Cryptocurrency Anti-Money Laundering Report

2018 Q2

CIPHERTRACE 2018 Q2 CRYPTOCURRENCY ANTI-MONEY LAUNDERING REPORT

CIPHERTRACE 2018 Q2 CRYPTOCURRENCY ANTI-MONEY LAUNDERING REPORT

Cryptocurrency AML Regulation Grows Globally in Response to Increasing Exchange Theft, Crypto Used in Crimes, and a Related Rise in Money Laundering

The phenomenal growth in the value of cryptocurrencies like Bitcoin over recent years has attracted investors, speculators, and thieves. In the last two years alone, some of the best and brightest criminal minds made off with $1.2[1] billion in cryptocurrency from exchanges. The first half of 2018 experienced a three-fold increase over the entire year of 2017. In addition, the FBI has reported an almost six-fold increase in the value of virtual currency in complaints from 2015 to 2017.

All of these illegally obtained funds are laundered by criminals to help hide their true identities and avoid arrest. In addition to these criminal actors, we have seen an increase in terrorist financing and nation state actors as well as a continued use of cryptocurrencies, especially bitcoin, for payment of drugs (including Fentanyl[2]) and weapons.

Criminals are often early adopters of new technologies. So not surprisingly Bitcoin and other virtual currencies attracted their interest because of several unique properties. Crypto transactions do not require criminals to use their real names, bank account numbers, etc., which can enable them to evade the watchful eye of law enforcement and other investigators. Instead, they can use pseudonyms; and transferring crypto funds does not require banks for other financial intermediaries—e.g., PayPal. Moreover, unlike robbing a bank, thieves can raid cryptocurrency exchanges with little fear of being caught.

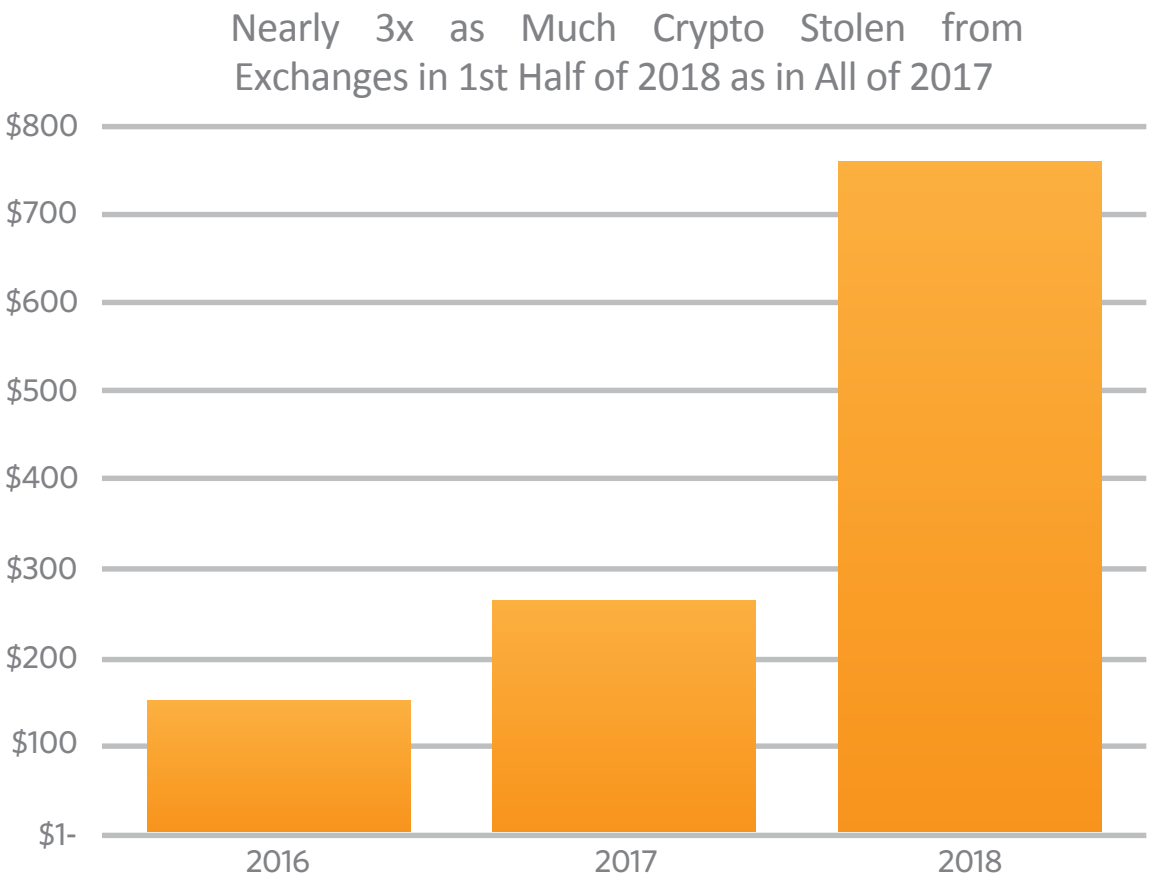
The resulting rapid growth in the theft of virtual currencies and their use for illicit purposes has also attracted the attention of regulators. Government agencies around the world are concerned not only about the impact that theft and extortion has on individuals and business but also how it drives an increase in money laundering. This is because once cryptocurrency is stolen from an exchange, received as ransom or acquired through other illegal activity, the cybercriminals need to get it into Blockchain system, somehow cleanse it, and then get it out for their use in the real world.

Key takeaways

1. In Q1and Q2 of 2018, nearly three times as much cryptocurrency was stolen as in all of 2017
2. Cyber extortionists, dark markets and ransomware perpetrators prefer bitcoin
3. Crypto money laundering is enabled by mixers, chain hopping and privacy coins
4. US FinCEN will enforce Anti-Money Laundering (AML) regulations globally
5. AML regulation and international cooperation is a FATF priority

Stolen Cryptocurrencies That Must Be Laundered

The first half of 2018 has seen nearly three times as much cryptocurrency stolen as in all of 2017. These funds needed to be laundered by the criminals in order to prevent their identities from being determined by law enforcement agencies.



Regulators Focus on Anti-Money Laundering Globally

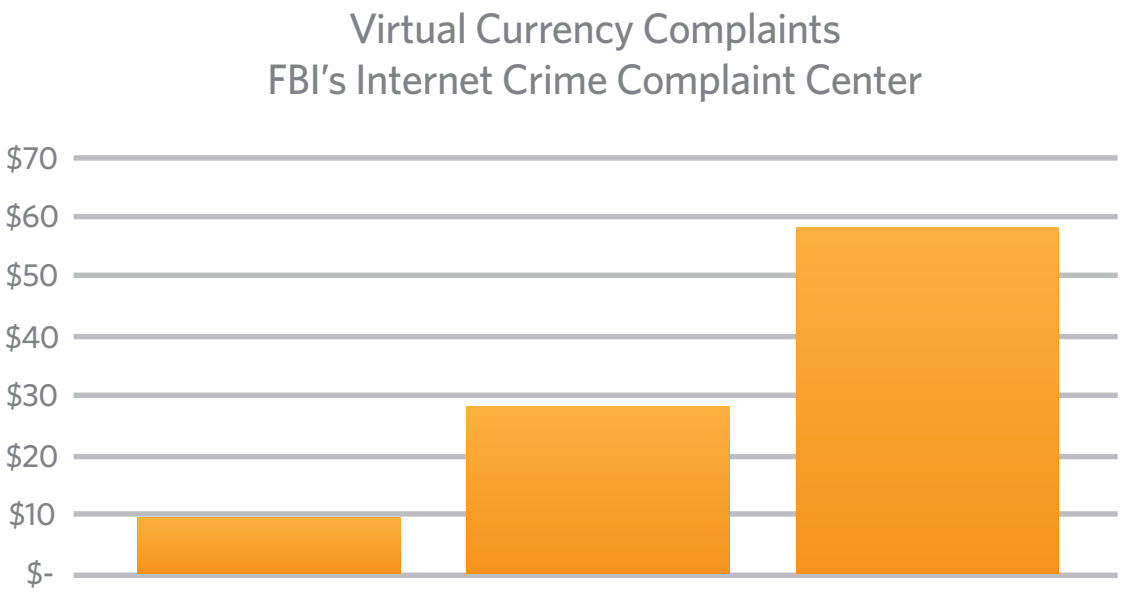
The Financial Crimes Enforcement Network (FinCEN) recently shared a similar concern. After citing cryptocurrency-denominated ransomware payments and $1.5 billion stolen in exchange hacks over a two-year period, Thomas Ott, Associate Director of the Department of the Treasury's bureau noted: "We have seen virtual currency exploited to support billions of dollars in what we would consider suspicious activity."

The U.S. Secret Service is also taking a hard look at privacy cryptocurrencies/coins like Monero and Zcash for their use for illicit purposes, while urging Congress to "consider additional legislative or regulatory actions." On June 20, 2018, the Secret Service announced it had "seized over $28 million in cryptocurrencies in the course of our criminal investigations, 12 primarily in the form of Bitcoin FY 2015 to present." The Deputy Assistant Director's testimony before Congress went on "It is critical that the

United States continues to work internationally to improve controls related to digital currency through organizations like the Financial Action Task Force. We should also consider additional legislative or regulatory actions to address potential challenges related to anonymity-enhanced cryptocurrencies, services intended to obscure transactions on blockchains (i.e., cryptocurrency tumblers or mixers) and cryptocurrency mining pools."[3]

The main branches of government are also actively considering new regulations. During a recent congressional hearing, representative Robert Pittenger of North Carolina called the illicit use of privacy coins and cryptocurrencies "One of the greatest emerging threats to U.S. national security."

The FBI noted that the value of virtual currencies contained in the Internet Crime Center 2017 reports were $58.3M,[4] citing cyber actor demands the of ransom payments, typically in virtual currency such as Bitcoin. They also noted "virtual currency is commonly demanded as the payment mechanism because it provides the criminal an additional layer of anonymity when perpetrating these schemes."

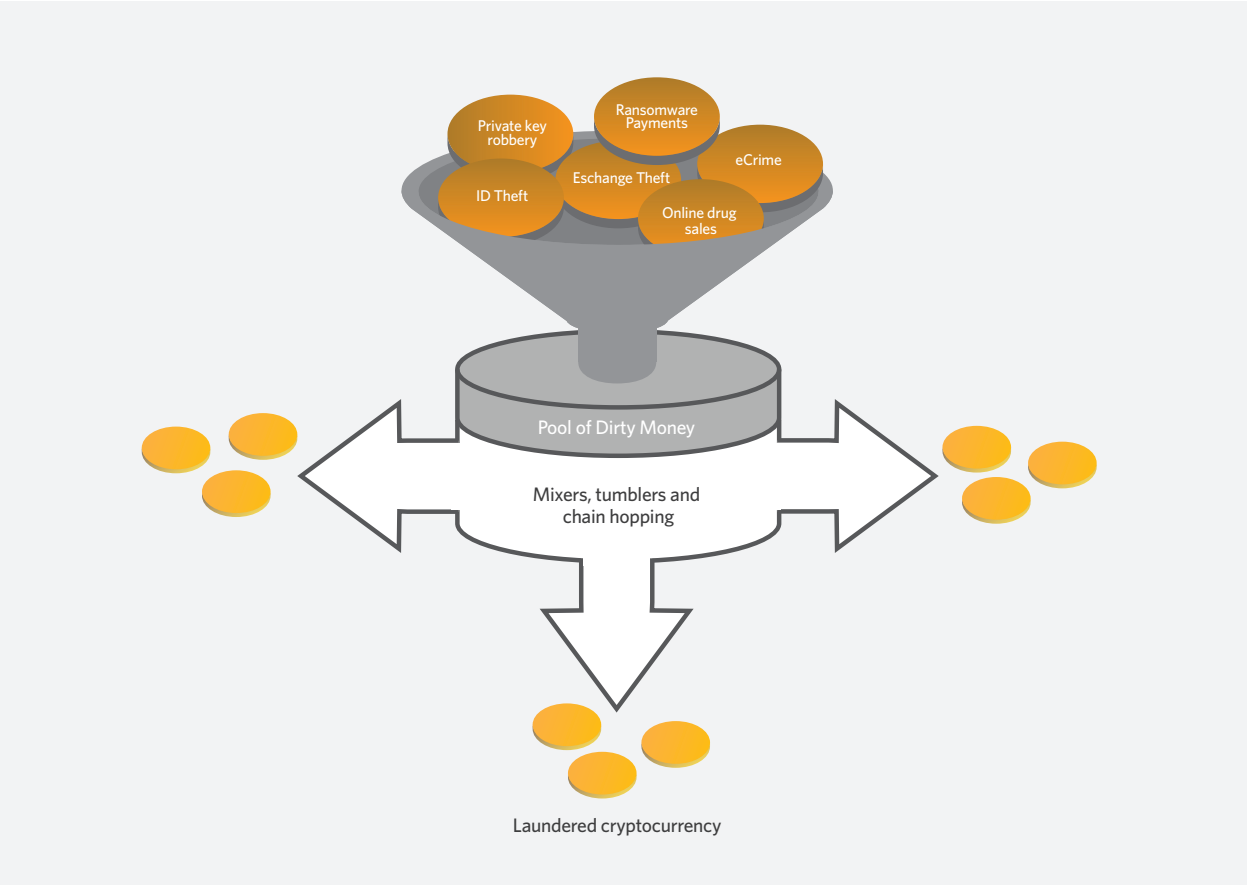


How Does Cryptocurrency Money Laundering Work?

Hiding the illicit origins of these funds, aka 'money laundering,' has also kept pace with the times. The age of crypto is far different from the days of Al Capone, who allegedly purchased 'Laundromats' to mix dirty money with legitimate business proceeds, and thereby obscure his organization's illegal profits derived from prostitution and bootleg booze.

The growing theft of cryptocurrencies and their increasing use by terrorists, extortionists, identity thieves, drug dealers, weapons dealers and human traffickers has ushered in a

new era of high-tech virtual money laundering. However, unlike cash, getting this dirty crypto money clean is a little more complicated.



The first step in the cleansing process is called Layering. In the traditional money laundering world, this would involve purchasing expensive items like gold bars, cars, jewelry or real estate, and then reselling them. In the virtual world, it involves moving money into the cryptocurrency system and moving it around by using mixers, tumblers and chain hopping. The more dirty crypto money that goes into the systems and the more it moves around, the harder it becomes for investigators to see through the web of action and trace a path back to the source. Additionally, the pseudo-anonymous nature of virtual currencies makes it exponentially more difficult to trace these funds as compared to cash. As one caveat, criminals will lose a percentage off the top to move the funds, but in the end the funds appear legitimate, making the loss worthwhile.

The next step toward clean money is Integration. After placing the funds in the cryptocurrency system and moving them around in a kind of virtual shell game, the criminals are closer to enjoying unencumbered and relatively safe use of their ill-gotten gains. There are still risks to integrating the funds into the mainstream financial system because exchanges and other parties involved in cryptocurrency transactions monitor

activity and may issue Suspicious Activity Reports (SARs), which flag high-risk transactions. However, once legitimized, the criminals have multiple options for recouping the funds from the financial system.

Money Laundering Mixers, Tumblers, and Foggers

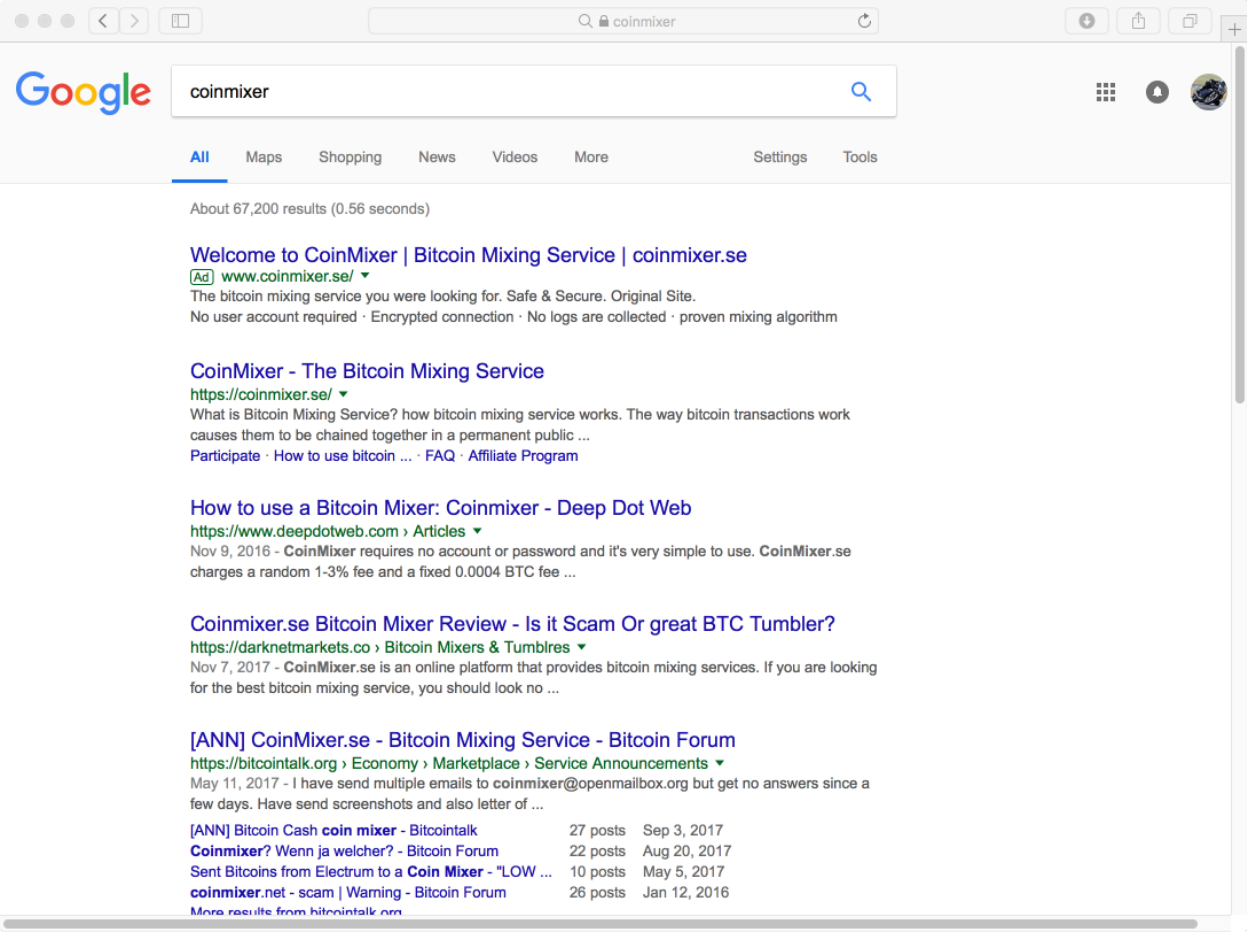
There are a number of money laundering services available for cryptocurrencies. These services are variously called mixers, tumblers, foggers and laundries. They take in funds from multiple customers, mix those funds together, and then output the mixed funds. The purpose of these money laundering services is to obfuscate the origin and receipt of cryptocurrencies. They typically charge between 1% and 3% per transaction for their services.

Well-known cryptocurrency money laundering services

- BestMixer.io
- Bitblender
- Bitcloak
- BitcoinFog
- BitLaunder
- BitMix.Biz
- Bitmixer
- Chipmixer.com
- Coinmixer
- cryptomixer.io
- DarkLaunder
- Helix
- Helix2
- Helixlight
- HelixMixer
- Outlawtumbler
- Penguinmixer
- PrivCoin.io

Some of these services have stopped servicing clients in the wake of regulatory enforcement. In July 2017, for instance, Bitmixer.io terminated its service.

We are seeing these money laundering services beginning to take advantage of large-scale advertising platforms for acquiring new customers. The example below is an advertisement on Google AdWords for Coinmixer, a Sweden-based cryptocurrency money laundering service.



Cryptocurrency money laundering services are now trying to disassociate input funds for mixing versus the output funds that are sent to the criminal who wishes to receive these laundered funds. This is done through having large pools of liquidity (i.e., holding millions of dollars' worth of Bitcoin or other cryptocurrencies), and keeping these pools separated. In 2016 and 2017, these funds were combined together, and the mixers relied on timing and value combination scrambling to hide the flow of funds from senders and receivers.

In late 2017 and in 2018, we began seeing these services paying particular attention to disassociating input pools and output pools of coins. They are doing this through collecting input funds into large pools, and then depositing these funds into exchanges. Then they move the funds between exchanges, and finally bring them out to an output pool. This approach not only reduces the transaction cost of moving the funds but also creates two or more international barriers for obfuscating the input and output funds at the exchange level.

Gambling Services as Money Laundering Facilities

Cryptocurrency gambling sites are also frequently used as money laundering facilities. There are between 100 and 200 gambling sites on the Internet that focus on cryptocurrencies. Criminals can establish accounts on these sites and then transfer funds

for laundering to them. They will make simple bets, or even in some cases simply withdraw funds to a new address without any bets at all. This helps to create a break in the funds flow trace that acts in many ways like a currency mixer.

Because these gambling sites have little to no "Know Your Customer" (KYC) regulation, it is difficult for law enforcement to obtain information about the funds transfers into and out of these services.

An example list of cryptocurrency gambling sites is available on https://gamblingbitcoin.com[5]

Are Crypto-to-Crypto Services Subject to Anti-Money Laundering Controls?

On June 21, 2018, CipherTrace attended and presented at the 5th Annual Europol Virtual Currency Conference[6], which was held at the Hague in the Netherlands. This conference attracted more than 300 attendees from law enforcement, regulatory agencies, cryptocurrency exchanges, and Anti-Money Laundering (AML) solution vendors. FinCEN's Jamal El-Hindi reiterated their statement: "We will hold accountable foreign-located money transmitters, including virtual currency exchangers, that do business in the United States when they willfully violate U.S. AML laws."[7]

> **"We will hold accountable foreign-located money transmitters, including virtual currency exchangers, that do business in the United States when they willfully violate U.S. AML laws."**
> FinCEN

Kevin O'Connor of FinCEN also stated that crypto-to-crypto exchanges were subject to AML controls because crypto assets are representative of fiat currency and assets. Furthermore, when questioned about the responsibility of offshore cryptocurrency exchanges and cross-currency swap engines such as Shapeshift.io, his response was that if they deal with US customers, they are beholden to US Anti-Money Laundering requirements.

OFAC Compliance for Cryptocurrencies

The Office of Foreign Assets Control (OFAC) publishes a list of individuals, companies, addresses, bank accounts and countries with which US companies are not permitted to do business. OFAC is going to add cryptocurrency addresses to this list. FinCEN has stated that exchanges must know their counterparties, which countries they are in, and if they are on the OFAC black list[8]. This opens up a large set of questions, best practices and technology requirements for identifying counterparties of cryptocurrency transactions.

Sophisticated Technology and Education Is Needed to Uncover High-Tech Money Laundering

Using cryptocurrencies makes it more convenient to launder money on a global basis compared with using traditional financial payment mechanisms. It happens online without the need to buy gold bars, sell a yacht, or fly to Miami with cash to buy a house. It also makes it harder for law enforcement, regulators and compliance departments at exchanges to find illicit transactions and track their origins and destinations.

In the days of Al Capone, for example, an FBI agent might have been able to camp out in a building across the street from a laundromat and watch cash handoffs through binoculars. But tracking funds through the Blockchain system requires the most advanced computer science and cybercrime knowhow. Which is why there is currently huge and growing demand for technology tools and expertise capable of "de-anonymizing" Blockchain transactions in order to uncover money laundering activity using Bitcoin, privacy coins, and other virtual currencies.

Timeline of Cryptocurrency Money Laundering and Criminal Prosecutions[9]

Jul-17	Aug-17	Sep-17	Oct-17	Nov-17	Dec-17
BTC-E fined $110m in Greece for supporting ransomware payments.	Dutch Police take over and operate Hansa dark market for a month before taking it down.	SEC files first ICO fraud case : Recoin.	Abu Dhabi regulates ICOs for cryptocurrency funding.	3.2 raised in Q4 by ICOs	SEC Takes Enforcement Action against Utility Token ICO Munchee.
AlphaBay darkmarket takedown shuts 40,000 vendors and blocks $1B in trade. Bitcoin mixing service BitMixer shuts down.		China bans ICOs			PlexCoin 15m fraud

Jan-18	Feb-18	Mar-18	Apr-18	May-18	Jun-18
SEC subpoenaes 80 cryptocurrency companies.	Japan's FSA punished nine exchanges after the Coincheck theft for lack of AML controls.	SEC requires cryptocurrencies "exchanges," as defined by the federal securities, to be registered.	Criminal and civil charges against two Centra Tech co-founders.	Australian Bank gets record ML fine.	SEC says Ether not a security.
South Korea Bans Anonymous trading.		Presidential order bans Petro, Venezuela's cryptocurrency.		Cryptocurrency Debit Card Startup Founders Indicted for $25m fraud.	FATF disscuss binding AML rules and puts Pakistan on the Grey List.

Cryptocurrency and Related AML Regulation by Country

Country	Regulations
Australia	Liberal
Bangladesh	Banned
Bermuda	Drafted
Boliva	Banned
Canada	Drafted
China	Banned
Ecuador	Banned
EU	In Progress
Gibraltar	ICO /AML regulations
Hong Kong	Warning
India	Banning
Israel	Delayed
Japan	In Place
Korea	In Place
Kyrgyzstan	Banned
Malaysia	KYC/AML
Malta	In place
Morocco	Banned
Nepal	Banned
Russia	In place /AML
Sweden	In place /AML
Switzerland	In place /AML
Taiwan	No ATMS
Thailand	Prohibitions
UAE	In Progress
UK	AML for exchanges
USA	In Progress

About CipherTrace

CipherTrace develops blockchain security, AML compliance and enforcement solutions that make cryptocurrencies, crypto tokens and enterprise private blockchains safe and secure. Founded in 2015 in Menlo Park, California, by experienced Silicon Valley entrepreneurs, CipherTrace operates globally. The CipherTrace team includes world-leading cryptocurrency security executives and programmers with deep expertise in cyber security, payment systems, and Bitcoin mining. Many members of the team were also early participants in the Bitcoin community. The company was originally funded by the Department of Homeland Security Science and Technology and DARPA to develop their respective cryptocurrency tracing capabilities, and now enjoys the backing of leading Silicon Valley venture capital investors.

About the CipherTrace Cryptocurrency Anti-Money Laundering Report

This is the inaugural CipherTrace Cryptocurrency Anti-Money Laundering Report. It will be published quarterly. We hope that it has been useful and informative. Please sent comments, corrections and ideas for future study to contact@ciphertrace.com.

---

[1] https://www.reuters.com/article/us-crypto-currency-crime/about-1-2-billion-in-cryptocurrency-stolen-since-2017-cybercrime-group-idUSKCN1IP2LU

[2] With Google, Bitcoins, and USPS, Feds realize it's stupid easy to buy fentanyl
Simple search led investigators to sales of $766 million worth of fentanyl. https://arstechnica.com/tech-policy/2018/01/feds-crack-illegal-drug-shipments-from-china-by-googling-fentanyl-for-sale/
Deadly Chinese Fentanyl Is Creating a New Era of Drug Kingpins
https://www.bloomberg.com/news/features/2018-05-22/deadly-chinese-fentanyl-is-creating-a-new-era-of-drug-kingpins

[3] https://democrats-financialservices.house.gov/uploadedfiles/06.20.2018_robert_novy_testimony.pdf

[4] https://pdf.ic3.gov/2017_IC3Report.pdf

[5] https://gamblingbitcoin.com/

[6] https://www.europol.europa.eu/newsroom/news/cryptocurrency-meets-law-enforcement-europol's-5th-virtual-currencies-conference

[7] https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware

[8] https://www.coindesk.com/goodbye-fungibility-ofacs-bitcoin-blacklist-remake-crypto/

[9] https://www.jdsupra.com/legalnews/sec-gets-tough-on-icos-files-first-62106/
https://www.darkreading.com/threat-intelligence/dark-web-marketplaces-dissolve-post-alphabay-hansa-takedown/d/d-id/1331971
https://www.jdsupra.com/legalnews/sec-gets-tough-on-icos-files-first-62106/
https://www.cnbc.com/2017/10/09/abu-dhabi-regulates-icos-for-cryptocurrency-company-funding.html
https://www.jdsupra.com/legalnews/sec-takes-enforcement-action-against-63668/
https://www.ccn.com/sec-subpoenas-80-cryptocurrency-firms-including-techcrunch-fund/
https://www.jdsupra.com/legalnews/sec-issues-guidance-to-cryptocurrency-33418/
https://www.jdsupra.com/legalnews/sec-v-plexcorps-cyber-unit-enforcement-30413/