December 2019

Illicit Financial Schemes Related to Fentanyl and other Opioids: Compliance Guide and Tips for Financial Institutions

Illicit trafficking, sale, distribution, and misuse of fentanyl and other synthetic opioids has landed the United States in the midst of unprecedented epidemic that not only results in death of more than 130 persons every day, it poses risks for the financial system who are being used for money laundering, sometimes in small denominations. Criminals generate billions of dollars in illicit drug proceeds and are using the U.S. financial system to advance their criminal enterprises and expand it further.

With an aim of safeguarding our financial system and enabling the Financial Institutions (FIs) in identifying and reporting activities under the Bank Secrecy Act, FinCEN issues advisories and in August 2019, it issued an advisory[1] to "assist financial institutions in detecting and reporting suspicious activity, making it harder and more costly for criminals to (i) commit these crimes; (ii) hide and use their illicit money; and (iii) continue fueling this epidemic".

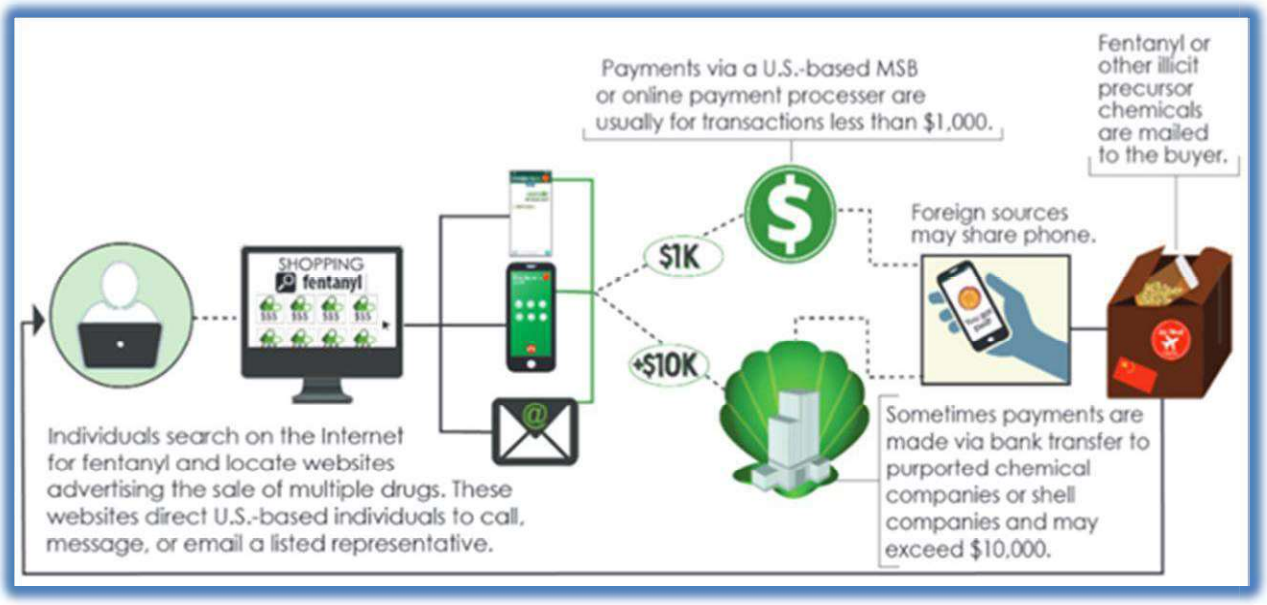
The advisory includes typologies related to sale of these illegal fentanyl and other synthetic opioids by foreign suppliers (primarily Chinese and Mexican), the methods used by Transnational Criminal Organizations (TCOs) to launder money and the financial methodologies associated with the sale and procurement of fentanyl over the Internet by purchasers located in the United States. It also includes red flags that would enable the FIs in creating alerts through their systems or otherwise monitor for the activities in case their institutions are being used for illicit manufacturing, importation, and/or distribution of illegal fentanyl and other synthetic opioids.

Typologies

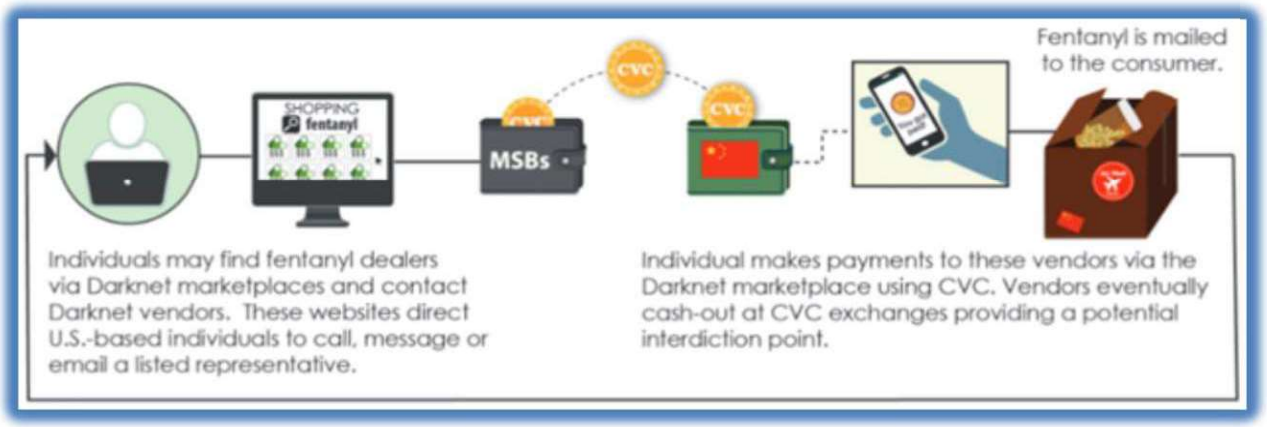
Whether the cross-border fentanyl trafficking is done by the TCOs or by smaller criminal networks, the predominant funding mechanisms include purchases from a foreign source using online payment processors and FIs (money services businesses and banks) or purchases from a foreign source of supply made using convertible virtual currency (CVC).

According to FinCEN, an analysis of sensitive financial data illustrates that when U.S. individuals purchase fentanyl directly from China and other foreign countries, they often structure the money transfers to evade Bank Secrecy Act (BSA) reporting and recordkeeping requirements, sometimes using multiple locations of the same FI. The analysis also revealed that the payments to the foreign sources are typically low-dollar-value transactions (less than $1,000), sometimes even conducted through multiple transactions. The following diagram illustrates how the FIs are being used for the payments related to these illicit activities between a buyer and seller:

[1] Whitepaper based on FinCEN Advisory: https://www.fincen.gov/sites/default/files/advisory/2019-08-21/Fentanyl%20Advisory%20FINAL%20508.pdf



Similar to purchases from a foreign source of supply using FIs or online payment processors, individuals purchase these illegal drugs using CVCs[2] as depicted in the following diagram:



FIs should be aware that quite often the criminals use shell companies to disguise the illicit drug proceeds as legitimate business transactions, and that individuals in the United States use their accounts to funnel money to international locations for this activity. These not only involve structured transactions, funnel

[2] FinCEN issued guidance regarding CVCs and an advisory earlier in 2019: FIN-2019-G001 and FIN-2019-A003 both dated May 9, 2019.

activity or bulk cash or monetary instruments cross-border smuggling but is increasingly using FIs for Trade Based Money Laundering (TBML) schemes, as this method of laundering money avoid the risks and difficulties associated with bulk cash smuggling.

FATF defines TBML as, "the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origins. In practice, this can be achieved through the misrepresentation of the price, quantity or quality of imports or exports. Moreover, TBML techniques vary in complexity and are frequently used in combination with other money laundering techniques to further obscure the money trail."[3] In this context, TBML often involves converting physical U.S. banknotes into a commodity (e.g. smartphone or jewelry) and then exporting or importing the commodity, without physical cross-border movement of the underlying currency.[4] The following figure depicts the typical cycle of TBML:

[3] http://www.fatf-gafi.org/publications/methodsandtrends/documents/trade-basedmoneylaundering.html

[4] FinCEN Advisory FIN-2014-A005 dated May 28, 2014

Some Key Red Flags indicating possible unusual or suspicious activities

While individual red flag may not be a conclusive indicator of suspicious activity, these help the FIs in reviewing the unusual activities against customer profile, due diligence information, negative news and transaction history. A single or multiple Red Flags, on investigation, may reveal suspicious activities that need reporting in terms of the Bank Secrecy Act. Some of the key indicators of unusual activities, i.e. the Red Flags related to Fentanyl-related Activities are:

- The company's NAICS code pertains to a different industry than the business name indicates.
- Company is associated with multiple businesses in unrelated industries.
- Company lacks or has vague company websites.
- Search on the address reveals presence of another business (with our without the same EIN), a different name or a residential address, even though the customer indicated otherwise
- Searches on the company reveal multiple active addresses, DBAs or operating locations, contradicting the information provided by the customer.
- Use of multiple accounts or locations for transactions.
- Structuring (the term used in statute for criminal activity (see 31 U.S.C. §5324), includes not only attempts to evade reporting requirements, but also attempts to evade the Travel Rule and related recordkeeping requirements).

What should the financial institutions do?

a. Be aware of the Red Flags related to the activity through the products and services offered;
b. Mitigate risks related to your products and services to ensure that it is within acceptable levels (e.g. Many large national banks restricted third-party cash deposits for private customer accounts to avoid Funnel Account Activities)
c. Train their employees on the Red Flags and unusual activity indicators;
d. Customize their monitoring rules and parameters to enable the Monitoring Systems generate Alerts for the Red Flags and related unusual activities;
e. Arrange Independent Validation of the Monitoring System, including for the adequacy of Rules and the accuracy of Alerts generated by their Monitoring System (also required to ensure compliance with OCC requirements and with NYS DFS Superintendent's Regulations Part 504);
f. Ensure that the Independent Testing (Internal Audit) is performed by Subject Matter Experts who can evaluate the rules and related disposition protocols, as well as determine the adequacy of validation as well as corrective actions taken on the recommendations of validation report, if any.

For further guidance or assistance regarding your AML/OFAC Programs; Training; Model Validations and Independent Testing requirements contact us at: info@RGSGlobalAdvisors.com.