ARE BANKS STUCK IN RUSH-HOUR (HUMAN) TRAFFIC(KING)?
Human trafficking remains one of the fastest growing illegal enterprises internationally. This issue is even more significant for banks, as they are in a unique position to identify red flags and prevent the facilitation of funding Human Trafficking.

Human Trafficking as a Global Issue for Financial Institutions

Human Trafficking is currently one of the fastest growing crimes internationally, as well as the most profitable. On an annual basis, the Association of Certified Anti-Money Laundering Specialists (ACAMS) has estimated that over 40 million people are victims of human trafficking, with approximately $150.2 billion in illegal profit each year. The profits of forced labor for each region are as follows:

The Financial Crimes Enforcement Network (FinCEN) defines human trafficking as 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. This crime, as others, require funneling of funds to support its success. Under Bank Secrecy Act and Anti-Money Laundering (BSA/AML) requirements, financial institutions must prevent the facilitation of human trafficking by monitoring customer accounts for suspicious activity.

Risks to Financial Institutions and Red Flags of Human Trafficking

Despite BSA/AML requirements, human traffickers target the financial services industry as their potential facilitators to fund this crime. Because human trafficking requires money to assist with the solicitation, transportation, kidnapping and exploitation of its victims, banks are used to launder money on both a global and local scale, including sending money to various jurisdictions. In an effort to stop this facilitation, FinCEN published its Guidance on Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking to detail the red flags specific for financial institutions. Key examples of customer activity that should be considered red flags include:

- Ongoing ATM/credit card transactions in even amounts between 10 PM and 6 AM;
- Credit card payments to online escort services for advertising;
- Use of anonymous monetary instruments to pay bills instead of personal checks;
- Structured cash deposits at multiple bank branch locations;
- Third party acting as custodian of the victim’s personal identification and usually accompanies this victim to the bank;
- Customer reading her address information from a form; and
- Customer using an interpreter to execute transactions, account-opening forms filled out in handwriting styles different from victims.

The reasoning for this monitoring is to determine if the account and transactional activity is inconsistent with the customer’s stated employment. If sudden changes in the activity occur outside of the customer’s expected profile, it could be a sign that the bank account is being used for human trafficking. Key examples of changes in expected activity that could signify human trafficking include:

- Unusual amounts of international purchases;
- Frequent or excessive travel expenses (foreign, out of town domestic and/or local);
- Irregular purchases on food, lodging or personal needs that do not reflect the customer’s daily living expenditures; and
- Rapid drawdown of deposited funds or salaries paid, often in cash and usage of funnel accounts, as well as high volume deposits through funnel accounts and immediate withdrawals from border towns.

Although no single red flag can confirm that human trafficking activity is occurring in a bank account,
financial institutions must ensure they have implemented an effective monitoring and training program to identify potential human trafficking red flags in connection with financial transactions.

The Responsibility of Financial Institutions

Financial institutions are subject to BSA/AML requirements to have an effective monitoring program in place to identify red flags in account activity. FinCEN issued guidance to help banks comply with human trafficking related BSA/AML requirements that may indicate financial activity related to human trafficking. This monitoring should be widely looked at because many traffickers deposit money from different areas and have many foreign deposits. Financial institutions are responsible for having monitoring procedures to detect human trafficking. Some of the following functions are recommended:

- Detect ongoing ATM/credit card transactions that are in even amounts between 10 PM to 6 AM, and identify patterns;
- Review credit card payments to online escort services to determine if they have the same number, high volumes of withdrawals and deposits in cash, and depositing in multiple bank branch locations;
- Monitor account activity to determine if its inconsistent, such as using it during different times during the day (many human traffickers deposit only in cash, in high volumes, during different times and in different banks so they go undetected);
- Determine if wires are sent from multiple locations to a common beneficiary account on the border, commonly known as a funnel account;
- Compare all customer addresses against all of the local post offices and postal stores in your area; and
- Conducting a string-search on the internet of your wires and Automated Clearing House (ACH) transactions against the high-risk countries for Human Trafficking.

After conducting transaction monitoring using the above steps, if a financial institution knows, suspects, or has reason to suspect that a transaction has no business or apparent lawful purpose or is inconsistent with the customer’s expected activity, and the financial institution knows of no “reasonable explanation” for the transaction, the financial institution should file a Suspicious Activity Report (SAR). SARs continue to be a valuable avenue for financial institutions to report suspected human trafficking. In addition, financial institutions must train their personnel to specifically identify red flags of human trafficking to be reported on a SAR, which will enable FinCEN and other law enforcement agencies to pursue these suspicious instances.

Sia Partners Added Value

Human Trafficking is the fastest growing crime and one of the most profitable ones, in the world, and financial institutions are at risk of facilitating its funding. This increase shows the vulnerability of financial institutions due in large part to the lack of BSA/AML controls such as transaction monitoring and proper training to customer-facing employees. It is instrumental for financial institutions to identify human trafficking red flags in order to mitigate potential corporate liability based on their failure to recognize financial transactions related to human trafficking. In order to help ensure that banks do not facilitate financial transactions related to human trafficking, banks must address their compliance issues related human trafficking, including BSA/AML requirements and best practices followed by other banks and ACAMS, including incorporating anti-human trafficking policies and procedures within their existing compliance framework.

Sia Partners has experience assisting financial institutions with their financial crime programs, and can leverage this experience to assess and enhance your bank’s BSA/AML procedures and trainings to adequately address human trafficking activity.
Sources


Copyright © 2019 Sia Partners. Any use of this material without specific permission of Sia Partners is strictly prohibited.
Sia Partners is a next generation consulting firm focused on delivering superior value and tangible results to its clients as they navigate the digital revolution. With over 1,400 consultants in 16 countries, we will generate an annual turnover of USD 280 million for the current fiscal year. Our global footprint and our expertise in more than 30 sectors and services allow us to enhance our clients’ businesses worldwide. We guide their projects and initiatives in strategy, business transformation, IT & digital strategy, and Data Science. As the pioneer of Consulting 4.0, we develop consulting bots and integrate AI in our solutions.

Follow us on LinkedIn and Twitter @SiaPartners

For more information, visit: www.sia-partners.com