# FinCEN ADVISORY

**FIN-2020-A008** **October 15, 2020**

# Supplemental Advisory on Identifying and Reporting Human Trafficking and Related Activity

***Human traffickers and their facilitators exploit the innocent and most vulnerable of our society for financial gain, employing an evolving range of money laundering tactics to evade detection, hide their proceeds, and grow their criminal enterprise.***

**This Advisory should be shared with:**

- *Chief Executive Officers*
- *Chief Operating Officers*
- *Chief Compliance Officers*
- *Chief Risk Officers*
- *AML/BSA Departments*
- *Legal Departments*
- *Cyber and Security Departments*
- *Customer-Facing Staff*
- *Money Services Businesses*
- *Casinos*

**SAR Filing Request:**

FinCEN requests financial institutions reference this advisory in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the following key term: "**HUMAN TRAFFICKING FIN-2020-A008**" and selecting **SAR Field 38(h)** (human trafficking). Additional guidance appears near the end of this advisory.

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to help save lives, and to protect the most vulnerable in our society from predators and cowards who prey on the innocent and defenseless for money and greed. This advisory supplements the 2014 FinCEN Guidance on Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking – Financial Red Flags ("2014 Advisory").[1]

Human traffickers and their facilitators exploit adults and children in the United States, and around the world, for financial gain, among other reasons. Victims are placed into forced labor, slavery, involuntary servitude, and peonage, and/or forced to engage in commercial sex acts. Anyone can be a victim regardless of origin, sex, age, or legal status.[2] And anyone can be a trafficker, from a single individual, such as a family member, to a criminal network, terrorist organization, or corrupt government regime.[3] The global COVID-19 pandemic can exacerbate the conditions that contribute to human trafficking, as the support structures for potential victims collapse, and

1. FinCEN Advisory, FIN-2014-A008, "Guidance on Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking – Financial Red Flags," (September 11, 2014).
2. *See* U.S. Department of Homeland Security, Blue Campaign, "What is Human Trafficking?"
3. *See* U.S. Department of State, "Trafficking in Persons Report," (June 2019); *see also* Financial Action Task Force, "Financial Flows from Human Trafficking," p. 15 (July 2018).

traffickers target those most impacted and vulnerable.[4] Other effects of the pandemic (e.g., travel limitations, shelter-in-place orders, teleworking) also may affect the typologies and red flag indicators provided below.

Unfortunately, in addition to the horrific toll on victims and their families, their very lives, dignity, and livelihood, human trafficking is now one of the most profitable and violent forms of international crime, generating an estimated $150 billion worldwide per year.[5] In the United States, human trafficking now occurs in a broad range of licit and illicit industries (e.g., hospitality, agricultural, janitorial services, construction, restaurants, care for persons with disabilities, salon services, massage parlors, retail, fairs and carnivals, peddling and begging, child care, domestic work, and drug smuggling and distribution).[6] Transactions involving proceeds generated by human trafficking can be the basis for federal criminal charges and asset forfeiture, as human trafficking and associated crimes constitute specified unlawful activities (SUAs) for the crime of money laundering.[7]

Since the 2014 Advisory, FinCEN collaborated with law enforcement to identify 20 new financial and behavioral indicators of labor and sex trafficking, and four additional typologies. This advisory provides: (i) new information to assist in identifying and reporting human trafficking, and to aid the global effort to combat this crime; and (ii) two illustrative recent case studies. The 2014 Advisory remains relevant, and provides information related to human smuggling, in addition to human trafficking.

**Human Smuggling**

*Acts or attempts to bring unauthorized aliens to or into the United States, transport them within the U.S., harbor unlawful aliens, encourage entry of illegal aliens, or conspire to commit these violations, knowingly or in reckless disregard of illegal status.*[8]

**Human Trafficking**

*The act of recruiting, harboring, transporting, providing or obtaining a person for forced labor or commercial sex acts through the use of force, fraud, or coercion.*[9]

4. Polaris, "COVID-19 May Increase Human Trafficking in Vulnerable Communities," (April 7, 2020). *See also* U.S. Department of State, "Trafficking in Persons Report," (June 2019) (discussing the vulnerabilities that traffickers target globally).
5. International Labour Organization, "Profits and Poverty: The Economics of Forced Labour," p. 13, (May 20, 2014). *See also* U.S. Department of the Treasury, "Combatting Human Trafficking," (January 29, 2020).
6. *See* U.S. Department of State, "Trafficking in Persons Report," pp. 491–492 (June 2019). Relatedly, goods that are produced by forced or child labor can be illegally imported into the United States. The U.S. Customs and Border Protection issues Withhold and Release Orders against imported merchandise suspected of being produced from forced or child labor. The U.S. Department of Labor maintains a list of goods and their source countries, which it has reason to believe are produced by forced or child labor in violation of international standards.
7. SUAs relevant to human trafficking cases include a variety of offenses listed under 18 U.S.C. §§ 1956(c)(7) and 1961(1), such as those listed in Title 18, unless otherwise specified.
8. *See* 8 U.S.C. § 1324. *See also*, U.S. Department of State, "Human Trafficking and Migrant Smuggling: Understanding the Difference," (June 27, 2017).
9. *See generally* 18 U.S.C. §§ 1581, 1584, 1589, 1590, 1591, 2421, 2422, 2423, and 2425; 22 U.S.C. §§ 7102(4) and (11); The Victims of Trafficking and Violence Protection Act of 2000 (Pub. L. No. 106-386); applicable state laws; and U.S. Department of State, "Report on U.S. Government Efforts to Combat Trafficking in Persons," (December 1, 2017).

In contrast to human smuggling, human trafficking does not require movement. Human traffickers can exploit individuals within the border of a country, and even in a victim's own home. Human trafficking can also begin as human smuggling, as individuals who enter a country voluntarily and illegally are inherently vulnerable to abuse and exploitation, and often owe a large debt to their smuggler.[10]

Because the information financial institutions collect and report is vital to identifying human trafficking and stopping the growth of this crime, it is imperative that financial institutions enable their detection and reporting of suspicious transactions by becoming aware of the current methodologies that traffickers and facilitators use. It is also critical that customer-facing staff are aware of behavioral indicators that may indicate human trafficking, as the only outside contact for victims of human trafficking may occur when visiting financial institutions.

## I. New Typologies of Human Trafficking

To evade detection, hide their illicit proceeds, and profit off the backs of victims, human traffickers employ a variety of evolving techniques. Below are four typologies, identified in Bank Secrecy Act (BSA) data since FinCEN issued the 2014 Advisory, that human traffickers and facilitators have used to launder money.

*1. Front Companies*

Human traffickers routinely establish and use front companies, sometimes legal entities, to hide the true nature of a business, and its illicit activities, owners, and associates. Front companies are businesses that combine illicit proceeds with those gained from legitimate business operations. Examples of front companies used by human traffickers for labor or sex trafficking include massage businesses, escort services, bars, restaurants, and cantinas.[11] In the case of businesses that act as a front for human trafficking, typically the establishment appears legitimate with registrations and licenses. The front company generates revenue from sales of alcoholic beverages and cover charges. Patrons, however, also can obtain illicit sexual services from trafficked individuals, usually elsewhere in the establishment.[12] In addition, illicit massage businesses or nail and hair salons can offer sexual services under the guise of legitimate businesses and/or exploit individuals for the purpose of forced labor.[13] Often, these establishments will appear to be a single storefront, yet are part of a larger network. Payments for these illicit services are usually in cash, and traffickers may invest the illicit proceeds in high-value assets, such as real estate and cars.

10. *See* U.S. Immigrations and Customs Enforcement, "Human Trafficking vs Human Smuggling," (Summer 2017); and *see also* U.S. Department of State, "Human Trafficking and Migrant Smuggling: Understanding the Difference," (June 27, 2017).
11. An establishment that provides food, drinks, dancing, and music, and is typically found in Latin American communities.
12. *See* Financial Action Task Force, "Financial Flows from Human Trafficking," p. 54 (July 2018). *See also* U.S. Department of Justice, "Sex Trafficking Ring Leader Gets Life in Federal Prison," (January 20, 2016).
13. U.S. Department of Justice, "What is Human Trafficking?" (January 6, 2017).

*2. Exploitative Employment Practices*

Some seemingly legitimate businesses use exploitative employment schemes, such as visa fraud and wage retention, to amass profit from labor and sex trafficking. For instance, some labor recruiters mislead or defraud victims, taking advantage of workers before and after they enter the United States. Some labor recruiters also mislead workers about the conditions and nature of a job, engage in contract switching, and confiscate or destroy workers' identity documents.[14] Foreign nationals who have legitimate temporary work or student visas also can be exploited.[15]

Another common practice is to charge exploitative fees to workers by withholding their salary or paying less than promised. The trafficker claims that the fees cover the costs of recruitment or access to job opportunities.[16] Recruitment fees can range from hundreds of dollars to tens of thousands of dollars, and take years to repay.[17] Victims' salaries are transferred to the traffickers or their co-conspirators via teller checks or wire transfers. Proceeds also can be "disguised" as a legitimate business expense, such as a cleaning service. Financial institutions may see multiple employees receiving their salaries in the same account, or payment for employment may be followed by immediate withdrawal or transfer into another account.[18]

*3. Funnel Accounts*

Funnel accounts generally involve an individual or business account in one geographic area that receives multiple cash deposits, often in amounts below the cash reporting threshold, from which the funds are withdrawn in a different geographic area with little time elapsing between the deposits and withdrawals.[19] Human traffickers may use interstate funnel accounts to transfer funds between geographic areas, move proceeds rapidly, and maintain anonymity.[20] In labor and sex trafficking schemes, human traffickers may open accounts in their name, or escort victims to a bank, and force them to open an account.[21] Traffickers maintain control of the victims' bank accounts through coercion, and direct victims to deposit money into their accounts and other accounts that the traffickers can access.[22] In some cases, victims also are coerced or forced to wire proceeds via money services businesses (MSBs) to facilitate the funneling of proceeds.

14. U.S. Department of State, "Paying to Work: The High Cost of Recruitment Fees," (June 27, 2017); *see also* U.S. Department of Justice, "Brothers Sentenced to 20 Years for Running Violent Human Trafficking Enterprise," (February 25, 2016).
15. U.S. Department of Justice, Journal of Federal Law and Practice, "Human Trafficking," Executive Office of United States Attorneys, pp. 5 and 28, (November 2017).
16. For more information *see* U.S. Department of Justice, "Leader of Human Trafficking Organization Sentenced to Over 15 Years for Exploiting Guatemalan Migrants at Ohio Egg Farms," (June 27, 2016); and U.S. Department of Justice, "Brothers Sentenced to 20 Years for Running Violent Human Trafficking Enterprise," (February 25, 2016).
17. *See* U.S. Department of State, "Paying to Work: The High Cost of Recruitment Fees," (June 27, 2017).
18. Financial Action Task Force, "Financial Flows from Human Trafficking," p. 28, (July 2018).
19. FinCEN Advisory, FIN-2014-A005, "Update on U.S. Currency Restrictions in Mexico: Funnel Accounts and TBML," p. 1, (May 28, 2014).
20. *See* U.S. Immigration and Customs Enforcement, "Using a Financial Attack Strategy to Combat Human Trafficking," (January 29, 2015).
21. For additional behavioral indicators of human trafficking, *see* Section II, *infra*.
22. Policies of certain large national banks to restrict third-party cash deposits for private customer accounts seem to have lessened the use of funnel account activity.

Case Study: Funnel Accounts Facilitate International Thai Sex Trafficking Ring

*4. Alternative Payment Methods*

In addition to payment via cash, traffickers also have accepted payment via credit cards, prepaid cards,[23] mobile payment applications, and convertible virtual currency.[24] Buyers of commercial sex use prepaid cards—a method of payment using funds paid in advance, which can be acquired anonymously with cash or on darknet websites—to register with escort websites and to purchase sexual services, flights, throw-away phones, and hotel rooms.[25]

Illicit actors also use virtual currency to advertise commercial sex online. For example, human traffickers have purchased prepaid cards, and then used the cards to purchase virtual currency on a peer-to-peer exchange platform. Human traffickers then use the virtual currency to buy online advertisements that feature commercial sex acts to obtain customers.[26]

FinCEN also has identified transactions in which human traffickers use third-party payment processors (TPPPs) to wire funds, which gives the appearance that the TPPP is the originator or beneficiary of the wire transfer and conceals the true originator or beneficiary. For example, human traffickers facilitate payments via TPPPs for the operation of online escort services and online streaming services that use voice-over Internet protocol technology. Human traffickers and their facilitators use TPPPs to wire funds to individuals or businesses both domestically and abroad.[27]

Case Study: Trafficking Involving Prepaid Cards and Bitcoin

## II. Behavioral and Financial Red Flag Indicators of Human Trafficking

In applying the red flags below and the red flags in the 2014 Advisory, financial institutions are advised that no single red flag is a clear indicator of human trafficking activity, although each can be indicative of forced labor and/or sex trafficking. Given that human trafficking is a predicate offense to money laundering, the financial red flags also may be indicative of other money laundering-related offenses. Financial institutions should consider additional factors, such as a customer's previous financial activity and the existence of typologies or other red flags, when determining whether transactions may be associated with human trafficking.

23. *See* U.S. Department of the Treasury, "National Money Laundering Risk Assessment," p. 15-16, (2018).
24. For more information about illicit activity involving convertible virtual currency *see* FinCEN Advisory, FIN-2019-A003, "Advisory on Illicit Activity Involving Convertible Virtual Currency," (May 9, 2019).
25. *See* New York County District Attorney Cyrus Vance Jr.'s testimony, "Following the Money: How Human Traffickers Exploit the U.S. Financial Markets: Hearing before the Subcommittee on Oversight and Investigations of the Committee on Financial Services of the U.S. House of Representatives," (January 30, 2018). *See also* U.S. Department of Homeland Security, "Using a Financial Attack Strategy to Combat Human Trafficking," (January 29, 2015); and U.S. Department of the Treasury, "National Money Laundering Risk Assessment," p. 15-16, (2018).
26. *See* New York County District Attorney Cyrus Vance Jr.'s testimony, "Following the Money: How Human Traffickers Exploit the U.S. Financial Markets: Hearing before the Subcommittee on Oversight and Investigations of the Committee on Financial Services of the U.S. House of Representatives," (January 30, 2018); and Financial Action Task Force, "Financial Flows from Human Trafficking," p. 55-56, (July 2018).
27. *See*, e.g., Financial Action Task Force, "Financial Flows from Human Trafficking," pp. 20-26, (July 2018).

## *Behavioral Indicators*

Many victims of human trafficking do not have regular contact with anyone other than their traffickers. The only outside contact they may have is when visiting financial institutions such as bank branches, check cashing counters, or money wiring services. Consequently, it is important that customer-facing staff consider the following behavioral indicators when conducting transactions,[28] particularly those that also present financial indicators of human trafficking schemes discussed below. As appropriate, such information should be incorporated into Suspicious Activity Report (SAR) filings and/or reported to law enforcement.[29] When incorporated into SAR filings, it is important that behavioral indicators, and the staff who witnessed them, are included in the SAR narrative so that information may be effectively searched for, and later used by, law enforcement.

This list is not exhaustive and is only a selection of behavioral indicators:[30]

1. A third party speaks on behalf of the customer (a third party may insist on being present and/or translating).
2. A third party insists on being present for every aspect of the transaction.
3. A third party attempts to fill out paperwork without consulting the customer.
4. A third party maintains possession and/or control of all documents or money.
5. A third party claims to be related to the customer, but does not know critical details.
6. A prospective customer uses, or attempts to use, third-party identification (of someone who is not present) to open an account.
7. A third party attempts to open an account for an unqualified minor.
8. A third party commits acts of physical aggression or intimidation toward the customer.
9. A customer shows signs of poor hygiene, malnourishment, fatigue, signs of physical and/or sexual abuse, physical restraint, confinement, or torture.
10. A customer shows lack of knowledge of their whereabouts, cannot clarify where they live or where they are staying, or provides scripted, confusing, or inconsistent stories in response to inquiry.

28. Additional resources discussing human trafficking and the role of financial institutions include the U.S. Department of Homeland Security, Blue Campaign, "Resources Page"; U.S. Department of the Treasury, "Combatting Human Trafficking," (January, 29, 2020); U.S. Department of State, "Tracking Suspicious Financial Activity to Address Human Trafficking," (June 28, 2018); U.S. Immigration and Customs Enforcement, "Using a Financial Attack Strategy to Combat Human Trafficking," (January 29, 2015); and Financial Action Task Force, "Financial Flows from Human Trafficking," (July 2018).
29. To report suspicious activity indicative of human trafficking to the U.S. Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Tip Line, call 1-866-DHS-2-ICE (1-866-347-2423) 24 hours a day, seven days a week, every day of the year. The Tip Line is also accessible outside the United States by calling 802-872-6199.
30. *See* Organization for Security and Co-operation in Europe, "Following the Money: Compendium of Resources and Step-by-step Guide to Financial Investigations into Trafficking in Human Beings," (November 7, 2019).

## *Financial Indicators*

To help identify and report transactions possibly associated with human trafficking, FinCEN has identified 10 new financial red flag indicators. These red flags do not replace the red flags identified in the 2014 Advisory, all of which remain relevant.[31] The Financial Action Task Force report on the "Financial Flows from Human Trafficking" also provides numerous indicators of money laundering related to human trafficking.[32]

11. Customers frequently appear to move through, and transact from, different geographic locations in the United States. These transactions can be combined with travel and transactions in and to foreign countries that are significant conduits for human trafficking.[33]

12. Transactions are inconsistent with a customer's expected activity and/or line of business in an apparent effort to cover trafficking victims' living costs, including housing (e.g., hotel, motel, short-term rentals, or residential accommodations), transportation (e.g., airplane, taxi, limousine, or rideshare services), medical expenses, pharmacies, clothing, grocery stores, and restaurants, to include fast food eateries.

13. Transactional activity largely occurs outside of normal business operating hours (e.g., an establishment that operates during the day has a large number of transactions at night), is almost always made in cash, and deposits are larger than what is expected for the business and the size of its operations.

14. A customer frequently makes cash deposits with no Automated Clearing House (ACH) payments.

15. An individual frequently purchases and uses prepaid access cards.

16. A customer's account shares common identifiers, such as a telephone number, email, and social media handle, or address, associated with escort agency websites and commercial sex advertisements.

17. Frequent transactions with online classified sites that are based in foreign jurisdictions.

18. A customer frequently sends or receives funds via cryptocurrency to or from darknet markets or services known to be associated with illicit activity. This may include services that host advertising content for illicit services, sell illicit content, or financial institutions that allow prepaid cards to pay for cryptocurrencies without appropriate risk mitigation controls.

19. Frequent transactions using third-party payment processors that conceal the originators and/or beneficiaries of the transactions.

20. A customer avoids transactions that require identification documents or that trigger reporting requirements.

31. FinCEN Advisory, FIN-2014-A008, "Guidance on Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking – Financial Red Flags," (September 11, 2014).
32. Financial Action Task Force, "Financial Flows from Human Trafficking," pp. 65-70, (July 2018).
33. For information on specific countries, and whether they are conduits for human trafficking, *see* U.S. Department of State, "Trafficking in Persons Report," (June 2019).

# Case Studies

## *Funnel Accounts Facilitate International Thai Sex Trafficking Ring*

In December 2018, 36 defendants were found guilty in St. Paul, Minnesota, for their various roles in operating an international sex trafficking ring, i.e., traffickers, house bosses, money launderers, and facilitators. Traffickers based in Thailand lured women to the United States through false promises of a better life. To facilitate the transport of the victims, the organization engaged in visa fraud by creating false identification documents, and forced many of the victims to enter into fraudulent marriages and debt bondage. In exchange, each victim incurred a debt of $55,000, which far exceeded actual expenses. Once in the United States, the victims were sent to various cities, isolated in a residence, and forced to pay off their debt by engaging in commercial sex acts.[34]

To conceal and redistribute the proceeds of the sex trafficking business, victims were forced to open U.S. bank accounts in Los Angeles in their own names. Once an account was opened, however, traffickers based in the United States took control of the account, kept a percentage of the cash generated, and sent the remainder back to the traffickers in Thailand. Other members of the organization, the "facilitators," rented the houses, apartments, and hotels, and facilitated the transport of victims.

The organization used funnel accounts to launder money deposited in cities across the United States to third-party launderers who made cash withdrawals in Los Angeles.[35] According to data made available to FinCEN, deposits were made in cash, and were just enough to cover account debits. To move funds to and from Thailand, the organization employed third-party money launderers who made bank accounts available and coordinated cash deposits and withdrawals.

Bulk cash smuggling was another scheme used to physically transport proceeds to Thailand. According to law enforcement, individuals were recruited to carry large volumes of cash in suitcases and transport the money to Thailand. To evade detection, the trafficking organization paid flight attendants to keep quiet, and in some limited instances, to transport bulk cash in their own luggage. Money also was concealed in clothing and dolls that were shipped to Thailand. To date, law enforcement has recovered $1.5 million in cash, and testimony revealed that more than $40 million was sent to Thailand by one money launderer alone.

34. For information on this case, *see* U.S. Department of Justice, "Twenty-One Additional Defendants Indicted for their Roles in Thai Sex Trafficking Enterprise," (May 25, 2017); *see also* U.S. Department of Justice, "Thirty-Six Defendants Guilty for their Roles in International Thai Sex Trafficking Organization," (December 13, 2018).
35. For a definition of third-party money launderers *see* U.S. Department of Homeland Security, "Third Party Money Launderers," (Summer 2017).

### *Trafficking Involving Prepaid Cards and Bitcoin*

In April 2016, law enforcement agents from HSI in El Paso, Texas, responded to a call made to local police regarding a woman who was being forcibly held by an individual identified as "Tae" at a motel. Officers discovered two adult victims when they searched the motel room. Police located William "Tae" Harris, who was stopped while driving a suspect vehicle in the area. He possessed a semi-automatic firearm. Harris and his passenger, Dean Hall, were members of the West Side City Crips gang from Phoenix, Arizona.

The subsequent HSI investigation revealed that Harris and Hall brought the victims to Texas from Arizona, where the victims were forced into prostitution, beaten, and suffered threats of violence. HSI determined that at least three other West Side City Crips were operating a prostitution scheme in El Paso. During a forensic extraction of Harris' mobile phone, HSI discovered bitcoin transaction data and was able to exploit Harris' bitcoin wallet information. Evidence revealed that the group's illicit activity revolved around the purchase of Vanilla Visa prepaid credit cards, which were then used to purchase bitcoin on the Paxful virtual currency exchange. Those bitcoin were used to purchase prostitution ads on Backpage.com. Furthermore, during Harris' prosecution, HSI uncovered and disrupted an attempted murder-for-hire in which Harris planned to have a key witness and her sister murdered.

In January 2018, Hall and Harris were convicted and sentenced for violating several anti-trafficking statutes. Hall was sentenced to 90 months' imprisonment and five years of supervised release, and Harris was sentenced to 180 months' imprisonment and ten years of supervised release.

## Guidance to U.S. Financial Institutions

### Customer Due Diligence and Identification of Beneficial Owners of New Legal Entity Accounts

As of May 11, 2018, FinCEN's Customer Due Diligence (CDD) Rule requires banks, brokers or dealers in securities, mutual funds, and futures commission merchants and introducing brokers in commodities to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions.[36] Identifying and verifying the beneficial owners of legal entities could facilitate the identification of the beneficiaries of the illicit proceeds.

36. *See* 31 CFR § 1010.230 (describing beneficial ownership requirements for legal entity customers).

## Information Sharing

Information sharing among financial institutions is critical to identifying, reporting, and preventing evolving fraud schemes. 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 relating to transactions that the institution suspects may involve the proceeds of one or more SUAs and such an institution still will remain protected from civil liability under section 314(b) safe harbor. The SUAs listed in 18 U.S.C. §§ 1956 and 1957 include an array of fraudulent and other criminal activities, including fraud against individuals or the government. FinCEN strongly encourages information sharing via section 314(b) where financial institutions suspect that a transaction may involve terrorist financing or money laundering, including one or more SUAs.[37]

## Suspicious Activity Reporting (SAR)

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, or attempts 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.[38]

### *SAR Filing Instructions*

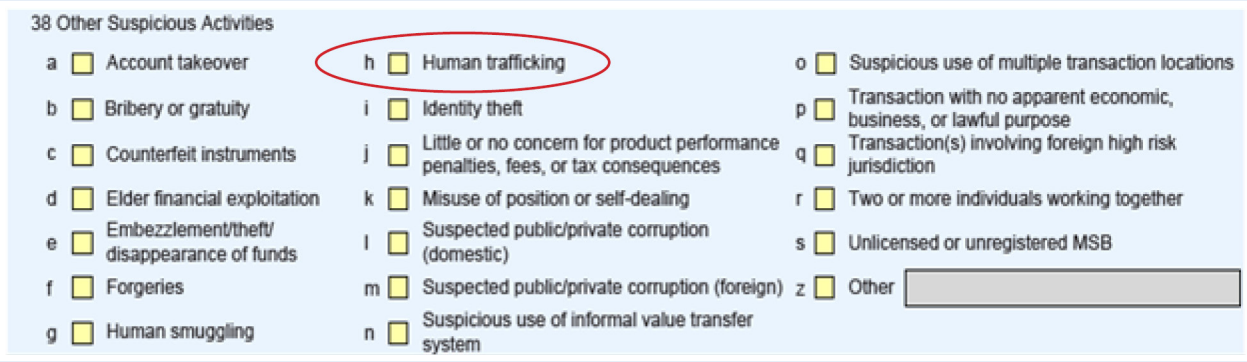
Financial institutions should provide all pertinent available information in the SAR form and narrative. A potential victim of human trafficking should not be reported as the subject of a SAR. Rather, all available information on the victim should be included in the narrative portion of the SAR. **FinCEN further requests that financial institutions reference this advisory by including the key term:**

**"HUMAN TRAFFICKING FIN-2020-A008"**

**in SAR field 2 (Filing Institution Note to FinCEN)** to indicate a connection between the suspicious activity being reported and the activities highlighted in this advisory. Additional information to include behavioral indicators, email addresses, phone numbers, and IP addresses also should be included when possible to aid law enforcement investigations.

37. For further guidance related to the 314(b) Program, *see* FinCEN Section 314(b) Fact Sheet (November 2016), and FinCEN Guidance FIN-2009-G002, "Guidance on the Scope of Permissible Information Sharing Covered by Section 314(b) Safe Harbor of the USA PATRIOT Act," (June 16, 2009).
38. 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320.

**Financial institutions that suspect human trafficking activity should also mark the check box for human trafficking (SAR Field 38(h)) on the SAR form.**


38 Other Suspicious Activities

| | | |
|---|---|---|
| a ☐ Account takeover | h ☐ Human trafficking | o ☐ Suspicious use of multiple transaction locations |
| b ☐ Bribery or gratuity | i ☐ Identity theft | p ☐ Transaction with no apparent economic, business, or lawful purpose |
| c ☐ Counterfeit instruments | j ☐ Little or no concern for product performance penalties, fees, or tax consequences | q ☐ Transaction(s) involving foreign high risk jurisdiction |
| d ☐ Elder financial exploitation | k ☐ Misuse of position or self-dealing | r ☐ Two or more individuals working together |
| e ☐ Embezzlement/theft/ disappearance of funds | l ☐ Suspected public/private corruption (domestic) | s ☐ Unlicensed or unregistered MSB |
| f ☐ Forgeries | m ☐ Suspected public/private corruption (foreign) | z ☐ Other |
| g ☐ Human smuggling | n ☐ Suspicious use of informal value transfer system | |

## For Further Information

Questions or comments regarding the contents of this advisory should be addressed to the FinCEN Regulatory Support Section at frc@fincen.gov.

**The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.**