FinCEN NOTICE

FIN-2021-NTC3 September 16, 2021

FinCEN Calls Attention to Online Child Sexual Exploitation Crimes

The Financial Crimes Enforcement Network (FinCEN) is issuing this Notice to call attention to an increase in online child sexual exploitation (OCSE). This Notice provides financial institutions with specific suspicious activity report (SAR) filing instructions, and highlights some financial trends related to OCSE.

Crimes related to OCSE, including the funding, production, and distribution of child sexual abuse materials (CSAM), have increased during the COVID-19 pandemic, according to multiple law enforcement authorities. This increase in activity is likely due to a confluence of factors, including: (1) increased internet usage by children who are spending more time online, both unsupervised and during traditional school hours; (2) restricted travel during the COVID-19 pandemic resulting in more sex offenders being online; and (3) increased access to and use of technology, including encrypted communications, bulk data transfer, cloud storage, live-streaming, and anonymized transactions.[1] Another trend is the rise in sextortion of minors, who are coerced or exploited into exchanging sexual images via the internet, mobile devices, and social media platforms.[2] OCSE offenders often groom[3] minors to share or post self-generated content online in exchange for money.

FinCEN performed a review of OCSE-related SARs and observed the following trends. Between 2017 and 2020, there was a 147 percent increase in OCSE-related SAR filings, including a 17 percent year-over-year increase in 2020. FinCEN also observed that OCSE offenders are increasingly

1. *See* Federal Bureau of Investigation (FBI) Press Release, "School Closings due to COVID-19 Present Potential for Increased Risk of Child Exploitation," (March 23, 2020), and U.S. Department of Justice, "Keeping Children Safe Online," (Updated, August 3, 2021). *See also* Europol, "Exploiting Isolation: Offenders and Victims of Online Child Sexual Abuse during the COVID-19 Pandemic," (June 13, 2020); Interpol, "Child Sexual Exploitation and Abuse – Threats and Trends," (September 20, 2020); and European Parliament, "Curbing the Surge in Online Child Abuse: The Dual Role of Digital Technology in Fighting and Facilitating its Proliferation," (November 2020).
2. Sextortion is an "online exploitation crime directed towards children in which non-physical forms of coercion are used, such as blackmail, to acquire sexual content from the child, engage in sex with the child, or obtain money from the child." *See* The National Center for Missing and Exploited Children (NCMEC), "Sextortion," (Accessed September 16, 2021).
3. According to the Department of Justice's (DOJ) Child Exploitation and Obscenity Section (CEOS), it is common for producers of child pornography to groom victims, or cultivate a relationship with a child and gradually sexualize the contact over time. The grooming process fosters a false sense of trust and authority over a child in order to desensitize or break down a child's resistance to sexual abuse. *See* DOJ CEOS, "Child Pornography," (Updated May 28, 2020). NCMEC has received reports that include instances of a child being groomed to sell or trade the child's sexual images or accept other incentives, such as gift cards. *See* NCMEC, "Online Enticement," (Accessed September 16, 2021).

using convertible virtual currency (CVC) (some of which provide anonymity), peer-to-peer mobile applications, the darknet, and anonymization and encryption services to try to avoid detection. CVC in particular is increasingly the payment method of choice for OCSE offenders who make payments to websites that host CSAM.[4] Finally, FinCEN found that OCSE facilitators attempt to conceal their illicit file sharing and streaming activities by transferring funds via third-party payment processors.[5]

Suspicious Activity Report (SAR) Filing Instructions

SARs, in conjunction with effective implementation of other BSA requirements, are crucial to identify and stop cybercrimes, including OCSE. Financial institutions should provide all pertinent and available information in the SAR narrative and attachments.[6]

- FinCEN requests that financial institutions reference **only** this notice in SAR field 2 (Filing Institution Note to FinCEN) using the keyword "**OCSE-FIN-2021-NTC3**"; this keyword should also be referenced in the narrative to indicate a connection between the suspicious activity being reported and the activities highlighted in this notice. Financial institutions may highlight additional advisory keywords in the narrative, if applicable.
- Financial institutions should also select SAR Field 38(z) (Other) as the associated suspicious activity type to indicate a connection between the suspicious activity reported and OCSE activity and include the term "OCSE" in the text box. If known, enter the subject's internet-based contact with the financial institution in SAR Field 43 (IP Address and Date).
- If human trafficking or human smuggling are suspected in addition to OCSE activity, financial institutions should also select SAR Field 38(h) (Human Trafficking) or SAR Field 38(g) (Human Smuggling), respectively.[7]
- FinCEN asks that reporting entities use the Child Sexual Exploitation (CSE) terms and definitions in the appendix below when describing suspicious activity, which will assist FinCEN's analysis of the SARs.

4. *See* U.S. Department of Justice Press Release, "South Korean National and Hundreds of Others Charged Worldwide in the Takedown of the Largest Darknet Child Pornography Website, Which was Funded by Bitcoin," (October 16, 2019), and U.S. Immigration and Customs Enforcement Press Release, "Dutch national charged in takedown of obscene website selling over 2,000 "real rape" and child pornography videos, funded by cryptocurrency," (March 12, 2020).
5. For a list of financial red flag indicators associated with human trafficking, including OCSE activity, *see* FinCEN Advisory, FIN-2020-A008, "Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity," (October 15, 2020). Recent publications related to financial intelligence and OCSE include: Egmont Group, "Combating Online Child Sexual Abuse and Exploitation through Financial Intelligence," (July 2020); and AUSTRAC Fintel Alliance, "Combating the Sexual Exploitation of Children for Financial Gain," (November 2019).
6. In the narrative, FinCEN requests that filers further address the details of the reported activity. When reporting OCSE-related activity, the inclusion of relevant technical cyber indicators (*e.g.*, chat logs, IP addresses, email addresses, filenames, and CVC addresses, such as bitcoin) is invaluable for locating and investigating the criminals perpetrating activity and thus critical to law enforcement.
7. OCSE does not necessarily indicate human trafficking or smuggling, but may overlap with regard to certain offenses noted in FinCEN's Human Trafficking Advisories, such as 18 U.S. Code § 1591 (sex trafficking of children or by force, fraud, or coercion), 18 U.S. Code § 2423 (transportation of minors), and 18 U.S. Code § 2422 (coercion and enticement).

- For additional information on reporting cyber-enabled crimes, including on how to file SARs, please see: FAQs for Reporting Cyber-Events, Cyber-Enabled Crime, and Cyber-Related Information. Collaboration between Bank Secrecy Act (BSA)/anti-money-laundering (AML) and cybersecurity units within financial institutions is an effective practice for gathering information helpful to identifying OCSE offenders and victims. Please refer to FinCEN's Advisory on Cyber-Events and Cyber-Enabled Crime, which contains examples of useful information to report including chat logs, IP addresses, email addresses, filenames, and CVC addresses, such as bitcoin. Financial institutions may consider sharing cyber-related information for the purposes of identifying and reporting money laundering and OCSE offenses.[8]

For Further Information

FinCEN's website at https://www.fincen.gov/ contains information on how to register for FinCEN Updates. Questions or comments regarding the contents of this notice should be addressed to the FinCEN Regulatory Support Section at frc@fincen.gov.

If you have immediate information to share with law enforcement, please contact the National Center for Missing and Exploited Children, which operates a Cyber Tip Line and hotline at 1-800-843-5678, in partnership with the FBI, DHS, and other law enforcement agencies.

8. *See* FinCEN, "Section 314(b) Fact Sheet," (December 2020), which states that the safe harbor from liability set forth in section 314(b) of the USA PATRIOT Act may apply in certain situations to the sharing of cyber-related information, such as IP addresses. For information on sharing cyber-related information outside BSA safe harbor protections, *see* U.S. Department of Homeland Security and U.S. Department of Justice, "Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015," (October 2020).

Appendix: CSE Terms and Definitions[9]

Term	Definition
Child Sexual Exploitation[10]	This conduct includes travel in interstate or foreign commerce to engage in illicit sexual conduct with any child under the age of 18; extraterritorial child sexual abuse committed by U.S. citizens and nationals; child sex trafficking; and all other acts involving criminal sexual abuse of children under the age of 18.
Offenses Involving Child Pornography[11,12]	The production, advertisement, distribution, receipt, or possession of child pornography, or the livestreaming of child sexual abuse. Production of child pornography includes "sextortion," where offenders use deceit or non-physical forms of coercion, such as blackmail, to acquire child pornography depicting the targeted minors.[13] Child pornography is any visual depiction (photo, video, or livestream) showing minors involved in sexually explicit conduct.[14]
Online Child Sexual Exploitation[15]	The use of the internet or mobile phones as a means (1) to engage or attempt to engage in child sexual exploitation; (2) to persuade, induce, entice or coerce a minor to engage in any illegal sexual activity; or (3) to commit an offense involving child sexual abuse material.
Facilitator/ Intermediary[16]	Facilitators and intermediaries are the individuals or entities whose conduct facilitates or aids and abets the commission of the sexual offense against the child.

9. For additional information on the legal definitions of the sexual exploitation of children, *see* DOJ, "Citizen's guide to U.S. Federal Child Exploitation and Obscenity Laws," (Updated November 12, 2020).
10. *See* DHS, "Strategy to Combat Human Trafficking, the Importation of Goods Produced with Forced Labor, and Child Sexual Exploitation," (January 2020).
11. *Id*. The phrase "child pornography" is used in this document because that is the term that appears in federal law. However, this material is more commonly referred to as "child sexual abuse material."
12. *See* 18 U.S.C. § 2256(8)
13. *See* The NCMEC, "Sextortion," (Accessed September 16, 2021).
14. *See* 18 U.S.C. § 2256(2) for a definition of "sexually explicit conduct" relating to child pornography.
15. *See* United Nations Interagency Working Group, "Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse," (Accessed September 16, 2021).
16. *Id*.