FinCEN NOTICE

FIN-2025-NTC2 September 8, 2025

FinCEN Notice on Financially Motivated Sextortion

Suspicious Activity Report (SAR) Filing Request

FinCEN requests that financial institutions reference this Notice by including the key term "**FIN-2025-SEXTORTION**" in SAR Field 2 (Filing Institution Note to FinCEN) and the narrative, select SAR Field 38(z) (Other) as the associated suspicious activity type, and include the term "**SEXTORTION**" in the text box. If known, enter the subject's IP address in SAR Field 43.

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) is issuing this Notice to financial institutions[1] to assist in identifying and reporting suspicious activity related to financially motivated sextortion, a disturbing and increasingly common typology that can devastate the lives and families of its victims. Financially motivated sextortion[2] occurs when perpetrators, using fake personas, coerce victims to create and send sexually explicit images or videos of themselves, only to threaten to release the compromising material to the victims' friends and family unless the victims provide payment. The perpetrators of financially motivated sextortion schemes can target anyone, with many victims being over the age of 18, according to law enforcement. However, minors—especially boys between the ages of 14 and 17[3]—are a particularly vulnerable population and have been increasingly victimized in these schemes.[4] As such and as highlighted throughout this Notice, many resources to assist victims of these schemes serve minors, and their parents and caregivers.

According to law enforcement, in recent years reports of financially motivated sextortion incidents have dramatically increased, prompting law enforcement action against perpetrators, many of whom are based overseas.[5] In 2024, the FBI received nearly 55,000 reports of crimes related to

1. *See* 31 U.S.C. § 5312(a)(2); 31 C.F.R. § 1010.100(t).
2. Sextortion is a crime that often involves adults coercing minors, especially teenagers, into sending explicit images online. *See* Federal Bureau of Investigation (FBI), "Stop Sextortion" (last visited Aug. 2025). Financially motivated sextortion is primarily motivated by financial gain rather than prurient interest and targets individuals of all ages. *See* FBI, "Financially Motivated Sextortion" ("FBI: Financially Motivated Sextortion") (last visited Aug. 2025); FBI Sacramento, "Sextortion: A Growing Threat Preying Upon Our Nation's Teens" ("FBI Sacramento Sextortion Article") (Jan. 17, 2024).
3. *See* FBI: Financially Motivated Sextortion, *supra* note 2.
4. Financially motivated sextortion schemes that victimize minors are also a form of Online Child Sexual Exploitation (OCSE). *See* Financial Action Task Force (FATF), "Detecting, Disrupting, and Investigating Online Child Sexual Exploitation" ("FATF OCSE Report") (Mar. 12, 2025), at pp. 5, 7. For more information on other forms of OCSE, *see* FinCEN, FIN-2021-NTC3, "FinCEN Calls Attention to Online Child Sexual Exploitation Crimes" (Sept. 16, 2021).
5. *See, e.g.*, FBI, "FBI Surges Resources to Nigeria to Combat Financially Motivated Sextortion" ("FBI Operation Artemis") (Apr. 24, 2025); Department of Justice (DOJ), "Ivorian Men Arrested for International "Sextortion" and Money Laundering Scheme Resulting in Minor's Death" ("DOJ Ivorian Sextortion Scheme") (May 9, 2025).

sextortion and extortion, with financial losses totaling $33.5 million, a 59 percent increase in the number of reports received in 2023.[6] Additionally, according to Homeland Security Investigations (HSI), between October 2021 and July 2025 HSI received 8,483 tips related to sextortion, leading to 854 victim identifications, 232 criminal arrests, 96 indictments, and 16 convictions. Financially motivated sextortion is also a global phenomenon that has resulted in countries seeking to address the issue collectively as well as within their own borders.[7]

Tragically, cases of financially motivated sextortion have led to an alarming number of suicides by victims. According to the National Center for Missing and Exploited Children (NCMEC), since 2021, at least 36 teenagers have taken their own lives in response to the threat of their sexually explicit images being leaked.[8]

Financially motivated sextortion schemes are a gross abuse of the U.S. financial system. As such, FinCEN urges financial institutions to be vigilant in identifying suspicious activity that may be connected with financially motivated sextortion in furtherance of law enforcement investigations and to help prevent further victimization.

The content of this Notice aligns with FinCEN's Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) National Priorities, which identifies cybercrime and fraud as key AML/CFT priorities.[9] The information contained in this Notice is derived from Bank Secrecy Act (BSA) data, open-source reporting, and information provided by law enforcement partners.

How Financially Motivated Sextortion Works

Financially motivated sextortion usually occurs online through social media platforms. Perpetrators either create fake accounts or hack accounts of real individuals to impersonate someone known by the victim or to present themselves as a potential new friend. Typically, the perpetrators of financially motivated sextortion schemes will pose as an attractive member of the opposite sex around the same age as the intended target.[10]

Perpetrators of financially motivated sextortion attempt to learn as much as they can about the intended victim's interests from their social media profiles before contacting the individual. The perpetrator may initially make contact on social media or popular online video gaming platforms and may suggest moving their conversation to private messaging or video chatting apps. Soon after making contact with the victim, perpetrators ask for nude photos or other sexually explicit material,

6. FBI, "2024 Internet Crime Report" (Apr. 23, 2025), at p. 36.
7. *See* FBI, "International Law Enforcement Agencies Issue Joint Warning about Global Financial Sextortion Crisis" (Feb. 7, 2025); *see also* AUSTRAC, "AUSTRAC, AFP, ACCCE and industry partners team up to fight child exploitation" (Apr. 20, 2023); United Kingdom National Crime Agency, "National Crime Agency launches online campaign to tackle 'sextortion' among young teenage boys" (Mar. 20, 2025).
8. *See* Testimony of Yiota Souras, Chief Legal Officer of NCMEC, U.S. House Energy and Commerce Committee, Subcommittee on Commerce, Manufacturing, and Trade, "The World Wild Web: Examining Harms Online" (Mar. 26, 2025), at p. 11.
9. FinCEN, "Anti-Money Laundering and Countering the Financing of Terrorism National Priorities" (June 30, 2021).
10. *See* FBI Sacramento Sextortion Article, *supra* note 2; *see also* FBI: Financially Motivated Sextortion, *supra* note 2.

or offer to exchange nude photos with the victim.[11] Once the victim has sent explicit material, the perpetrator engages in financial extortion, threatening to publish the victim's compromising photos or to share them with the victim's friends and family unless the victim sends the perpetrator money.[12] Perpetrators of financially motivated sextortion schemes can extort their victims in a matter of minutes,[13] and often continually harass victims to make additional payments.[14] Victims have reported being further victimized by scammers falsely claiming to be recovery experts, attorneys, or law enforcement agents, who offer to retrieve a victim's explicit material or "go after the perpetrators." These scammers attempt to exploit victims' feelings of helplessness or embarrassment for financial gain and often charge high fees for their supposed services.

The perpetrators of financially motivated sextortion schemes are often located outside the United States—primarily in West African countries such as Benin, Cote d'Ivoire, and Nigeria, or Southeast Asian countries such as the Philippines—and typically target victims in English-speaking countries.[15] According to FinCEN's analysis of BSA data, the top reported jurisdictions where the subjects of suspicious transactions potentially related to financially motivated sextortion schemes were located, in rank order, include: Cote d'Ivoire, the United States, the Philippines, Monaco, Burkina Faso, the Dominican Republic, Kenya, Benin, and Nigeria (hereinafter referred to as "Jurisdictions of Concern"). In some cases, perpetrators may operate as part of an organized criminal group; however, in most instances, the perpetrators are individuals or small groups.[16] Some perpetrators may attempt to disguise their location through the use of virtual private networks (VPNs).

Reporting Financially Motivated Sextortion

Victims of financially motivated sextortion schemes should immediately report the activity to law enforcement. Victims can report it to the FBI through their local FBI field office, by calling **1-800-CALL-FBI**, or reporting it online at tips.fbi.gov.

Victims can also call the U.S. Department of Homeland Security's Know2Protect[17] Tipline **833-591-KNOW (5669)** or fill out the online NCMEC CyberTipline form at report.cybertip.org. A minor victim also can reach out directly to NCMEC for support at gethelp@ncmec.org or call NCMEC at **1-800-THE-LOST**.

Anyone being exploited should also:

- **Report** the perpetrator's account via the platform's safety feature.

11. *See* FBI, "Sextortion" (last visited Aug. 2025); *see also* HSI, "Sextortion: It's More Common Than You Think" (updated Feb. 10, 2025).
12. *See* FBI: Financially Motivated Sextortion, *supra* note 2.
13. *Id.*
14. *See* FATF OCSE Report, *supra* note 4, at p. 15.
15. *See* FBI Sacramento Sextortion Article, *supra* note 2; FBI Operation Artemis and DOJ Ivorian Sextortion Scheme, *supra* note 5.
16. *See, e.g.*, DOJ Ivorian Sextortion Scheme, *supra* note 5.
17. For more information about DHS's Know2Protect campaign to stop online child exploitation, visit https://www.dhs.gov/know2protect.

- **Block** the predator.
- **Save** the perpetrator's profile, messages, and images; those can help law enforcement identify and stop the perpetrator.
- **Turn** their phone on airplane mode until law enforcement can review it.
- **Ask** for help from a trusted adult or law enforcement.
- **Not send any money**: cooperating with the perpetrator rarely stops the blackmail and harassment—but law enforcement can.

For more information on sextortion and financially motivated sextortion, visit the FBI's resources on the threats at: fbi.gov/sextortion and fbi.gov/financialsextortion. NCMEC has also developed an interactive resource to educate minors and their parents to the difficult decisions that victims of financially motivated sextortion schemes must make. This interactive resource is available at noescaperoom.org.

Financial Sextortion Payments

Perpetrators of financially motivated sextortion schemes may initially demand that the victim send them a large payment to avoid the perpetrator releasing the victim's explicit material. Since minor victims typically do not have access to large amounts of money—or may have no money—a negotiation process normally ensues until the perpetrator and victim agree upon a dollar amount. Despite receiving an initial payment, however, the perpetrator will often continue to demand more payments from the victim. According to law enforcement and BSA reporting, most victim payments are for relatively small amounts (e.g., payments from minors may be between $10-$50, whereas adult victims typically pay higher amounts from $500-$2,500).[18] In some cases, minor victims may steal money from family members to meet the perpetrator's demands.

Payment Methods

Victims are often directed to send the extorted payments to a money mule[19] through a peer-to-peer (P2P) payment platform using a phone number or email address provided by the perpetrator.[20] However, other payment methods requested by the perpetrator could include a victim mailing checks, cash, or money orders to a third party, or sending convertible virtual currency (CVC) directly using P2P payment platforms or CVC kiosks.[21] In other instances, perpetrators may instruct victims to purchase prepaid access cards (*i.e.*, gift cards). In such cases, they may request a victim send a picture of a card's PIN so that the value can be extracted to make purchases of goods and other items.

18. *See also* FATF OCSE Report, *supra* note 4, at pp. 15, 20.
19. Money mules are people who are used, wittingly or unwittingly, by illicit actors to transfer value, either by laundering stolen money or physically transporting goods or other merchandise. *See* FATF, "Professional Money Laundering" ("July 2018 FATF Report") (July 2018), at p. 22.
20. *See* FBI: Financially Motivated Sextortion, *supra* note 2.
21. *See generally* FinCEN, FIN-2025-NTC1, "FinCEN Notice on the Use of Convertible Virtual Currency Kiosks for Scam Payments and Other Illicit Activity" (Aug. 4, 2025).

P2P payments made by victims may contain memos or other messages that subtly refer to the ongoing extortion (e.g., "delete the photos" or "please stop"). However, law enforcement has observed an increasing trend whereby perpetrators are directing victims to use benign or even charitable references such as "for orphans" or "for family" to evade scrutiny by financial institutions and law enforcement.

Case Study:

Ogoshi Brothers Sentenced to Lengthy Prison Terms in Sextortion Scheme that Resulted in Death of Teen

On September 5, 2024, Samuel Ogoshi and Samson Ogoshi of Lagos, Nigeria, were each sentenced to 210 months in prison followed by 5 years of supervised release for the crime of Conspiracy to Sexually Exploit Minors. On March 25, 2022, a 17-year-old high school student died as a result of this sextortion scheme, which targeted over 100 other victims, as well.

As detailed in their plea agreements, Samuel and Samson Ogoshi engaged in a scheme while living in Nigeria to sexually exploit more than 100 victims, including at least 11 identified minor victims. They purchased hacked social media accounts and used them to pose as young women, making fake profiles and using the messaging feature on the social media accounts to contact victims. They conducted online research about their victims to learn where they lived, attended school, worked, and the identities of their family and friends. They then solicited their minor victims to produce sexually explicit images of themselves. Once they received the images, they created a collage of pictures that included the sexually explicit image with other images of the victim and their school, family, and friends. The Ogoshi brothers threatened to disclose the collages to the family, friends, and classmates of the victim unless the victim agreed to pay money using online cash applications.[22]

Use of Money Mules

Perpetrators of financial sextortion schemes often leverage networks of money mules across multiple jurisdictions[23] to launder victims' payments, thereby adding layers of distance between themselves and their victims.[24] Certain money mules may be recruited by criminals via job advertisements for 'transaction managers' or through online social media interactions. Criminal

22. DOJ, "Ogoshi Brothers Sentenced To Lengthy Prison Terms In Sextortion Scheme That Resulted In Death Of Teen" (Sept. 5, 2024); *see also* Minutes of Sentencing, *United States v. Ogoshi, et al.*, No. 2:22-cr-00025-RJJ (W.D. Mich. Sept. 5, 2024).
23. *See, e.g.*, DOJ, "Five U.S.-Based Defendants Charged With Money-Laundering Conspiracy That Facilitated Foreign Sextortion Scheme" (Aug. 2, 2024); *see also* DOJ, "All Charged Money Launderers Tied to Nigerian Sextortion Scheme Plead Guilty" (Apr. 3, 2025); Indictment, *United States v. Green*, No. 2:24-cr-00017-RJJ (W.D. Mich. July 16, 2024); Plea Agreements, *United States v. Green* (various dates).
24. FBI, "Money Mules" ("FBI Money Mules") (last visited Aug. 2025).

networks that are perpetrating these schemes may also leverage diaspora populations in the United States with connections to the scammers to act as complicit money mules.[25] According to law enforcement, money mules complicit in these schemes typically profit from their services by taking a percentage fee—typically 20 percent—of the money they move through their accounts. Additionally, financial sextortion victims may be coerced into serving as money mules for the scammer.

As noted above, money mules receive victim payments in a range of ways, including P2P transfers, wire transfers, through money services businesses, or the mail.[26] These funds may then be further layered through the financial system by transferring the funds across multiple money mule accounts on P2P platforms and bank accounts. Law enforcement has also increasingly observed money mules converting these funds into CVC via P2P payment platforms. To further obfuscate the payment trail, these funds may eventually be withdrawn in cash by the money mule. A money mule will aggregate funds and send them to the overseas perpetrator. To move these funds overseas, the money mules typically either use a money transmitter who can arrange for the proceeds to be paid out in the local currency of the destination country, or the money mules may convert the consolidated funds into CVC and send the CVC to a CVC wallet that can be accessed by the perpetrators. In cases where the victim makes a payment using a prepaid access card, money mules may be tasked with purchasing goods like electronics or luxury clothing, which they then ship to the orchestrator of the scam overseas.[27]

Case Study:

Four Delaware Men Charged with International Sextortion and Money Laundering Scheme

According to a superseding indictment, Sidi Diakite, 30; Almamy Diaby, 22; Abdul Aziz Sangare, 26; and Abdoul Aziz Traore, 31—all residents of Wilmington, Delaware—and other co-conspirators allegedly operated an international, financially motivated sextortion and money laundering scheme in which the conspirators engaged in cyberstalking, interstate threats, extortion, money laundering, and wire fraud. As part of the scheme, the conspirators, utilizing multiple payment methods, attempted to extort approximately $6.9 million from thousands of potential victims, and they successfully extorted approximately $1.9 million from these victims through P2P platforms alone. The superseding indictment also charges Hadja Kone, 28, of Wilmington, Delaware, who was previously arrested in April; and Siaka Ouattara, 22, of Abidjan, Cote d'Ivoire. As alleged in the superseding indictment, the conspirators posed as young women online and initiated communications with thousands of potential victims,

25. *See* July 2018 FATF Report, *supra* note 19.
26. *See* FBI Money Mules, *supra* note 24.
27. *See, e.g.*, First Superseding Indictment, *United States v. Kone, et al.*, No. 1:24-cr-00041-1-GBW (D. Del. Aug. 15, 2024) ("*United States v. Kone*") (unsealed Sept. 5, 2024), at pp. 7-8.

who were primarily young men and included minors from the United States, Canada, and the United Kingdom. Ouattara, Kone, Diakite, Diaby, Sangare, Traore, and others also operated infrastructure to transfer the funds illegally obtained from the victims to conspirators located in Côte d'Ivoire and elsewhere overseas.[28]

The conspirators allegedly provided detailed instructions and directed victims to pay specified amounts of money to money mules in the United States. Payment methods included: (1) P2P payment transfer services; (2) money transmitters, payable to the money mules; (3) U.S. Postal Service money orders; and (4) prepaid access cards.

The conspirators allegedly used a variety of methods to collect and "cash out" the victims' funds, including: (1) receiving funds into the money mules' P2P accounts they controlled, transferring funds to linked U.S. bank accounts, and withdrawing the funds as cash; (2) retrieving cash in-person at locations of money transmitters; (3) receiving U.S. Postal Service money orders and cashing the money orders; and (4) obtaining identifiers of prepaid access cards and purchasing and receiving shipments of goods, including, luxury clothing, computers, and cell phones.

Finally, the conspirators allegedly employed several methods to transfer the victims' funds, after they had been converted to cash or goods, to Ouattara and others who were located in Cote d'Ivoire and elsewhere overseas, including: (1) delivering cash in-person to a money transmitter location and transferring the funds to Ouattara and others; (2) delivering cash in-person to a New York-based money transmitter, who arranged for funds to be converted to local currency and paid out in Cote d'Ivoire to Ouattara and others; and (3) re-shipping the purchased goods, directly or indirectly, to Ouattara and others.[29]

AI-Enabled Financially Motivated Sextortion and Online Child Sexual Exploitation

Recent increases in the availability of generative AI tools have enabled perpetrators of financially motivated sextortion schemes to insert a victim's likeness into realistic, sexually explicit images and videos (*i.e.*, "deepfakes").[30] The sale, production, or distribution of AI-generated child sexual abuse material (CSAM) and other illicit sexually explicit content is a form of online child sexual exploitation. According to law enforcement, when potential victims refuse to send sexually explicit material, perpetrators have used manipulated content to extort these individuals. Since April 2023, the FBI observed an uptick in sextortion victims reporting the use of fake images or videos created from content posted on a victim's social media page or web postings or non-explicit photos or

28. DOJ, "Four Delaware Men Charged with International "Sextortion" and Money Laundering Scheme" (Sept. 9, 2024); *United States v. Kone, supra* note 27.
29. *See United States v. Kone, supra* note 27, at pp. 7-8.
30. For more information about the use of AI-generated deep-fakes in fraud, *see* FinCEN, FIN-2024-Alert004, "FinCEN Alert on Fraud Schemes Involving Deepfake Media" (Nov. 13, 2024).

videos provided by the victim to the perpetrator or captured during video chats.[31] Based on an analysis of BSA reporting, transactions related to the suspected creation and purchase of illicit AI-generated content are often completed using CVC or other payment mechanisms such as prepaid cards, which predators may believe maintain their anonymity.

Take It Down

In May 2025, the TAKE IT DOWN Act was signed into law. The Act criminalizes the nonconsensual online publication or threat of online publication of intimate images, including AI-generated content (*i.e.*, deepfakes).[32]

Victims of financially motivated sextortion schemes should be aware that there are resources available to assist them, including takeitdown.ncmec.org.[33] This resource provides a free service to help remove online nude, partially nude, or sexually explicit photos and videos taken of victims under 18 from participating websites.

Red Flag Indicators of Financially Motivated Sextortion

FinCEN has identified the following red flag indicators to help detect, prevent, and report potential suspicious activity related to financially motivated sextortion. Because no single red flag is determinative of illicit or other suspicious activity, financial institutions should consider the surrounding facts and circumstances, such as a customer's historical financial activity, whether the transactions are in line with prevailing business practices, and whether the customer exhibits multiple related red flags, before determining if a transaction or attempted transaction is indicative of financially motivated sextortion or is otherwise suspicious.

Red Flag Indicators for Victims Experiencing Financially Motivated Sextortion

1. A customer, including a customer who is a minor with an account co-signed by a parent or guardian, makes a series of payments over a short period of time using P2P payment platforms to a recipient in a Jurisdiction of Concern, especially if the customer has no discernable personal connection to that geographic area.

2. A customer, especially a customer who is a minor with an account co-signed by a parent or guardian or who is a young adult, makes a series of P2P transfers that may be low, round dollar amounts (e.g., between $10-50) that are hundreds of dollars or less over a short period of time to an individual, or individuals, with whom the customer has no prior transaction relationship. The customer who receives these funds then rapidly transfers them via a P2P transfer to another account or accounts.

31. *See* FBI, I-060523-PSA, "Malicious Actors Manipulating Photos and Videos to Create Explicit Content and Sextortion Schemes" (June 5, 2023).
32. *See* Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act (TAKE IT DOWN Act), Pub. L. No. 119-12, 139 Stat. 55 (2025).
33. NCMEC, "Take it Down" (last visited Aug. 2025).

3. A customer makes payments that include payment memos with messages indicating extortion (*e.g.*, "delete the pictures," "please stop") and typically occur during late night and early morning hours.[34]

4. A customer, including a customer who is a minor with a P2P account co-signed by a parent or guardian, purchases CVC through a P2P platform and subsequently transfers the CVC to an unhosted CVC wallet with exposure to illicit finance risk based on blockchain analytics or to a CVC wallet with whom the customer has had no prior transaction relationship with no business or apparent lawful purpose.

5. A customer, including a customer who is a minor with an account co-signed by a parent or guardian, makes multiple, uncharacteristic purchases of prepaid access cards. These prepaid access cards are typically then redeemed in a different jurisdiction from where the cards were purchased.

Red Flag Indicators for Money Mule Accounts

6. A customer, including a customer who is a minor with an account co-signed by a parent or guardian, receives multiple P2P payments from unrelated accounts with which the customer had not previously interacted. The customer then rapidly transfers these funds via a P2P payment to another unrelated account or accounts. This activity may be indicative of a victim who is being coerced to act as a money mule.

7. A customer's account receives many deposits or transfers from P2P payment platforms, that may be hundreds of dollars or less, over a short period of time that are quickly withdrawn in cash or transferred to other accounts with no business or apparent lawful purpose.

8. A customer's P2P or bank account experiences a high volume of transfers to and from accounts in a Jurisdictions of Concern with no business or apparent lawful purpose.

9. A customer receives multiple P2P payments and subsequently uses these funds to purchase CVC. The customer then transfers the purchased CVC to an unhosted CVC wallet with exposure to illicit finance risk based on blockchain analytics or a CVC wallet that is hosted by a CVC exchange in a Jurisdiction of Concern.

10. A customer deposits or cashes multiple money orders that may be hundreds of dollars or less from individuals with whom the customer previously had no interaction and who may be geographically distant from the customer's location with no business or apparent lawful purpose.

34. *See* FATF OCSE Report, *supra* note 4, at pp. 20-21.

Reminder of Relevant BSA Obligations and Tools for U.S. Financial Institutions

Suspicious Activity Reporting
Other Relevant BSA Reporting
USA PATRIOT ACT Section 314(b) Information Sharing Authority

Suspicious Activity Reporting

A financial institution is required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity; is intended or conducted to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity.[35] All statutorily defined financial institutions may voluntarily report suspicious transactions under the existing suspicious activity reporting safe harbor.[36]

When a financial institution files a SAR, it is required to maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR.[37] Financial institutions must provide any requested SAR and all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency.[38] When requested to provide supporting documentation, financial institutions should take special care to verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency. A financial institution should incorporate procedures for such verification into its BSA compliance or AML program. These procedures may include, for example, independent employment verification with the requestor's field office or face-to-face review of the requestor's credentials.

SAR Filing Instructions

SARs, and compliance with other BSA requirements, are crucial to identifying and stopping financially motivated sextortion schemes. FinCEN requests that financial institutions indicate a connection between the suspicious activity being reported and the activities highlighted in this notice by including the key term "**FIN-2025-SEXTORTION**" in SAR Field 2 (Filing Institution Note to FinCEN), as well as in the narrative. Financial institutions may highlight additional advisory, alert, or notice keywords in the narrative, if applicable.

35. *See* 31 C.F.R. §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, 1030.320.
36. *See* 31 U.S.C. § 5318(g)(3). Financial institutions may report suspicious transactions regardless of amount involved and still take advantage of the safe harbor.
37. *See* 31 C.F.R. §§ 1020.320(d), 1021.320(d), 1022.320(c), 1023.320(d), 1024.320(c), 1025.320(d), 1026.320(d), 1029.320(d), 1030.320(d).
38. *Id.*; *see also* FinCEN, "Suspicious Activity Report Supporting Documentation" (June 13, 2007).

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 financially motivated sextortion activity and include the term "**SEXTORTION**" in the text box. If known, enter the subject's IP address in SAR Field 43.

Financial institutions should include all available information relating to the account and locations involved in the reported activity, identifying information related to other entities and persons involved in transactions potentially indicative of financially motivated sextortion. Financial institutions also should provide all available information regarding other domestic and foreign financial institutions involved in the activity; where appropriate, financial institutions should consider filing a SAR jointly on shared suspicious activity.[39]

Information Sharing

Information sharing among financial institutions is critical to identifying, reporting, and preventing financially motivated sextortion schemes or other illicit financial activity. Financial institutions and associations of financial institutions sharing information under the safe harbor authorized by section 314(b) of the USA PATRIOT Act are reminded that they may share information with one another regarding individuals, entities, organizations, and countries suspected of possible terrorist financing or money laundering.[40] FinCEN strongly encourages such voluntary information sharing. FinCEN encourages U.S. financial institutions to use, and potentially expand, their existing processes to collect and share information with foreign financial institutions in furtherance of investigations that involve cross-border activity.

39. *See* 31 C.F.R. §§ 1020.320(e)(1)(ii)(A)(2))(i), 1021.320(e)(1)(ii)(A)(2)), 1022.320(d)(1)(ii)(A)(2), 1023.320(e)(1)(ii)(A)(2)(i), 1024.320(d)(1)(ii)(A)(2), 1025.320(e)(1)(ii)(A)(2), 1026.320(e)(1)(ii)(A)(2)(i), 1029.320(d)(1)(ii)(A)(2), 1030.320(d)(1)(ii)(A)(2).
40. *See* FinCEN, "Section 314(b) Fact Sheet" (Dec. 2020).

The Financial Crimes Enforcement Network's Advisory Program communicates priority money laundering, terrorist financing, and other illicit finance threats and vulnerabilities to the U.S. financial system. Financial institutions may use this information to support effective, risk-based, and reasonably designed anti-money laundering and countering the financing of terrorism (AML/CFT) programs and suspicious activity monitoring systems to help generate highly useful information for law enforcement and national security agencies.

For Further Information

FinCEN's website at 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 by submitting an inquiry at www.fincen.gov/contact.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit activity, counter money laundering and the financing of terrorism, and promote national security through strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.