August 21, 2019

Advisory to Financial Institutions on Illicit Financial Schemes and Methods Related to the Trafficking of Fentanyl and Other Synthetic Opioids

Transnational criminal organizations (TCOs), including Mexican, Chinese and other foreign fentanyl suppliers, and Internet purchasers located in the United States, engage in the trafficking of fentanyl, fentanyl analogues, and other synthetic opioids and the subsequent laundering of the proceeds from such illegal sales.

This advisory should be shared with Chief Executive Officers, Chief Operations Officers, Chief Risk Officers, Legal Departments, Chief Compliance/BSA Officers, AML Officials, Sanctions Compliance Officials, and Cybersecurity Units.

Introduction

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory[1] to alert financial institutions to illicit financial schemes and mechanisms related to the trafficking of fentanyl, fentanyl analogues, and other synthetic opioids,[2] and to assist them in detecting and reporting related activity.

The United States is in the midst of an unparalleled epidemic of addiction and death, fueled by the illicit trafficking, sale, distribution, and misuse of fentanyl and other synthetic opioids. The statistics are sobering; between 2013 and 2017, deaths in the United States from synthetic opioids, other than methadone, increased over 800 percent.[3] Every day in the United States, more than 130 people die from an opioid-related overdose.[4] These numbers alone cannot fully capture the devastation wrought by this epidemic, the consequences of which are far reaching and everlasting, from grieving parents and orphaned children, to the enormous economic and public policy costs,[5] and the destruction of current and future generations.

The epidemic is tearing away at the social and economic fabric of our communities, while TCOs, international drug traffickers, money launderers, and other criminal actors profit off

---

[1] This advisory is also part of a larger, United States government Fentanyl advisory covering the movement, manufacturing, marketing, and monetary aspects of the trafficking of fentanyl and other synthetic opioids. A summary of the *21st Century Drug Trafficking: Advisories on Fentanyl and Other Synthetic Opioids*, which includes links to each advisory, can be found here: https://www.whitehouse.gov/wp-content/uploads/2019/08/White-House-Fentanyl-Advisories-Summary.pdf

[2] The chemical names of synthetic opioids often sold online include: Acetylfentanyl, Butyrfentanyl, Carfentanil, FUF Fentanyl HCL, Furanylfentanyl, Isobutyrfentanyl, Lofentanil, 4'-methyl Acetyl fentanylHCL, Valerylfentanyl, and the U series, including U-47700. According to the Drug Enforcement Administration (DEA), informal slang terms for these variants include: 30s, Blues, Dragon's Breath, Fent, Fentanyl, Fenty, M-30s, etc. Additional slang words for fentanyl and other synthetic opioids can be found in the: DEA Intelligence Report on Drug Slang CodeWords.

[3] Centers for Disease Control and Prevention (CDC), National Center for Health Statistics, Multiple Cause of Death Files, 1999-2017 CDC WONDER Online Database, December 2018. Accessed December 2018.

[4] CDC/National Center for Health Statistics, National Vital Statistics System, Mortality. CDC WONDER, Atlanta, GA: U.S. Department of Health and Human Services, CDC; 2018. https://wonder.cdc.gov.

[5] National Institute on Drug Abuse, "Opioid Overdose Crisis," January 2019.

the misery of victims. Criminal networks and others generate billions of dollars in illicit drug proceeds, and use the U.S. financial system and economy to advance their criminal enterprises and continue this epidemic to generate more criminal profits, resulting in more deaths and addictions. FinCEN and other U.S. government agencies are collaboratively working with foreign partners, including Mexico, to end the fentanyl epidemic. This advisory will 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. By using the information in this advisory and safeguarding our financial system, financial institutions will help save lives, protect innocent families, and ensure the safety and future of our communities. Indeed, this is the real value and utility behind information generated, maintained, and reported under the Bank Secrecy Act by financial institutions. This advisory highlights the primary typologies and red flags derived from sensitive financial reporting which are associated with (i) the sale of these drugs by Chinese, Mexican, or other foreign suppliers; (ii) methods used by Mexican and other TCOs to launder the proceeds of fentanyl trafficking; and (iii) financial methodologies associated with the sale and procurement of fentanyl over the Internet by purchasers located in the United States.[6] Fentanyl is sold in the United States in many forms, all of which can be deadly. Fentanyl can be purchased alone; mixed with heroin, cocaine, or methamphetamine; or pressed into pill form and falsely sold as prescription opioids, many times being ingested by unsuspecting victims.

Typologies

Fentanyl trafficking in the United States generally follows one of two pathways: direct purchase of fentanyl from China by U.S. individuals for personal consumption or domestic distribution; or cross-border trafficking of fentanyl from Mexico by TCOs and smaller criminal networks. Within these two categories, the predominant funding mechanisms associated with fentanyl trafficking patterns include: (i) purchases from a foreign source of supply made using money services businesses (MSBs), bank transfers, or online payment processors; (ii) purchases from a foreign source of supply made using convertible virtual currency[7] (CVC) (such as bitcoin, bitcoin cash, ethereum, or monero); (iii) purchases from a U.S. source of supply made using an MSB, online payment processor, CVC, or person-to-person sales[8]; and

[6] Note that under U.S. federal law, fentanyl is a Schedule II controlled substance, which is lawfully produced and distributed in the United States by manufacturers of prescription drugs approved by the Food and Drug Administration and is widely used in medicine. This advisory focuses on the illicit manufacturing, importation, and/or distribution of illegal fentanyl and other synthetic opioids. Furthermore, while this advisory focuses on typologies involving fentanyl produced abroad and trafficked into the United States or purchased online, FinCEN is aware of trafficking in, and overprescribing of, pharmaceutical fentanyl in the United States and monitors and reports on illicit transactions associated with this activity.

[7] A type of virtual currency that either has an equivalent value in real currency or acts as a substitute for real currency. FIN-2013-G001, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," March 18, 2013; *see also* FIN-2019-G001, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," May 9, 2019, and FIN-2019-A003, "Advisory on Illicit Activity Involving Convertible Virtual Currency," May 9, 2019.

[8] Person-to-person in this context refers to the physical method of meeting in person and exchanging cash for fentanyl.

(iv) other, more general money laundering mechanisms associated with TCO procurement and distribution.

Direct Purchase of Fentanyl from China by U.S. Individuals for Personal Consumption or Domestic Distribution

Purchases from a Foreign Source of Supply Using MSBs Such as Money Transmitters or Online Payment Systems

Transactions related to the sale or purchase of fentanyl often involve money transfers to individuals in China and other foreign countries through MSBs, online payment processors, or bank transfers to individuals located in foreign countries. 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.[9] Individuals frequently transfer the funds using multiple MSB agent locations. Additionally, although payment recipients may seem to be unrelated to one another, in many cases, they often share the same phone numbers.

These transactions generally begin with individuals located in the United States contacting foreign websites selling fentanyl or other prescription or illicit drugs[10] regulated under the Controlled Substances Act. The websites, which are typically registered to or operated by individuals located in China, direct users to contact a representative of the company or individual by telephone, message (e.g., video messaging, text messages, or the use of messaging applications), or email.

Once the buyer and the sales representative come to an agreement, the sales representative typically directs the buyer to send the payment to a particular person through an MSB located in the United States, online payment processor, or bank transfer (*see Figure 1*). The contact information often includes a telephone number, which may be associated with the foreign-based website and may also be used by many other foreign payment recipients or likely couriers. The payments to these foreign sources are typically low-dollar-value transactions (less than $1,000), sometimes conducted through multiple transactions or in a single transaction. In other cases, the foreign supplier may direct the individual to send a bank transfer directly to a front company operating in the chemical manufacturing field or to a shell company that is unrelated to chemicals or chemical production activity. These payments are typically higher-dollar-value transactions (over $10,000) and may be associated with bulk drug or precursor chemical purchases.[11] These companies, or their representatives, then typically mail or ship the illicit narcotics directly to the buyers in the United States for personal consumption or redistribution.[12]

---

[9] "Structuring," as the term is 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. FinCEN's regulations on structuring (*see generally* 31 CFR § 1010.100(xx) and 31 CFR § 1010.314) focus on evasion of cash transaction reporting (CTR) requirements.

[10] To include fentanyl analogues or other synthetics with no legitimate medical use.

[11] Fentanyl precursor chemicals refer to the basic or parent chemicals that form fentanyl. *See* Controlled Substances Act and the List of Controlled Substances.

[12] *See* DEA, 2018 National Drug Threat Assessment, October 2018.

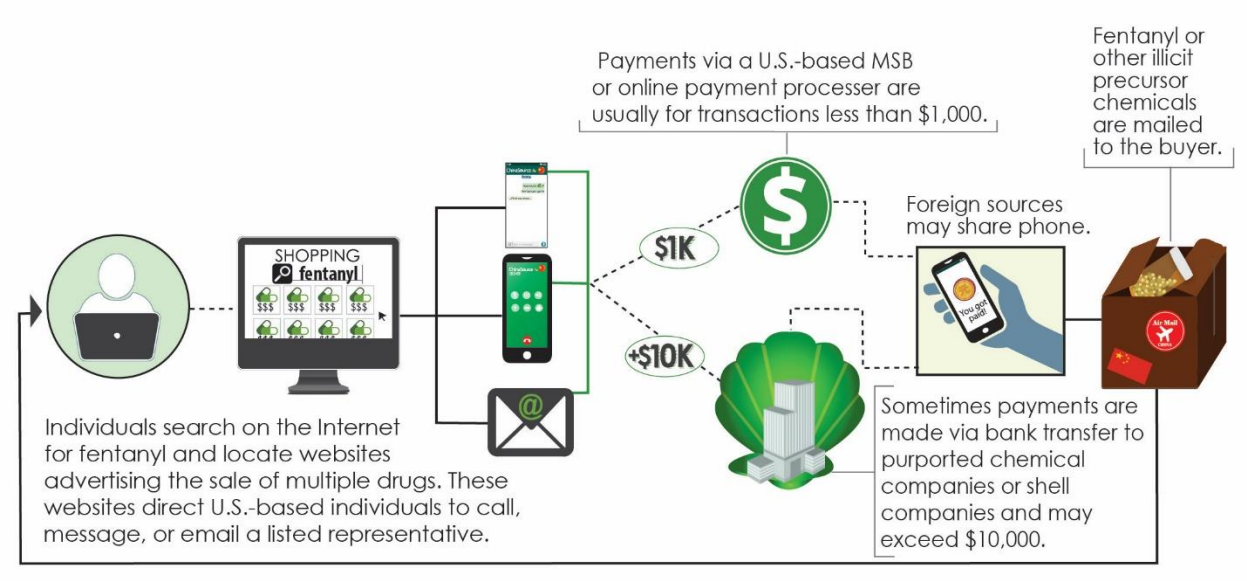

Figure 1: MSB, Online Payment Processor, or Bank Transfer to Foreign-Based Contact

Purchases from a Foreign-located Supplier Using CVC

Drug traffickers and consumers increasingly use Clearnet and Darknet[13] e-commerce markets, paired with online payment systems and virtual currencies, to further anonymize fentanyl purchase and distribution.[14] An analysis of sensitive financial data indicates that domestic illicit drug manufacturers, dealers, and consumers use online payment platforms or CVC to purchase precursor chemicals or completely synthesized narcotics primarily sourced from China.

Filing institutions have identified potential drug traffickers based on embedded messages or references on websites that mention illegal drug transactions using CVC exchangers.[15] Such messages and websites provide valuable financial intelligence on the source or destination of money and products.

[13] The Internet is typically separated into three distinct parts: (i) the open Internet, also known as the Clearnet, which encompasses sites publicly accessible through well-known and publicly advertised search engines; (ii) the Deep Web, which consists of content not indexed and sites that cannot be found by normal search functions, such as paywall-protected pages; and (iii) the Darknet, which consists of many segments, which are areas of the Internet accessible only via specialized anonymizing software, such as the The Onion Router (Tor) network. (Sites only reachable through the Tor network are recognizable through their ".onion" URL domain suffix.) While Darknet content is varied, it is also home to hidden services such as criminal marketplaces that allow individuals to buy and sell illegal items, such as drugs, firearms, and other hazardous materials, with greater anonymity than is possible on the traditional Internet. Generally, these Darknet market websites use a variety of anonymizing and encryption technologies in an attempt to shield communications and transactions from interception and monitoring.

[14] *See* DEA, 2018 National Drug Threat Assessment, October 2018.

[15] An "exchanger" is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency. *See* FIN-2019-G001, "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," May 9, 2019; and *see also* FIN-2013-G001, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," March 18, 2013.

CVC Payment to Foreign Contact Method

Similar to purchases from a foreign source of supply using MSBs or online payment processors, individuals located in the United States search for fentanyl and identify potential websites that may provide the opportunity to purchase illicit drugs online. Foreign representatives will instruct the U.S.-based individual to send payments through CVC, such as bitcoin, bitcoin cash, ethereum, or monero [16] (*see Figure 2*).

Additionally, U.S.-based individuals may find fentanyl dealers on Darknet markets and contact Darknet vendors located worldwide, including in the United States. Individuals purchasing fentanyl on the Darknet will also pay vendors using CVC. Darknet vendors and chemical companies then mail the illicit narcotics directly to the U.S.-based individuals. The Darknet vendors may eventually seek to exchange CVC for traditional fiat currency such as U.S. dollars (USD) using both U.S.- and foreign-based CVC exchangers, or sell the virtual currency themselves to the public as unlicensed money transmitters.[17] Higher-amount transactions, coupled with other suspicious indicators, are more likely to be related to a vendor, redistributor, or street dealer compared with the activity of a personal consumer.

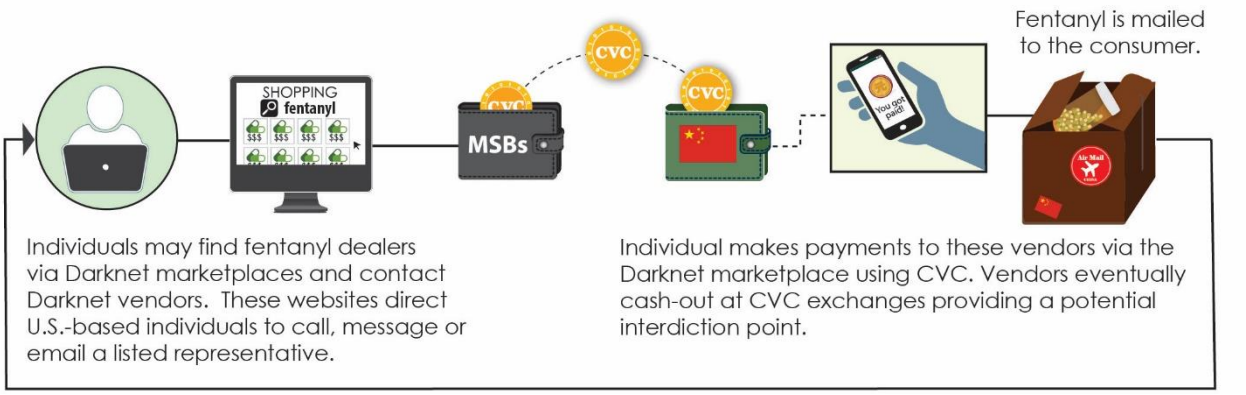

Figure 2: CVC Payment to Foreign-based Contact Method

Purchases from a U.S.-located Supplier Using an MSB, Online Payment Processor, CVC, or Person-to-Person Transaction

Individuals located in the United States use the Internet or local connections to buy fentanyl from suppliers who are also located in the United States. In this type of transaction, individuals typically make payments in one of two ways. First, payments can be made using

[16] FinCEN notes these are just examples of CVCs and that other types of CVCs may be also be used.
[17] FinCEN regulations define "money transmitter" to include a "person that provides money transmission services" or "any other person engaged in the transfer of funds." 31 CFR § 1010.100(ff)(5).

both MSBs and online payment platforms, similar to the way payments are made to foreign suppliers. After the payment is received, the supplier typically ships or mails the fentanyl to the consumer.[18] Second, in more traditional drug trafficking transactions, individuals make payments in person with cash (person-to-person transactions). In this scenario, fentanyl is hand-delivered in exchange for cash, and then the drug traffickers deposit or launder the cash. The cash transaction dollar values may vary depending on variables, such as geographic location and the amount (or weight) of the illicit narcotics that are purchased.

Cross-border Trafficking of Fentanyl by TCOs and Smaller Criminal Networks

TCO Procurement and Distribution

Mexico is a transit and production point for the trafficking of many illicit drugs and Mexican TCOs operate as the dominant purveyors of these illicit drugs, which also include fentanyl.[19] Mexican TCOs control the smuggling routes across the Southwest Border (SWB) and arrange the transport and distribution of fentanyl throughout the United States.[20]

Subsequently, Mexican TCOs arrange the consolidation, placement, and movement of illicit proceeds derived from fentanyl sales in the United States. FinCEN's review of confidential financial information reveals transactions that involve structured cash deposits, money transfers, and wire transfers for the ultimate credit of accounts in the U.S. SWB region and Mexico. FinCEN finds that this confidential financial information frequently describes individuals who conduct excessive cash transactions using ATMs, unsourced cash, and no verifiable or legitimate purpose for the transactions. Drug trafficking networks often use shell companies to disguise the illicit drug proceeds as legitimate business transactions. BSA data also shows that individuals located in the United States use their accounts to funnel funds between domestic and international locations. Some of the more common money laundering methodologies used by Mexican TCOs are described below:

1. Bulk Cash Smuggling[21]: To smuggle bulk cash across the border from the United States to Mexico, a TCO, or a third party it retains, conceals more than $10,000 in currency or other monetary instruments on a person, luggage, or in any conveyance for transportation from a place within the United States to a place in Mexico.

[18] One common thread among these transactions is the potential use of mailing and shipping systems to disseminate fentanyl. Traffickers regularly ship fentanyl and its analogues through the mail to drug dealers and users in the United States. The shippers often layer transactions and mask their identities, making it difficult for the Postal Inspection Service or Customs and Border Protection to identify which packages, among the hundreds of thousands arriving every day, contain illicit drugs.
[19] *See* DEA, 2018 National Drug Threat Assessment, p. 21, October 2018.
[20] *See* DEA, 2018 National Drug Threat Assessment, pp. 33-34, October 2018.
[21] In 2017, California, Ohio, and Arizona reported the highest dollar amounts in bulk cash seizures for a combined total of $138.8 million. This amount decreased significantly, by approximately 49 percent, in comparison to the previous year's top-three grossing states for seizures. *See* Deputy Chief of Operations Office of Global Enforcement, DEA, "Statement Before The Subcommittee on Border Security and Immigration," United States Senate, December 12, 2018.

U.S. law enforcement suspects that most bulk currency smuggled into California from other U.S. states is payment for drug shipments.[22] The majority of this illicit bulk currency is then transported across the border into Mexico through privately owned vehicles or commercial tractor-trailers.[23]

2. Trade-Based Money Laundering*:* Large amounts of bulk cash resulting from illegal drug sales, including fentanyl, can be difficult to transport across U.S. borders undetected, prompting drug traffickers to look to less conspicuous alternatives, such as trade-based money laundering (TBML) schemes. TBML often involves using illicit proceeds to buy goods for export, as the subsequent sale of the goods effectively launders the proceeds.[24] The Financial Action Task Force (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."[25] In this context, TBML often involves converting physical U.S. banknotes into a commodity and then exporting or importing the commodity, without physical cross-border movement of the underlying currency.[26] For example, drug traffickers will convert the monetary value of bulk currency (i.e., banknotes) into a good with an equivalent monetary value, such as a smartphone, automobile, or jewelry.

   To facilitate TBML, a TCO transfers funds from the United States back to international jurisdictions using either internal accountants or an independent accountant, also referred to as a "money broker." The following TBML example uses an external broker in Mexico (*see Figure 3*).[27] The TCO and broker negotiate a money pick-up and transfer a commission fee prior to the TBML operation. The TCO then informs the broker where to pick up the USD drug proceeds using an encrypted code, as a proceeds confirmation or validation means. The broker may use an assistant or hire launderers (often called "smurfs") to pick up the proceeds on the broker's behalf. Upon proceeds pick-up, the launderers may:

   i. deposit proceeds into U.S. financial institutions (often structured to avoid recordkeeping and reporting requirements) and then transfer the funds as goods or debt payments to U.S. vendors and exporters; or

[22] Deputy Chief of Operations Office of Global Enforcement, DEA, "Statement Before The Subcommittee on Border Security and Immigration," United States Senate, December 12, 2018.
[23] *Ibid.*
[24] *See* 2018 National Money Laundering Risk Assessment (2018 NMLRA).
[25] *See* FATF, Trade Based Money Laundering, p. i, June 23, 2006.
[26] *See* FinCEN Advisory, "Update on U.S. Currency Restrictions in Mexico: Funnel Accounts and TBML," FIN-2014-A005, May 28, 2014; and *see* 2018 NMLRA.
[27] There are many Black Market Peso Exchange variations, including nuances to this scenario. TBML elements and the types of players in these transactions are normally consistent. Also, while this advisory is specific to fentanyl trafficking from Mexico, the TBML methodology can also be used with many countries, to include Central/South America.

ii. transport (also called "drop" or "hand off") the bulk cash to third parties, including U.S. exporters, for subsequent deposit and integration into the U.S. financial system.

Prior to the money pick-up, the money broker negotiates a contract and exchange rate with a Mexican importer to pay for exported USD-denominated goods on the importer's behalf (i.e., a third-party payment). Once the broker receives the Mexican peso-denominated deposits from the importer, the broker's account is "loaded," and he can then facilitate the money pick-up by the launderer(s) or smurf(s) and make a simultaneous payment to the TCO to reconcile accounts. In this type of offsetting transaction, often called a "mirror transfer,"[28] the launderer picks up the money, and confirms that the broker received the proper amount (normally via text or a phone call), and the broker then transfers or "hands off" a peso-equivalent amount of USDs to the TCO. Sometimes this type of transaction commences when the Mexican importer pays the broker (thereby "loading" his account) prior to the initial money drop in the United States.

The vendor who receives USDs from the launderer will then export the goods to the Mexican importer according to the money broker's shipping directions. After receiving the goods, the importer sells them on the Mexican open market at a markup, and the importer's account is reconciled or balanced.

Figure 3

[28] *See* DEA, 2017 National Drug Threat Assessment, p. 128, October 2017.

3. Structured MSB Money Transfers: Professional money laundering organizations hire loosely associated parties (including "money mules"[29]) to send money transfers to Mexico via U.S. MSBs, primarily money transmitters, structured to evade reporting requirements. In this context, structuring (i.e., keeping the amount of the money transfer below the applicable threshold of $3,000 in order to avoid identification and reporting requirements) is accomplished through one of, or a combination of, the following:

    - The illicit proceeds are divided between multiple individuals who send the transfers;
    - An individual uses multiple MSB agent locations to send transfers; and/or
    - An individual sends multiple transactions consecutively.

4. Funnel Account Activity: Multiple individuals acting on behalf of the TCO deposit cash proceeds of illicit drug sales into a personal or business account. The deposits are often made in multiple states geographically distant from the branch in which the account was opened or domiciled and geographically different from the location of the withdrawal activity.[30] The deposits are structured (i.e., kept below the applicable threshold of $10,000, in this instance, to avoid identification and recordkeeping requirements).[31] The use of funnel account activity by TCOs may have been partially disrupted by the decisions of certain large national banks to restrict third-party cash deposits for private customer accounts.

Case Studies of Fentanyl-related Illicit Finance

Example of Funnel Accounts Funding Wires to Mexico Disguised as Legitimate Business
Financial Institution Type: Depository Institutions

In December 2018, a federal jury convicted Herman E. Aguirre and Troy R. Gillon of narcotics conspiracy. Aguirre was also convicted of operating a continuing criminal enterprise and money laundering conspiracy.[32] In 2016, these two individuals were indicted along with 15 co-conspirators for their role in a criminal network of individuals and food and produce companies affiliated with the Sinaloa Cartel trafficking in thousands of kilograms of heroin, fentanyl, and cocaine from Mexico into the United States by disguising the shipments in pallets described

[29] The Federal Bureau of Investigation (FBI) defines "money mule" as "someone who transfers illegally acquired money on behalf of or at the direction of another." FBI, Money Mule Awareness Booklet, p. 2, December, 2018.
[30] *See* FinCEN Advisory, "Update on U.S. Currency Restrictions in Mexico: Funnel Accounts and TBML", FIN-2014-A005, (May 2014).
[31] *Ibid.*
[32] Department of Justice, U.S. Attorney's Office, Western District of New York, "Federal Jury Convicts Two Defendants of Narcotics Conspiracy Tied To The El Chapo Mexican Drug Cartel," December 20, 2018.

as containing "sea cucumbers."[33] The TCO's operation spanned Mexico, Arizona, California, and elsewhere, with the Sinaloa Cartel, led by Joaquín "El Chapo" Guzmán and Ismael "El Mayo" Zambada, as its source of supply.[34] The TCO opened accounts in banks in southern California, which were used to receive cash deposits at drug sale locations in Northeastern cities.[35]

Darknet and Clearnet Marketplace Fentanyl Transactions
Financial Institution Type: MSBs and Depository Institutions

Matthew and Holly Roberts were sentenced to 135 and 96 months in federal prison, respectively, for their roles in distributing fentanyl and other narcotics through multiple Darknet marketplace[36] accounts.[37] At the time of their arrest in 2018, the couple were the most prolific Darknet fentanyl vendors in the world. They used "private messaging, encryption software, Virtual Private Networks and proxies through the Tor network" as well as pre-paid Visa and gift cards, and mailed decoy items, such as glow bracelets, to hide the fact they were mailing narcotics.[38]

Their customers made purchases with virtual currency, which the couple then sent to virtual currency exchangers to convert the funds into U.S. fiat currency.[39]

Note: Based on analysis of sensitive financial data, Holly Roberts added funds to stored value cards and immediately removed funds via ATM withdrawals and online purchases. Matthew Roberts and associates received excessive cash deposits into their accounts from sources outside of the account's geographic area followed immediately by cash withdrawals.

Kingpin Act Sanctions – *Chinese Synthetic Opioid Traffickers*

Through sanctions investigations into Chinese nationals involved in synthetic opioid trafficking, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) designated Chinese national Jian Zhang as a significant foreign narcotics trafficker, the first fentanyl-related designation pursuant to the Foreign Narcotics Kingpin Designation Act

[33] Western District of New York, "17 Defendants Indicted in International Drug Trafficking Ring," August 9, 2016.
[34] Department of Justice, U.S. Attorney's Office, Western District of New York, "Federal Jury Convicts Two Defendants of Narcotics Conspiracy Tied To The El Chapo Mexican Drug Cartel," December 20, 2018.
[35] Western District of New York, "17 Defendants Indicted in International Drug Trafficking Ring," August 9, 2016.
[36] Dream Market, Silk Road, AlphaBay, Darknet Heroes League, Nucleus, and several others.
[37] Department of Justice, U.S. Attorney's Office, Northern District of Ohio, "Texas couple sentenced to prison; they were the most prolific dark net fentanyl vendor in the world at the time of their arrest last year," February 7, 2019. Department of Justice, U.S. Attorney's Office, Northern District of Ohio, "Texas couple who had thousands of online sales of fentanyl and other drugs pleaded guilty to drug crimes," October 23, 2018. Department of Justice, Office of Public Affairs, "Operation Darkness Falls Results in Arrest of One of the Most Prolific Dark Net Fentanyl Vendors in the World," August 22, 2018.
[38] Department of Justice, U.S. Attorney's Office, Northern District of Ohio, "Texas couple sentenced to prison; they were the most prolific dark net fentanyl vendor in the world at the time of their arrest last year," February 7, 2019.
[39] Department of Justice, Office of Public Affairs, "Operation Darkness Falls Results in Arrest of One of the Most Prolific Dark Net Fentanyl Vendors in the World," August 22, 2018.

(Kingpin Act).[40] Zhang's trafficking of fentanyl and other controlled substances to the United States was tied to the overdose deaths of U.S. citizens. In addition to Zhang, OFAC designated a chemical company named Zaron Bio-Tech (Asia) Limited, a Hong Kong entity operating in Shanghai, China, that was owned and controlled by Zhang. Zhang used Zaron Bio-Tech to facilitate the unlawful importation of fentanyl and other controlled substances into the United States. OFAC also designated four individuals, including Zhang's mother and father, who assisted his narcotics trafficking activities by using global MSBs to receive funds for fentanyl purchases from individuals located in the United States.[41]

In 2014, OFAC sanctioned two Chinese nationals, Bo Peng and Zhang Lei, as specially designated narcotics traffickers pursuant to the Kingpin Act,[42] as well as two Chinese companies, CEC Limited and Kaikai Technology Co., Ltd., for their role in international drug trafficking relating to synthetic opioids, cannabinoids, and cathinones. OFAC also designated three additional Chinese nationals for their role on behalf of Zhang Lei.[43]

Darknet Fentanyl Purchases

The Darknet is commonly used for a number of illicit activities, including fentanyl trafficking. In July 2017, the U.S. Department of Justice seized AlphaBay servers and assets; AlphaBay was the largest criminal Darknet market on the Internet at the time.[44] AlphaBay required its users to transact in CVC (including bitcoin, monero, and ethereum) to obfuscate transactions and related parties. The Darknet site was a major platform for transactions involving fentanyl and heroin, which were linked to overdose deaths. AlphaBay operated for over two years on the Darknet, and hundreds of thousands of people around the world used the site to buy and sell deadly and illegal drugs, stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms, and toxic chemicals. U.S. officials estimate, based on the law enforcement investigation, that AlphaBay was used to launder hundreds of millions of dollars linked to its illegal transactions.[45]

Red Flag Indicators for Fentanyl-related Activity

The red flags noted below may help financial institutions in identifying suspected schemes related to illicit fentanyl trafficking. Some red flags listed may also be applicable more generally to drug trafficking, or apply to other trafficked drugs, or to other money laundering or illicit activity, but are detailed in order to provide context for financial activity related to fentanyl. In applying the red flags, financial institutions are advised that no single transactional red flag necessarily indicates suspicious activity conclusively. Financial

[40] *See* Treasury Press Release: "Treasury Sanctions Chinese Fentanyl Trafficker Jian Zhang," April 27, 2018.
[41] *Ibid.*
[42] *See* Treasury Press Release: "Treasury Sanctions Prolific Chinese Synthetic Drug Traffickers," April 27, 2018.
[43] *See* Treasury Press Release: "Treasury Sanctions Members of a Chinese Synthetic Drug Trafficking Organization," July 29, 2014.
[44] U.S. Department of Justice, "AlphaBay, Largest Online Dark Market, Shut Down," July 20, 2017.
[45] *Ibid.*

institutions may consider additional contextual information and the surrounding facts and circumstances, such as a customer's historical financial activity and whether the customer exhibits multiple indicators, before determining that a transaction is suspicious. Financial institutions may also perform additional inquiries and investigations where appropriate.

MSBs: Money Transfer Red Flags

1. The money transfer beneficiary lists a phone number or email address associated with a pharmaceutical company or chemical sales website.

2. U.S. remitter sends low-dollar money transfers to an individual in China for no apparent legitimate purpose. Individual transfers may range from $10 to $100, with an aggregated amount of multiple transfers totaling approximately $600. Conversely, a U.S. remitter sends a high volume of money transfers to apparently unrelated individuals.

3. Multiple U.S. remitters send money transfers to the same individual beneficiary in China (i.e., many to one).

4. Seemingly unrelated beneficiaries share the same phone number or email address to receive transactions.

5. The volume of outgoing money transfers is not consistent with the expected activity of a U.S. remitter.

6. A U.S. remitter adjusts the money transfer amount to avoid BSA reporting and recordkeeping requirements (i.e., structuring). When a U.S. remitter sends multiple structured money transfers, additional red flags may be involved:

    - Remitter uses multiple agent locations.
    - Remitter sends money transfers to the same beneficiary consecutively, instead of aggregated in a single sum.
    - Two or more seemingly unrelated remitters are linked together by shared attributes such as common addresses or profile information. These remitters then coordinate transactions to evade the recordkeeping threshold.

Depository Institutions: Structuring and Funnel Account Activity Red Flags

7. Account owners or third parties structure cash deposits at bank branches nationwide into the same account, which funds outgoing transactions on the SWB, including cash withdrawals or wire transfers to Mexico (i.e., funnel account activity and rapid movement of funds).

8. The depository institutions have a suspicion concerning the physical condition of deposited banknotes (e.g., the bills smell of drugs, detergent, or are excessively worn).

9. The source of funds cannot be corroborated.

10. Multiple transactions below the applicable Currency Transaction Report (CTR) threshold (i.e., structuring), which may involve additional indicators:

    - Suspicious use of multiple locations.
    - Two or more individuals working together.
    - Suspicious use of multiple accounts.

11. Transaction out of pattern for customers or business type.

12. Transaction with no apparent business purpose.

Depository Institutions: Shell Company Red Flags

13. Unclear business model:

    - The company's North American Industry Classification System (NAICS) code(s) is/are in a different industry than the business name indicates.
    - Commercial databases reveal the company is associated with multiple businesses in unrelated industries.
    - Open source information reveals that the company lacks or has vague company websites.

14. Company address or location discrepancy:

    - Online or other open source searches on the address provided reveal a business with a different name, or an operating location inconsistent with the business model, such as a residence.
    - Commercial databases associate the company with multiple active addresses or operating locations, but reveal few, if any, indications the company has franchises or multiple branches, subsidiaries, or agents.

15. Company name discrepancy:

    - The company's name is vague, non-descriptive, or does not align with its business model.

- Commercial databases reveal the company has three or more name variations or has multiple "doing business as" (dba) names.

16. Employer Identification Number (EIN) discrepancy:

- Commercial databases reveal the company is a small business with fewer than 500 employees but has multiple EINs or shares EINs with other businesses.

Depository Institutions and MSBs: Clearnet and Darknet Marketplace Fentanyl Purchase Red Flags

17. Direct or indirect transactions with Darknet marketplaces or CVC mixing services.[46] The names of several current popular Darknet marketplaces include[47]:
18. Empire
    - Tochka/Point
    - Valhalla
    - Rapture
    - Berlusconi

19. Customers with past criminal histories for drug-related offenses.

20. Customers discussing drug purchases in the transaction notes field available on the exchange, including referencing drugs or weight measurements like grams (e.g., "1 gram fent"). Customers may reference the informal slang names[48] (e.g., "Fenty") or the actual chemical names (e.g., "Acetylfentanyl").

21. Use of virtual private network (VPN) services or Tor to access CVC exchange accounts.

Valuable Information in Reporting Suspicious Activity

Suspicious Activity Involving Websites and Embedded Messages

Online payment systems or CVC exchangers may have access to embedded messages or other information that reference Internet purchases of illegal drugs. This information can be

[46] Tumbling or mixing involves the use of mechanisms to break the connection between an address sending CVC and the addresses receiving CVC.
[47] See the Red Flag section of the "Marketing Advisory," which is a part of a larger, United States government Fentanyl advisory covering the movement, manufacturing, marketing, and monetary aspects of the trafficking of fentanyl and other synthetic opioids. A summary of the *21st Century Drug Trafficking: Advisories on Fentanyl and Other Synthetic Opioids*, which includes links to each advisory, can be found here: https://www.whitehouse.gov/wp-content/uploads/2019/08/Fentanyl-Advisory-Marketing-Tab-B.pdf
[48] *See* DEA Intelligence Report on Drug Slang Code Words.

extremely useful for financial institutions in determining suspicious activity linked to potential drug trafficking and to law enforcement for investigative purposes.

Suspicious Activity Involving CVC

CVC transactions generate a significant variety of information elements that may be extremely useful to law enforcement in investigating potential illicit conduct involving CVC transactions. Specifically, the following information is particularly helpful to law enforcement:

- virtual currency wallet addresses
- account information
- transaction details (including virtual currency transaction hash)
- relevant transaction history
- available login information (including IP addresses)
- mobile device information (such as device International Mobile Equipment Identity (IMEI))
- information obtained from analysis of the customer's public, online profile and communications

When filing a Suspicious Activity Report (SAR), financial institutions should provide all pertinent available information in the SAR form and narrative.

Reminder of Regulatory Obligations for U.S. Financial Institutions

Consistent with existing regulatory obligations, U.S. financial institutions should take reasonable, risk-based steps to identify and limit any exposure they may have to funds and other assets associated with individuals and entities engaged in the financial facilitation or trafficking in fentanyl or other synthetic opioids.

Reminder of Anti-Money Laundering (AML) and Regulatory Obligations for U.S. Financial Institutions Regarding Due Diligence, Customer Identification, and Suspicious Activity Reporting

FinCEN is providing the information in this advisory to assist U.S. financial institutions in meeting their risk-based due diligence and other BSA obligations to help identify individuals who may be engaged in the financial facilitation or trafficking in fentanyl or other synthetic opioids.

Enhanced Due Diligence Obligations

FinCEN reminds U.S. financial institutions that they must comply with their due diligence obligations under the BSA and its implementing regulations.[49] In addition to their general due diligence requirements, covered financial institutions are required to implement a due diligence program for private banking accounts held for non-U.S. persons designed to detect and report any known or suspected money laundering or other suspicious activity through those accounts.[50]

FinCEN also reminds covered financial institutions of their obligation to implement due diligence programs for correspondent accounts they maintain for foreign financial institutions that include appropriate, specific, risk-based and, where necessary, enhanced policies, procedures, and controls reasonably designed to detect and report known or suspected money laundering activity involving such accounts.[51]

Customer Identification

[49] *See* 31 U.S.C § 5318(h) and 31 CFR § 1010.210 for AML program requirements, and as applied to specific financial institutions in 31 CFR §§ 1020.210, 1021.210, 1022.210, 1023.210, 1024.210, 1025.210, 1026.210, 1027.210, 1028.210, 1029.210, and 1030.210.
[50] *See* USA PATRIOT Act § 312, codified at 31 U.S.C. § 5318(i) and 31 CFR § 1010.620(a). The definition of "covered financial institution" is found in 31 CFR § 1010.605(e). The definition of "private banking account" is found in 31 CFR § 1010.605(m). The definition for the term "non-U.S. person" is found in 31 CFR § 1010.605(h).
[51] *See* USA PATRIOT Act § 312 (31 U.S.C.§ 5318(i)); 31 CFR §1010.610(a).

In addition, certain financial institutions also must have a written customer identification program,[52] to allow the institution to form a reasonable belief that it knows the true identity of each of its customers. At a minimum, these financial institutions must, at account opening, obtain and verify each customer's name, date of birth for individuals listed on the account, address, and identification number.[53]

An MSB's AML program must establish adequate and appropriate procedures and controls commensurate with the money laundering and terrorist financing risks posed by foreign agents or counterparties with which that MSB does business.[54]

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, 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.[55]

SAR Filing Instructions

When filing a SAR, financial institutions should provide all pertinent available information in the SAR form and narrative. FinCEN requests that financial institutions use only the updated mandatory SAR form (as of February 1, 2019) and reference this advisory using the following key term in SAR field 2 (Filing Institution Note to FinCEN): "FENTANYL FIN-2019-A006"

to indicate a possible connection between the suspicious activities being reported and activities highlighted in this advisory.

SAR reporting, in conjunction with effective implementation of due diligence requirements and OFAC obligations by financial institutions, has been crucial to identifying proliferation financing as well as money laundering and terrorist financing. SAR reporting is consistently beneficial and critical to FinCEN and U.S. law enforcement analytical and investigative efforts, OFAC designation efforts, and the overall security and stability of the U.S. financial system.[56]

For Further Information

Additional questions or comments regarding the contents of this advisory should be addressed to the FinCEN Resource Center at FRC@fincen.gov.

[52] *See* 31 CFR §§ 1020.220, 1023.220, 1024.220, and 1026.220.
[53] *See, e.g.*, 31 CFR § 1020.220.
[54] *See* FinCEN Interpretive Release 2004-1, 69 FR 239, December 14, 2004.
[55] *See* 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320.
[56] For Law Enforcement Case Examples, *see* SAR Activity Review, Issue 19, beginning on p. 19.

Financial institutions wanting to report suspicious transactions that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).

The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

###

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