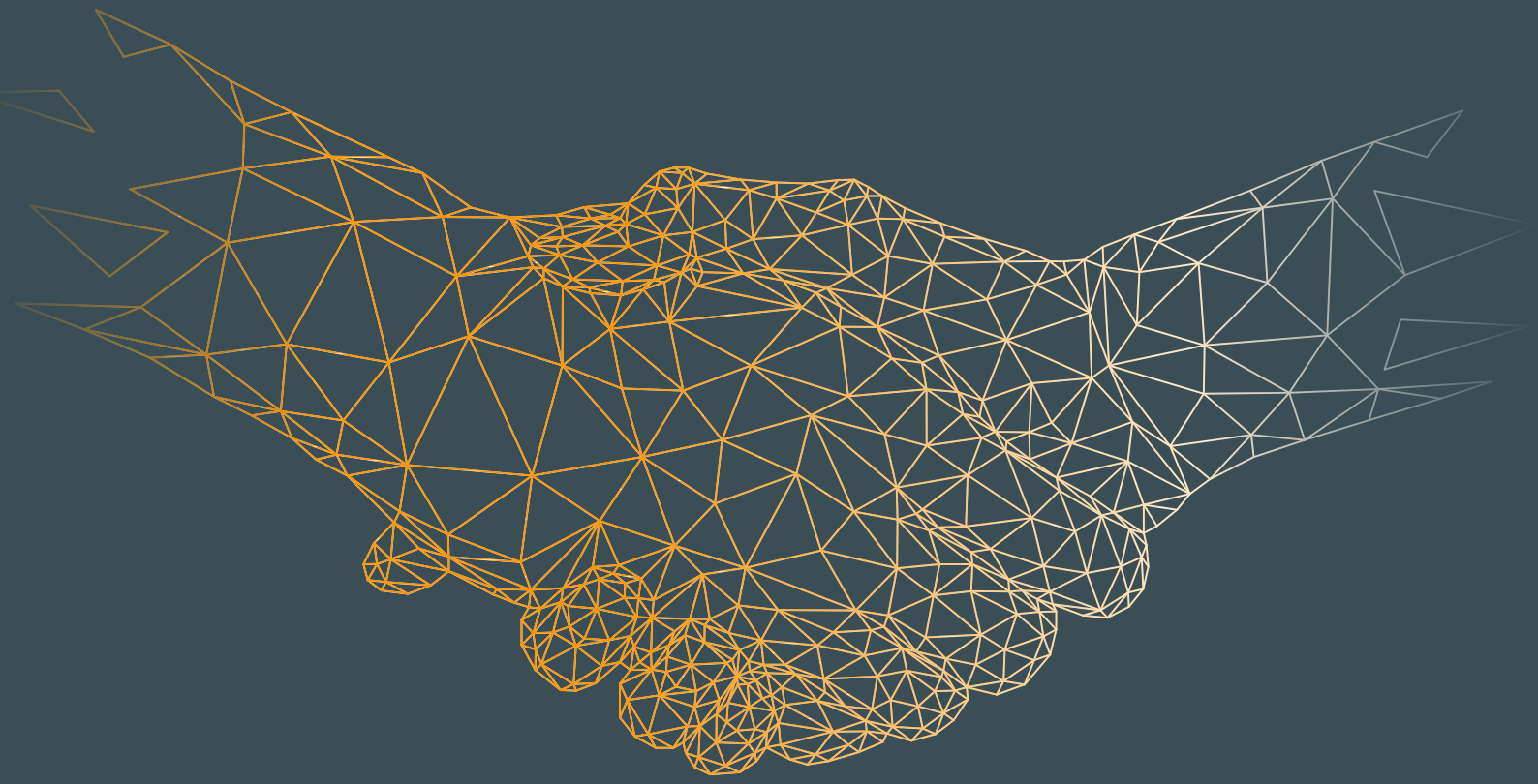
As part of their plea agreement, the Ogoshis were ordered to pay restitution to their victims, including the family of the victim who took their own life. In September 2024, the defendants were sentenced to 210 months in prison followed by 5 years of supervised release for their crimes.

Source: United States of America

While few countries were able to demonstrate attempts and/or success in applying asset recovery measures to OCSE cases, the few instances that exist show that it is possible to do so successfully. The FATF encourages countries to consider the targeted use of these tools as part of their law enforcement approach to OCSE.

Section 5:

Challenges, Recommendations, Opportunities and Conclusion



Challenges in Detecting, Disrupting, and Investigating Online Child Sexual Exploitation

Current challenges

Lack of comprehensive global understanding of the scope and scale of OCSE and its proceeds, and consideration in national risk understanding – It remains that there are no clear, consistent definitions of the types of crimes that OCSE encompasses. Nor, therefore, are there reliable global estimates for the proceeds of OCSE, or for LSAC or FSEC as sub-categories of OCSE. This may minimise the perceived impact of these crimes and understanding of the illicit financial flows related to these crimes. This likely contributes to limiting the focus of some competent authorities responsible for tackling illicit financial flows, such as AML policy makers and competent authorities, on these crimes and their proceeds, leading to insufficient global attention on OCSE.

This also means, especially when coupled with those barriers which conceal the detection and identification of the scale of OCSE, jurisdictions are not considering (or not sufficiently considering) these crime types when identifying and assessing their domestic ML risks. On aggregate, ML risk assessments do not identify this activity in line with the, particularly human, cost associated with it. As a result, there is generally a lesser domestic understanding of these crimes, and how to successfully detect, investigate and prevent them.

Technology – Technology continues to evolve and expand at an exponential rate, influencing nearly every aspect of our existence, including how we live, work, communicate, interact and socially connect with the world around us. While the internet, computers, smartphones, artificial intelligence, blockchain and other technologies can and do provide many benefits, these same technologies are utilised by OCSE offenders and contribute to its alarming escalation and trajectory. For example, the increasing prevalence of VAs, including anonymity enhanced VAs, as well as increasing end-to-end encryption of communications is creating additional barriers in detecting OCSE.

Incomplete domestic information sharing – To reach a robust understanding of these crimes, and successfully detect, investigate, and prevent them, it is critical for competent authorities and the private sector to work hand in hand, but also for competent authorities themselves to be cooperating effectively. The nature of these crimes are such that financial institutions and social media companies are on the frontline in holding critical information and evidence, and in the case of FSEC are best placed to identify it occurring in real time. Strong and trusted cooperation to share information domestically, from complaint reporting to financial reporting to social media information, is key to building a full picture of instances of OCSE and how to combat it.

Currently information sharing is incomplete, and not consistently optimised to detect, investigate, and prevent OCSE. This can be due to a lack of familiarity between the relevant parts of a country's competent authorities, for example, there may be limited interaction historically between the stakeholders within a country's AML regime and their law enforcement working on OCSE. The private sector may not have trusted relationships with law enforcement, or law enforcement may not sufficiently understand the wealth of information the private sector hold.

This diversity of required partnerships, some competent authorities' inability to share with all partners and the associated diversity of information offered by stakeholders combatting OCSE and its related financial flows, can lead to incomplete and/or misunderstood domestic information sharing which could be better co-ordinated and more complete.

Barriers in international information sharing – Many of the barriers in domestic information sharing equally apply internationally, for example, the lack of familiarity among some countries, as well as the challenges we see apply in international cooperation and information exchange on ML/TF more widely. In addition, the inconsistency in legal frameworks on OCSE, and extent to which LSAC and FSEC are explicitly criminalised in jurisdictions, can

hinder cross-border collaboration. The often innately international dynamics of these crimes mean that international information sharing is fundamental in detecting, identifying, and investigating OCSE, but also in enabling victims to be safeguarded, and preventing further abuse.

Cross-platform detection – Offenders have been observed to operate seamlessly across a variety of social media platforms and financial institutions. This diversity of activity can lead to challenges in identifying activity typological of the financial flows of OCSE. Without the ability to share information between and amongst social media platforms and financial institutions, it is difficult to get an accurate view of the activities of an individual facilitator due to this decentralised method of operating.

Emerging challenges

Nudify-ing imagery – Increasingly sophisticated software to "nudify" images (i.e., transform a non-explicit image into an explicit image) is becoming freely available on the internet. Such technology can generate explicit images of children, sometimes images that would be considered very embarrassing. These images could be used to extort vulnerable persons without ever having deceived them into providing actual explicit images. If such software becomes high quality, convincing and freely available, it could dramatically exacerbate the instances of OCSE worldwide, increasing the proceeds generated and harm done.

Generative Artificial Intelligence – Generative AI has the potential to be used to automate the commission of FSEC, through its use to develop extortion scripts, find prospective victims and have introductory conversations with them, potentially in many different languages. As the universe of potential victims of FSEC is virtually unlimited, any automation of this already low-investment criminal activity would increase the threat level, and potentially see a continued exponential rise in the occurrence and value of the proceeds of this crime type[1].

Potential for increasing involvement of organised crime groups and the commercialisation of OCSE – Currently the typically low level of proceeds related to LSAC and FSEC mean involvement of significant organised crime groups is limited. However, there is some evidence of criminal business structures in developing countries increasingly exploiting the commercial opportunities presented by paid LSAC. For FSEC, groups or teams have already been observed working together and using common methodologies, as well as, operating as part of broader fraud and scam operations. Increased commercialisation of LSAC and FSEC and moving away from proceeds being generated primarily to meet basic needs, would likely drive increased ML activity related to OCSE proceeds.

Recommendations for Jurisdictions to Improve their Ability to Detect, Disrupt, Investigate and Prosecute Online Child Sexual Exploitation

Beyond the use and adoption of good practices described in this report, stakeholders such as FATF Global Network members, competent authorities, practitioners, policymakers, financial institutions, designated non-financial businesses and professions, VASPs, non-profit organisations and any other individuals or bodies with an interest in better understanding the financial flows related to OCSE and detecting, disrupting, investigating, prosecuting and recovering assets linked to OCSE are encouraged to consider the following recommendations:

Consider as a victim-based crime - The high level of long-lasting harm caused to victims means that first and foremost all stakeholders should maintain a victim-centric approach to responding to these crimes. While cyber-enabled, categorising

1. At the end of 2024, NCMEC has already received more than 7000 generative AI-generated child exploitation reports. https://www.missingkids.org/blog/2024/the-growing-concerns-of-generative-ai-and-child-sexual-exploitation

and responding to OCSE as purely cybercrime, rather than a cyber-enabled victim-based crime, comes with the danger of losing sight of the violent sexual crimes or devastating sexual exploitation that sit behind OCSE activity. Similarly, while financial intelligence offers significant opportunities for FIUs, law enforcement, payment platforms, financial institutions, VASPs and others to detect and investigate OCSE, maintaining focus on the victim and harm behind the transactions should remain central to investigative strategies.

Adopt and disseminate Financial Indicators of OCSE to relevant stakeholders – Jurisdictions should consider adopting the indicators of financial transactions linked to LSAC and to FSEC provided in this report into their national response to OCSE. They should also disseminate the updated indicators to relevant authorities and regulated entities and take steps to encourage their integration into transaction monitoring processes.

Deepen awareness of OCSE crimes and their investigation – At the outset of this project, many participants were not familiar with these crime types, and this lack of awareness and familiarity made it difficult to source information from the FATF and the broader FATF Global Network. To familiarise implicated competent authorities, jurisdictions should consider awareness raising for all competent authorities and training of relevant staff on the financial indicators and investigation of OCSE transactions. Countries should also consider the benefit of training investigators focused on OCSE offences on relevant aspects of ML and financial investigations.

More broadly, jurisdictions should take a preventative approach in considering public messaging and awareness raising campaigns to sensitise children and their families to the risks of OCSE and to what support is available.

Identify and assess risk of financial flows and ML associated with OCSE – Given the lower level of proceeds generated by LSAC and FSEC relative to others, jurisdictions may not be inclined to include them for consideration during their risk assessment processes. However, the level of harm associated and the financial motivation behind these crimes should encourage jurisdictions to consider these proceed generating crimes under their national risk assessments. More broadly, jurisdictions could consider the level of human consequence and harm of these proceed generating offences when considering ML risks to aid in ensuring sufficient response to crimes of high human impact but lower proceed generation.

Public private cooperation – As per some of the cutting-edge examples provided in this report, jurisdictions should proactively develop relationships with the private sector and civil society partners working to disrupt these crimes. Competent authorities, the private sector and civil society all have unique capabilities and pieces of information and channels to take action. To best combat these crime types, information needs to flow freely (within the bounds of the law), so that all participants can take advantage of that information. All participants should have a common understanding of the threats facing the jurisdiction and know the most efficient ways available to them to report suspicion or instances of these threats (i.e., such as the submission of key words on STRs/SARs, reporting hotlines or otherwise).

Competent authorities should also ensure strong mechanisms to provide feedback on information shared by the private sector, both to ensure quality reporting and information sharing but also to strengthen the private sector's risk understanding and ability to identify suspicious activity and transactions. For example, where a reported suspicious transaction is confirmed as linked to LSAC or FSEC, communication of this to the reporting entity is highly valuable in feeding into and updating their risk indicators or can lead them to look further into linked accounts and transactions which may expose further suspicious activity.

Mechanisms for public-private cooperation should also consider providing the means for private-to-private information sharing to mirror the operation of OCSE across different online platforms and financial institutions and improve the ability for cross-platform detection of OCSE activity.

Enhancing domestic cooperation and information sharing – Jurisdictions should also develop mechanisms for facilitating cooperation and information sharing across their relevant authorities to allow a holistic approach to addressing OCSE that optimises the value of financial intelligence and investigation. Sufficient familiarity between relevant authorities should be ensured, and jurisdictions should also consider the value of a specified, and specialist, resource on LSAC or FSEC, or OCSE more widely, that works to ensure a standardised and comprehensive response by authorities and law enforcement.

Proactively develop international partnerships – As per this report, in many instances, these crimes have international elements, frequently with repeated partner countries. Whether working for a competent authority in a transaction source country or a transaction destination country, individuals and authorities can proactively create relationships with counterparts and/or leverage existing, or develop new, multi-national forums and task forces. Such direct, and trusted, relationships internationally have proven critical in detecting, disrupting, investigating and prosecuting OCSE.

Temporary suspension powers – The FATF Standards require that countries have the power to suspend financial transactions. These powers should be used in cases of financial transactions related to the laundering of the proceeds of OCSE.

Pursuit of asset recovery measures – The project team uncovered very few instances where asset recovery laws were applied to cases of OCSE. However, some countries have demonstrated that they have been able to use these laws successfully to recover the assets of OCSE offenders and provide restitution to their victims. The FATF encourages countries to more frequently use asset recovery laws as a means to combat OCSE. Countries could consider using their regional asset recovery interagency networks or INTERPOL's Silver Notice to trace and recover criminal assets linked to OCSE.

Adopt a multifaceted approach – From this report and the submissions received from the members of the FATF Global Network, it is clear that in order to successfully detect, disrupt, investigate and prosecute OCSE, and indeed reduce its prevalence as seen recently in the case of FSEC in Australia (refer to para 112), it is essential that a multifaceted, global response, is adopted by stakeholders. This response should encompass those actions as reflected in the recommendations in this report, including local and international law enforcement action, contemporary and specific OCSE laws across jurisdictions, public-public and public-private cooperation, adoption of OCSE offending in national risk assessments, and targeted prevention and education initiatives through schools, community organisations and engagement with social media companies and trusted social media platforms. Only through a comprehensive and multifaceted approach can the international community effectively combat this serious threat to the well-being of children worldwide.

Opportunities

Disruption of contact offending: There is a known typology of consumers of LSAC progressing from online consumption of livestreamed child sexual abuse to travelling to destinations to conduct contact abuse themselves (child sex tourism). Detecting consumption of LSAC and identifying and taking appropriate action against consumers is an opportunity to disrupt or prevent this escalation of behaviour, which prevents further instances of sexual abuse of victims. As noted in this report, when overlayed with other data sources, such as NCMEC's CyberTipline reports, financial intelligence linked to LSAC can assist to build more accurate profiles of possible offenders, which can in turn be shared with domestic border security agencies – to potentially prevent possible offenders from leaving the country or to identify travellers for closer scrutiny upon their return – or shared with international law enforcement partners for consideration and potential action in local jurisdictions.

Disruption of other crime: As seen in Operation Huntsman, the bank mules involved in laundering FSEC ransom payments were also identified as enablers of a breadth of high proceed generating fraud crimes. The Operation's action against these mules for their involvement in FSEC compromised their utility for enabling perpetrators' higher value crime, diminishing their domestic mule network and access to efficient, low-cost means to receive extorted or fraudulent funds. This, coupled with the known typology of FSEC perpetrators also conducting other frauds and scams, offers the opportunity through the identification of perpetrators, or associated actors, of FSEC to disrupt the commission of other crimes.

Conclusion

OCSE is a heinous crime that preys on some of society's most vulnerable people, our children. There are no clear, consistent definitions describing the types of crimes that OCSE encompasses. Accordingly, there are no accepted estimates of proceeds that these crimes generate. What is clear is that this crime type is massive in scope and the trajectory of instances of this crime are increasing at an alarming rate.

There are many unknowns in the research regarding this crime type, but what is not in question is the significant cost to victims and their families. OCSE has devastating consequences on victims, consequences that are severe and impact victims throughout their lives. Some situations involving OCSE have even resulted in suicide. ML risk is not simply an expression of the money that is generated by a crime. ML risk includes the consideration of the consequences of the crime, including consequences for the victim and societies that incur further social costs. In the case of OCSE, these consequences are massive and dwarf any consideration of the value of the proceeds that the crime type generates.

This impact means it is imperative that all jurisdictions work together globally to detect, disrupt and investigate the commission of OCSE. Financial intelligence and the deployment of victim-centric investigative strategies have a critical role to play in this, offering opportunities for detection and disruption of OCSE not possible through other means and in a manner than can reduce reliance on victim testimony. Utilisation of financial intelligence has directly led, as demonstrated by delegation contributions, to the identification and safeguarding of LSAC victims and to real time interventions of support for victims of FSEC, underlining the powerful impact the effective use of financial intelligence can have.

Annex A:

Identifying Financial Transactions Linked to Online Child Sexual Exploitation

It should be appreciated that the below indicators linked to the detection of online child sexual exploitation (OCSE) are constantly evolving, and jurisdictions should continue to inform and strengthen these indicators through continued collaboration between their FIUs, reporting entities, law enforcement, and other stakeholders.

Identifying Financial Transactions Linked to Live-streamed Sexual Abuse of Children

Consumers who pay to view live-streamed sexual abuse of children (LSAC) typically use popular money value transfer services (MVTS), predominantly online peer-to-peer (P2P) payment systems such as PayPal. While less common, some consumers make direct bank deposits or transfer virtual assets (VAs) through virtual asset service providers (VASPs), and there is evidence of the increasing use of other applications to make payments, such as the all-purpose Grab app available in some regions, or through OnlyFans. The obliged entities providing or facilitating these financial services can detect transactions that may be linked to cases of LSAC by using a combination of the indicators outlined below:

General Indicators of Transactions Related to Live-streamed Sexual Abuse of Children

- Transactions from developed countries to high-risk jurisdictions for child sexual exploitation.
- Significant age differences between remitters and receivers.
- Transactions of low (i.e., 10-200 EUR per instance), even-denominated amounts either in source or destination country currency, or in the virtual asset equivalent of even-denominated fiat amounts (i.e., a virtual asset amount that is equivalent to an even amount of fiat currency).
- Payments being made to receivers in another jurisdiction, with whom the remitter has no apparent legitimate connection.
- Transactions made at irregular intervals but made repeatedly to accounts on the same day or on successive days.
- Transactions made late at night or early in the morning (signalling that the consumer may be in a different time zone).
- Transaction purpose refers to social media or social media usernames, sexual or pornographic terms, or date/time that material was streamed.
- Extended financial history characterised by payments over a long period, signalling a long-term relationship has formed between the consumer and facilitator.
- Transaction may be described as being for medical or subsistence costs or refer to relationships between the remitter and receiver. For example, descriptors such as "family support", "school fees", "assistance", "support", "medical bills", "accommodation", "education", "financial assistance", "gift", "purchase of clothes", "purchase of toys", "uniform", "friend", "boyfriend", "girlfriend", or "sponsor".
- Purchases at vendors that offer online encryption tools, VPN services, software to clear online tracking, or other tools or services for online privacy and anonymity.
- Accounts or customers that have a high volume of transactions to Facebook, Microsoft, Google Play, OnlyFans, TikTok, Instagram or other social media sites (such as Micous).
- Transaction linked to an individual on a public registry of sex offenders.

Transactions Conducted by Consumers

- Transactions conducted to accounts in, or accessed in, high-risk jurisdictions for LSAC (e.g., accounts accessed via ATM cash withdrawals, or account logins through IP address in a jurisdiction of concern).
- Purchases on dating platforms or platforms that offer adult entertainment content.
- Purchases on webcam/livestreaming platforms, including those providing adult entertainment.
- Purchases on online gaming platforms or gaming stores.
- Purchases of video capture software.
- Funds sent to or received from an individual 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.
- Transactions linked to an individual who is the subject of adverse media involving child sexual exploitation-related offences.

Transactions Conducted by Facilitators/Abusers

- Money remittances are usually withdrawn immediately.
- Receivers are under investigation by law enforcement for the suspicion of being part of facilitating online child sexual exploitation.
- Payments for premium features or services on social media platforms.
- Purchases of video capture software for use on websites or social media.
- Transactions on online gaming platforms or gaming stores.
- Acquisition of spyware or surveillance applications.
- Multiple deposits of similar amounts traced to foreign sources, particularly from high-risk LSAC consumer countries, including deposits from these foreign sources at the same or similar time.
- Payments to online file hosting vendors/platforms.
- 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).

While one of the above indicators in isolation may not necessarily signify payments relating to potential cases of LSAC, using a combination of indicators and other relevant factors regarding transactions and clients can help obliged entities to observe patterns that may signal suspicious activity.

Identifying the Financial Sexual Extortion of Children through Financial Transactions

The majority of victims report having paid ransoms to facilitators via MVTS (predominantly online P2P payment systems such as PayPal), bank transfers, VAs through VASPs or gift cards. The obliged entities providing these services have the capability to spot transactions that may be indicative of financial sexual extortion of children (FSEC) by using a combination of the indicators listed below:

General Indicators of Transactions Related to Financial Sexual Extortion of Children

- Transactions conducted between two individuals where there is no apparent relationship (i.e., no common surname, no clear business purpose).
- Transactions generally of less than 500 EUR, but sometimes ranging up to 1500 EUR in even-dominated amounts.
- Initial transaction between remitter (victim) and receiver (perpetrator) generally less than 250 EUR.
- Multiple transactions from a remitter to a receiver over a short period of time and then stopping entirely.
- Transactions conducted to a common country of operation of perpetrators of FSEC (i.e., Cote d'Ivoire, Nigeria, Philippines etc.). Obliged entities should take note of the shifting trend of countries where this is predominantly taking place over time.
- Transaction purpose refers to social media or social media usernames, sexual or pornographic terms, threatening/pleading language or date/time that material was received.
- The transaction recipient is not local to the remitter.
- Payment details appear like a charitable donation.
- Transaction linked to an individual on a public registry of sex offenders.

Transactions Conducted by Victims

- Transactions that are conducted by a teenage or young adult male and to a lesser degree teenage or young adult female.
- Transactions originating in primarily English-speaking countries, if international. Obliged entities should note that this will become less of a marker over time as facilitators become more sophisticated.
- Receipt of complaints from individuals about transaction links to sexual extortion.
- Payments typically occurring between 7pm and 7am (usually as the sexual extortion is happening in real time).
- The remitter (victim) does not enter a payee name (i.e., only enters a general label for recipient) or enters a payee name that does not match the actual account holder.
- Diminishment of funds in the remitter's accounts within a matter of hours (usually less than 24 hours).
- Uncharacteristic purchase of digital gift cards or gaming credits.

- Uncharacteristic uses of individuals' P2P platform accounts.
- Uncharacteristic purchase of VAs.
- When questioned by bank staff, the remitter is evasive or offers an implausible explanation for the activity.
- Victim purchasing multiple gift cards (for example, Amazon, PlayStation or other gaming providers).

Transactions Conducted by Perpetrators

- An account receiving multiple apparently unlinked transactions.
- Receiving account having multiple unlinked rationales identified for the transactions being received by the account.
- Amounts received quickly removed from account.
- Payments to online services offering privacy and/or anonymity (i.e., encryption, VPN, virtual phone numbers, etc.).
- Payments associated with multiple pre-paid credit cards or gift cards.
- Receipt of funds from multiple online file hosting marketing services (e.g., pay-per-download models) across different jurisdictions.
- Purchase of goods (vehicles, real estate, household appliances) in a short period of time, subsequent to receiving money, without justification for the means used.
- Persons with a lifestyle and consumption that is not consistent with the income earned from their work activity.

It is important to note that any one of the indicators listed above is insufficient to raise suspicion of a potential financially motivated sexual extortion attempt, but that obliged entities should consider all factors surrounding a transaction and whether the transaction meets a number of the indicators described above.

Disclaimer

This document and/or any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Financial Action Task Force
www.fatf-gafi.org