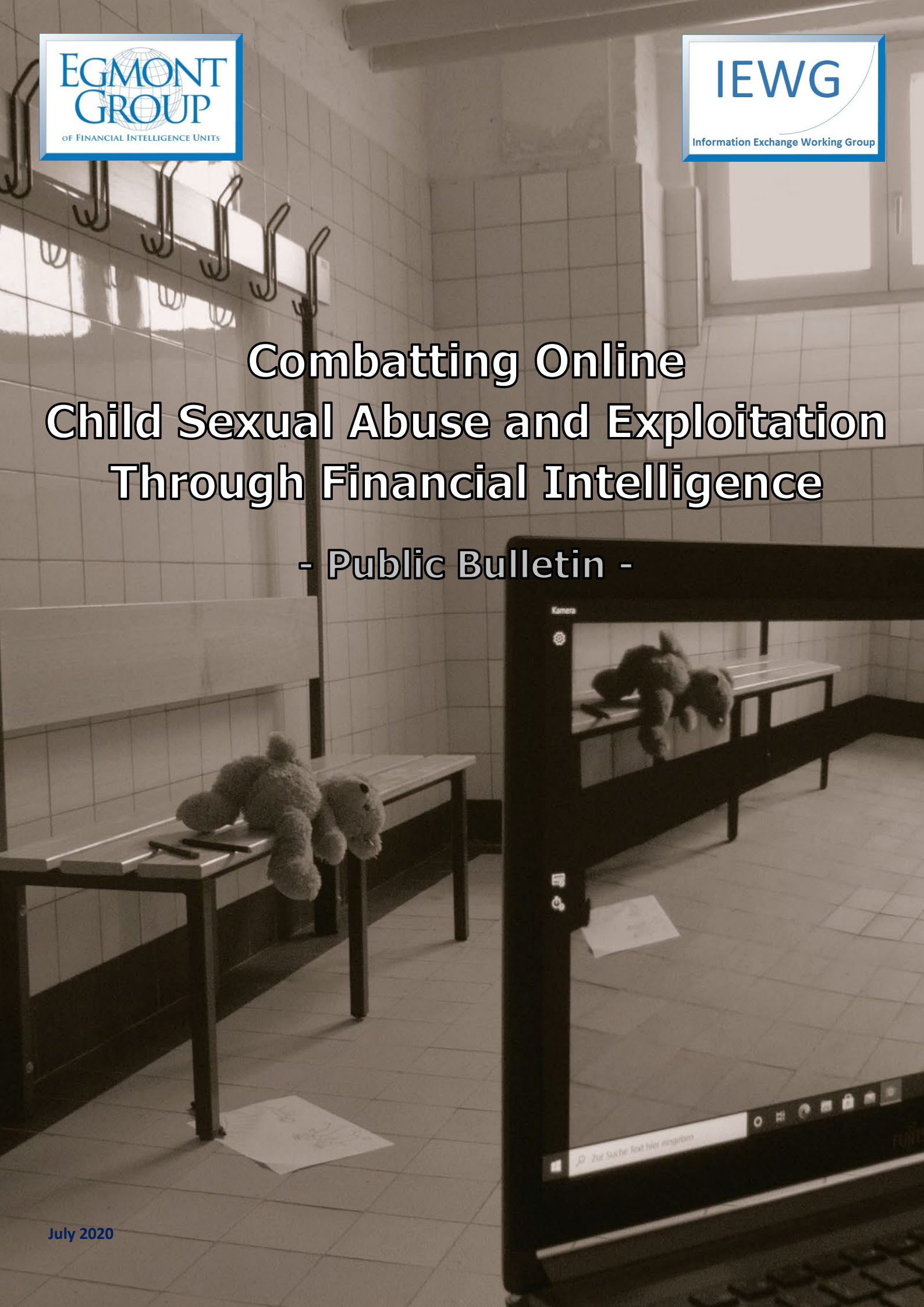

Combatting Online Child Sexual Abuse and Exploitation Through Financial Intelligence

- Public Bulletin -

July 2020

Project Leads: Australia, Philippines, UK.

Project members / participants / contributors: Australia, Canada, Denmark, France, Germany, Guatemala, Indonesia, Isle of Man, Latvia, Luxembourg, Malaysia, Mexico, Netherlands, Nigeria, Norway, Peru, Philippines, Seychelles, Interpol.

The project also undertook engagement with the following private sector entities: American Express; MoneyGram; PayPal; TransferWise; Western Union; and WorldRemit.

CONTENTS

EXECUTIVE SUMMARY

This is the public version of the Egmont Group project report on combatting online streaming of child sexual abuse and exploitation. It contains the project's overarching conclusions and key findings. Sensitive information that may reveal FIU or law enforcement methodologies has been removed, as has information relating to vulnerabilities that may be abused by offenders.

Online streaming of child sexual abuse and exploitation (CSAE) is a horrific crime that causes significant harm to specific groups of children and to the wider society in which it pervades.[1] Aided by technological advancement and supported by the reach of interconnected global networks, it is a crime that targets the most vulnerable members of societies – children. Online streaming of CSAE is a significant threat which is likely to continue to increase as facilitators, largely in impoverished communities, gain access to technological advancements, providing them with the means to abuse and exploit children for financial gain, and offenders with the opportunity to commit such crimes from a distance.

Noting that online streaming of CSAE is a crime often underpinned by financial transactions, this positions Financial Intelligence Units (FIUs) as key partners for law enforcement agencies (LEAs). Utilising the data held by the global network of FIUs provides opportunities to enhance strategic and tactical intelligence efforts to combat CSAE. The analysis of reports submitted by private sector entities, including Suspicious Activity Reports (SARs) and Suspicious Transaction Reports (STRs), enables FIUs to provide LEAs with actionable intelligence relating to the movement of funds and the identification of both offenders and facilitators.

The Egmont Group commenced this project to develop and consolidate the strategic intelligence picture associated with payments identified as relating to online streaming of CSAE. The project sought to utilise the data held by Egmont Group member FIUs and other sources, including private sector entities, to inform an understanding of financial transactions suspected to be linked to online CSAE.

The project team worked to improve multilateral information sharing efforts in order to identify transactional data held by FIUs. Taking the information shared by project participants the project team produced a consolidated list of financial indicators and keywords linked to online streaming of CSAE. These financial indicators and keywords can be used by FIUs to proactively identify financial transactions likely to be linked to online streaming of CSAE within their datasets. The identification of these transactions provides FIUs with the means to flag activity to national and international LEAs.

The project also initiated, or otherwise considered, forms of information exchange with the private sector, to develop tactical intelligence and inform an understanding of the respective merits of different forms of information exchange. The types of information exchange

[1] Online streaming involves the delivery of images (video) and sound over the internet in real time as the events being recorded and transmitted are taking place.

considered in this project have generated value for either FIUs or reporting entities in terms of identifying high-risk activity likely to be related to online streaming of CSEA.

The project team also produced key findings to enable FIUs to better contribute to efforts to tackle online streaming of CSAE, ranging from options for more effective handling of intelligence and the types of information exchange with the private sector that may assist in achieving this goal. The project team anticipates this increased understanding of financial risk factors and best practices will allow FIUs to adapt their business practices to actively contribute to efforts to combat online streaming of CSAE.

PART 1 – BACKGROUND AND SCOPE

Terminology in this report

This report uses the term child sexual abuse and exploitation (CSAE), which is more encompassing than other variants (e.g. child sexual abuse or child sexual exploitation). Other descriptors of this type of offence are used in this paper, but only when directly quoting from another report or to reflect the terminology used in the cited legislation.

Online streaming involves the delivery of images (video) and sound over the internet as the events being recorded and transmitted are taking place in real time. It is distinct from still or pre-recorded imagery otherwise known as indecent images of children.

Background

During the July 2019 Egmont Group Plenary meetings in The Hague, the Information Exchange Working Group (IEWG) endorsed a project to consider how financial intelligence could be harnessed to combat online streaming of CSAE. The concept note for the project established the project outputs, namely a paper covering:

- The global strategic intelligence picture on financial flows associated with online streaming of CSAE, including the identification of risks and mitigation measures.
- A summary of operational data exchanged between project participants and the use / impact for FIUs, law enforcement partners and private industry.
- Key issues for consideration in the global effort to combat online streaming of CSAE through the receipt, analysis and dissemination of financial intelligence by FIUs.
- Financial indicators, keywords and datasets to be used by FIUs and the private sector to identify financial activity linked to online streaming of CSAE and, more specifically, the facilitators and offenders.

The project also aimed to include structured engagement with the private sector, with a focus on money service businesses (MSBs) and payment service providers to enhance mutual understanding of their risk indicators and consequently enhance SAR/STR reporting.

Scope

The project focussed specifically on online streaming as opposed to other forms of distribution of CSAE material, such as the creation of indecent images of children and peer–to-peer exchange of this material. This is due to the development of criminal business models specifically established for online streaming, which bring a financial dimension to the activity that is not always prevalent in the other forms of CSAE.

PART 2 – STRATEGIC INTELLIGENCE PICTURE

Basic concepts of online streaming of CSAE

Online streaming of CSAE involves facilitators abusing their own children, extended family or other children at the request of an offender(s) situated in a different location. Utilising online streaming technology, offenders can view and instruct the direction of this abuse from a distance, without needing to leave their jurisdiction or home. Offending from a distance reduces the risk to the offender of LEA attention at the point of arrival or departure from the victim's country.

Online streaming of CSAE is a significant threat, which is likely to continue to increase. This is due, in part, to the increasing number of voice over internet protocol (VoIP) platforms, as well as the advancing consumer uptake of digital devices with ever-increasing functionality. In addition, the publicised efforts of LEAs may have discouraged some offenders from undertaking contact sexual abuse, including travelling to other countries to undertake such abuse. According to the findings of the *Virtual Global Taskforce (VGT) Child Sexual Exploitation Environmental Scan*[2], produced by Europol's European Cybercrime Centre, the online streaming of abuse is no longer an emerging trend but rather is an established reality.

The growth in online streaming of CSAE has also been facilitated by the expanding reach of 4G, and recently 5G, in many parts of the world. Access to such technology has made it almost effortless for offenders to network and enable the exploitation of children's use of social media platforms.

The financial dimension

In impoverished communities, online streaming offers a financial incentive for criminal networks, which creates a commercial element for CSAE. The illicit business models in relation to this activity, whereby offenders pay to view CSAE material via online streaming, means there is a money trail in the form of payments and profits.

It is not clear to what extent organised crime groups (OCGs) are involved in online streaming of CSAE. It is possible that organised activity differs from disorganised activity due to a higher volume of funds movement. However, it is judged that online streaming of CSAE is the most prevalent form of commercial sexual exploitation of children. While it is noted that a lack of large profits means wide-scale involvement of OCGs is likely to be limited, there is some evidence of criminal business structures in developing countries exploiting the commercial opportunities presented by online streaming of CSAE.[3]

Access to any related financial transaction activity is of value to support the efforts of FIUs and LEAs in combatting these crimes.

[2] https://www.europol.europa.eu/newsroom/news/2015-vgt-child-sexual-exploitation-environmental-scan

[3] Europol *Internet Organised Crime Threat Assessment (IOCTA) 2018*

Facilitators and associated business models

In a study on child pornography produced by the Anti-Money Laundering Council (AMLC - FIU The Philippines), which was a major source for the project, it was cited that an exploratory study considering the nature and extent of child sexual abuse streamed online in the Philippines in 2013 found three main categories according to the scale of operation:

- ***Individual operations*** are run from private homes, internet cafes or a 'Pisonet' (computers that will provide internet access for 5 minutes for every PhP1.00). Children involved in online sexual abuse are also commonly involved in street prostitution.
- ***Family-run operations*** are common in very crowded and poor neighborhoods where children are coerced by parents and other family members.
- ***Large-scale operations*** may involve whole neighborhoods where children are hired or trafficked. But many of the operations are family-run wherein the traffickers are mostly relatives and friends of the trafficked person.

The study also noted that a facilitator may purchase online tools or software to support online streaming and/or enhance images and video creation.

Self-generated material

Instances have been observed where children post CSAE material onto social media by providing false dates of birth to circumvent social media rules and policies and appear as adults despite being underage. Seemingly self-generated child abuse material is evident on social media and the victim receives money to their personal account before the streaming takes place. This methodology may be employed by the offender for the purpose of avoiding detection or it could be the children are seeking to generate funds for themselves. Often the children are referred to as 'cam-girls' but the images can also be produced by male children.

There has been a significant increase in the amount of self-generated material streamed online via popular social media applications with embedded streaming functionality. Victims are often groomed by offenders to engage in online streaming of sexual acts for peers on platforms, after which the material finds its way to other online sexual offenders.[4] In these cases the victims are more often from relatively affluent, Western backgrounds and appear to be in a home setting, usually their own bedroom. This type of offending makes the victim susceptible to sextortion for further imagery or illicit content. The Internet Watch Foundation found that images and videos were captured from the original upload location and further distributed in online forums, with the aim of receiving paid downloads.[5]

Jurisdictional risks

While online streaming of CSAE is a global issue, victims of the abuse are generally located in impoverished communities across a number of jurisdictions. According to the *2018 Internet Organised Crime Threat Assessment* (IOCTA) by Europol, the Philippines remains the most

[4] Europol *Internet Organised Crime Threat Assessment (IOCTA) 2018*

[5] Internet watch Foundation, *Trends in online child sexual exploitation: examining the distribution of captures of live-streamed child sexual abuse*, 2018.

common country where the abuse takes place. This is likely due to high-speed internet connectivity, growing availability of relatively cheap smartphones and tablets, widespread use of the English language, a high number of relatively poor families and perceptions that do not see online streaming of CSAE as being in conflict with social norms.

Moreover, in the report *Global Monitoring-Status of Action Against Commercial Sexual Exploitation of Children in the Philippines, (2nd ed.)* published by ECPAT International in 2016[6], according to the government officials tasked with combatting the problem, the Philippines child sex industry is one of the biggest in the world exceeding USD1 billion a year.[7]

However, the features described above are not limited to the Philippines, money movements suspected to relate to online streaming of CSAE are observed in a number of other jurisdictions.

Payment patterns for online-streamed material

The remittance of payments related to CSAE mainly occurs through MSBs and internet payment providers. However, some payments are observed via banks, noting that modern payment platforms are sometimes linked to traditional bank accounts. Observations also point towards the use of online money transfer platforms, as well as remittance services paid for in cash. There are limited examples of the use of virtual currencies.

The project also considered patterns and values of the payments, so FIUs can better identify transactions for the purposes of online streaming of CSAE, and provides this detail in the full report. Payments are always sent before the material is streamed, reflecting the financial incentive for facilitators.

Geographic aspects

The project identified a large number of jurisdictions identified as receiving or remitting funds for live streaming. Typically, the country where the activity is facilitated is in the developing world, with the activity being purchased or viewed from more developed countries. However, this is not universal, law enforcement has identified that perpetrators sometimes use online money transfer agencies to send the money via another jurisdiction.

[6] https://www.ecpat.org/wp-content/uploads/2016/04/a4a_v2_eap_philippines.pdf

[7] https://www.ecpat.org/wp-content/uploads/2016/04/a4a_v2_eap_philippines.pdf

PART 3 – ANALYSIS OF FINANCIAL DATA

The financial transactions associated with online streaming of CSAE present opportunities for law enforcement to take operational action against offenders, both those viewing and facilitating the abuse. Information contained in financial transactions also creates profiling opportunities for FIUs to enhance strategic and tactical intelligence. SARs and STRs are useful sources of intelligence relating to the methods used to remit funds in addition to containing key identification information of the suspects involved.

FIUs have reported that information contained in SARs/STRs enables detailed analysis leading to focussed law enforcement activity, including arrests and convictions, as well as other disruptive interventions aimed at preventing CSAE.

This section considers relevant financial data and intelligence gained either through the project, or otherwise by project team members.

Keywords and financial indicators

Project team members indicated that the analysis of SARs/STRs using a more complete collection of keywords has previously resulted in the identification of a greater number of suspicious transactions linked to suspected CSAE. The sharing of keywords and financial indicators with financial industry partners has improved the quality and quantity of reporting and enabled FIUs to identify and action the suspicious reporting in a timely manner.

For this reason, a consolidated list of financial indicators and keywords to screen SARs/STRs was produced by the project team and shared with project members. Participating FIUs were asked to review the consolidated list of financial indicators and keywords and provide feedback to the project team with any views or additional material to enrich what had already been collated during the project. Several FIUs reported that, as a result of applying the keywords, thousands of previously unidentified transactions were identified, although this was not a universal position and two participating FIUs reported that the keywords did not result in them identifying any new transactions. Feedback was provided by FIUs and the indicators and keywords were subsequently refined.

The list of keywords and financial indicators was then shared with private sector entities in phase 2 of the project. One private sector entity advised that it was developing its transaction monitoring rules based on a combination of the keywords and its own work. This produced a large number of matches with financial transactions and, after taking time to work through the transactions, some SARs/STRs resulted from this work and were then reported to FIUs in multiple jurisdictions. This engagement helped the project team further understand what kind of indicators and keywords are most useful for reporting entities.

Nominal data

The project confirmed that nominal data, specifically relating to the facilitators of online streaming of CSAE, has the potential to lead more directly to the identification of financial flows associated with online streaming of CSAE. It helps to distinguish transaction patterns related to CSAE from other crimes (such as romance scams) that share similar financial profiles and thus reduce false positives. Some FIUs and LEAs may consider sharing nominal data with the private sector, for example through public-private partnerships, if such approach would potentially lead to increased effectiveness in the reporting regime of their specific jurisdiction.

Non-financial data

The project has demonstrated that it is difficult to delineate financial transactions related to payment for online streaming of CSAE from payment for adult sexual content, scam activity or other CSAE related material such as images. Furthermore, all payments may not be attributable to CSAE, but rather the transactional activity and destination of the remittance could lead the SAR/STR reporter to assign the suspicion of CSAE. It should be noted that other crimes in action such as some fraud typologies or 'sextortion' may have similar financial profiles.

This underlines the need for further work with relevant parts of the financial sector to refine understanding, financial indicators and keywords as part of the response to online streaming of CSAE. Importantly, it also highlights the relevance of other cyber-related datasets in providing a holistic picture of the relevant financial activity.

Work under the project has considered the potential utility of such data if used by the private sector, for example, the Child Rescue Coalition (CRC), a US non-profit organisation, holds such data.

CONCLUSIONS

The various models of information exchange considered by this project have generated value in terms of identifying financial activity linked to offenders engaged in and/or facilitating online streaming of CSAE. This establishes the value of financial intelligence to identify unknown entities based on known criteria and risk factors linked to online streaming of CSAE.

The use of some forms of non-financial / cyber-related data, not normally held by FIUs, appears to result in high quality intelligence and indicates a potential value not achieved via other forms of data exchange. It also shows benefit in combining financial information with other forms of information in this way and undertaking data exchange between non-FIU entities.

It is important that work to explore avenues and opportunities for FIUs to engage in data exchanges with relevant national and international LEAs and private sector entities related to CSAE continues to be prioritised going forward.