

U.S.A. Anti-Money Laundering Approach to Criminal Use of Virtual Currency

Patricia Ruth McWilliam Lee*

목 차

I. Introduction	IV. Financial Crimes Enforcement Network (FinCEN) and Virtual Currency
II. U.S.A. Laws on Money Laundering	V. International Issues
III. Requirements on Transactions Related to Virtual Currency	VI. Proposed New Laws
	VII. Conclusion

미국 정부는 수십 년 동안 자금 세탁과 싸우고 있다. 자금 세탁 방지와 관련된 가장 중심적인 법률은 은행 비밀법이다. 금융 범죄 집행 네트워크 (FinCEN, 이하 핀센)는 자금 세탁 방지를 위해 싸우고 있는 주요 기관 중 하나이다. 핀센은 2011년에 가상 화폐를 포함하는 가상 통화를 포함하도록 비은행 자금 사업자(Money Services Business)의 정의를 수정했다. 이 법률에 따라 핀센(FinCEN)은 금융 기관이 미국에서 사업을 수행하는 한 해외 국가에 대한 조치를 취할 권한을 부여한다. 핀센(FinCEN)은 미국에 소재하는 부동산을 압류할 수 있다. 핀센(FinCEN)은 익명의 성격으로 인해 가상 화폐를 사용하여 돈을 쉽게 세탁할 수 있음을 인식했다. 핀센(FinCEN)은 다른 미국 기관과 협력하여 등록 요구 사항을 통해 자금의 불법 사용을 방지하고 금융 기관이 의심스러운 행동을 보고하도록 권장한다. 미국은 다른 국제기구와 함께 암호 화폐 사용과 관련된 범죄 행위를 막기 위해 노력하고 있다. 특히 암호 화폐의 인기가 높아지고 전 세계적으로 사용되는 것으로 보인다. 정부는 암호 화폐 및 기타 가상 화폐의 사용을 장려를 원하는 한편, 불법 행위를 숨기거나 불법 행위의 혜택을 누리려는 자금 세탁에 대해서는 규제할 것이라고 한다.

[주제어] 자금세탁방지, 은행비밀보호법, 암호화폐, 금융범죄단속네트워크, 미국세청, 자금세탁, 금융서비스사업, 가상화폐

DOI: 10.35148/ilsilr.2020.45.51

투고일: 2020. 1. 1. / 심사완료일: 2020. 1. 28. / 게재확정일: 2020. 2. 6.

* Associate Attorney at the Law Office of David J. McWilliam in South Carolina, USA, and Former Associate Professor at Konkuk University Law School

I . Introduction

The world of money is rapidly changing from brick and mortar banks, and paper money, to completely online banks and virtual currency not supported by any government. These changes may be exciting, but they can also lead to uncertainty in the law. Because of the nature of the internet and virtual currency, there are opportunities for people to abuse the characteristics of these virtual funds. One major concern related to the use of cryptocurrency is that there is an element of anonymity which could be exploited by criminals to launder money and avoid detection.

Money laundering is an activity that people engaged in illegal behavior use to try to “clean” their ill-gotten gains. The common example is that people earn money through organized crime and then run that money through a legal business so that the criminal can freely use the money without attracting government attention. Often criminals are more worried about the Internal Revenue Service (IRS) than other government agencies. The government may investigate if a person appears to have more cash to spend than that person reported as income to the IRS.

In the past, cash was laundered through different schemes to legitimize funds from illegal activity. In the American drama, “Breaking Bad”, the main character bought a car washing business to report his drug money as if the money were lawfully earned through the business. The major issue with virtual currency is that criminals have opportunities to launder money on a global scale. They may be able to transfer the money through different nations that are not concerned about the source of the funds. The United States government actively fights against laundered virtual currency, but instead of creating new laws, the government has expanded the definitions within those laws to cover virtual money and cryptocurrency funneled through financial institutions.

Cryptocurrency is typically easier to track than other forms of digital currency because it is encrypted. The point of the encryption is to allow the currency to be traded freely without a central organization keeping track of where the virtual money is held and who owns it. Each unit of the currency is identifiable without the need of a central registry. Bitcoin is the most well-known example of cryptocurrency. Currently, Facebook is attempting to start

offering a cryptocurrency called the Libra. The Federal Reserve Chairman, Jerome Powell, supports halting the Facebook project because of concerns over the strength of domestic currency and vulnerability for exploitation of the Libra.¹⁾ It appears as if the government is worried about misuse of these virtual funds, as well as the effect on the economy.

As noted above, United States government agencies are combating criminals that may take advantage of cryptocurrency's unique characteristics to hide illegal financial behavior. Cryptocurrency may be used to cover up customs violations, tax violations, and cybercrimes.²⁾ Some estimate that between \$100 billion and \$300 billion are being laundered each year for criminal enterprises.³⁾ Terrorists may use these types of funds to support their activities.⁴⁾ Because of these concerns over misuse of cryptocurrency, the federal government has expanded the definition of money and financial institutions to ensure that transactions involving virtual money must adhere to the anti-money laundering laws already in place. The main federal law on money laundering is the Bank Secrecy Act. The IRS and the Financial Central Enforcement Network (FinCEN) have worked together with other financial organizations to keep track of money that flows in and out of the United States, as well as money moved within the country. The government has stated that the most effective tools to prevent illegal use of cryptocurrency are reporting and registration requirements, as well as financial institutions reporting suspicious behavior.⁵⁾ These weapons are used to combat money laundering within the United States.

The Egmont Group, an international organization that works to build cooperation among nations to halt money laundering, described how professional money launderers often carry out their activities in regards to virtual currency. To start, the criminal must transfer funds to an e-wallet or address at a distribution platform which the professional launderer can access.⁶⁾ The second step is an act called layering, which is a way to make it more difficult

1) Press Release, *The Effect of Cryptocurrency on Money Laundering*, Market Watch (July 15, 2019), <https://www.marketwatch.com/press-release/the-effect-of-cryptocurrency-on-money-laundering-2019-07-15>.

2) *Id.*

3) *Id.*

4) *Id.*

5) *Id.*

6) Information Exchange Working Group (IEWG), *Professional Money Laundering Facilitators*, Egmont Group Bulletin, 5 (July 2019), <https://www.egmontgroup.org/sites/default/files/filedepot/external/20190701%20-%20IEWG%20>

to trace the money. When it comes to virtual currency, criminals may use money mule networks or complex chains of transfer make it difficult to track the funds.⁷⁾ Once the money is “clean”, the professional money cleaners may be able to give the funds back to the criminals or the criminals’ trusted associated.⁸⁾ These are the steps that lawmakers are concerned about the laundering of cryptocurrency and why many lawmakers want to prohibit or slow down the influx of virtual currency in the United States.

II. U.S.A. Laws on Money Laundering

The American government created anti-money laundering laws to fight against organized criminal enterprises which attempted to hide the source of their money. The first law, the Bank Secrecy Act, was named for the fact that people were taking advantage of bank secrecy laws in foreign countries to deposit funds.⁹⁾ Since 1970, the government has expanded the laws on money laundering to more effectively detect and stop any illegal activities. The rules focus on monitoring suspicious activity and mandatory reporting to make it more difficult for would-be launders to hide where they obtained their funds.

1. Bank Secrecy Act

The Bank Secrecy Act is the law central in the fight against money laundering. This act was established in 1970 and set out the requirements for financial institutions and private individuals for keeping records and reporting their money.¹⁰⁾ The law required that those affected by the law must state the source, amount and movement of their money whenever

Professional%20ML%20Networks%20Bulletin%20-%20final.v.pdf.

7) *Id.*

8) *Id.*, 6.

9) Internal Revenue Service, 4.26.5.2, *History of Bank Secrecy Act*, Internal Revenue Manual (10-03-2012). Available online at https://www.irs.gov/irm/part4/irm_04-026-005.

10) Public Law 91-508. Available online at <https://uscode.house.gov/statutes/pl/91/508.pdf>. See also Financial Crimes Enforcement Network, *History of Anti-Money Laundering Laws*, <https://www.fincen.gov/history-anti-money-laundering-laws>.

money is moved in or out of the country or deposited at a bank. The law required that those covered by the law must disclose cash transactions over \$10,000 and maintain a paper trail. The statutes created by this law have been expanded and modified over the years. The following laws build on the Bank Secrecy Act.

2. Money Laundering Control Act

The next law was enacted in 1986, entitled Money Laundering Control Act.¹¹⁾ This law stated that money laundering of any monetary instrument was a federal offense. Some of the pertinent aspects make it a crime to use any money produced by unlawful activity to conceal or disguise from where the money came.¹²⁾ It also punished people who failed to make the reports required by the Bank Secrecy Act and stated that violations of law could result in civil and criminal forfeiture.¹³⁾ Banks were ordered to make and follow procedures for monitoring compliance with the law and keeping correct records.

3. Anti-Drug Abuse Act

The Anti-Drug Abuse Act of 1988 expanded the definition of financial institutions to include businesses, such as car dealers and real estate closing agents.¹⁴⁾ The law required that these businesses had to report currency transactions. Also, if a person purchased monetary instruments valued at over \$3,000, the provider had to verify the purchasers' identity. The government appeared to want to limit criminals' ability to launder money through different businesses that involved large cash purchases.

4. Annunzio-Wylie Anti-Money Laundering Act

In 1992, the government passed the Annunzio-Wylie Anti-Money Laundering Act which

11) Public Law 99-570. Available online at <https://uscode.house.gov/statutes/pl/99/570.pdf>. *History of Anti-Money Laundering Laws, supra* note 10.

12) 18 U.S.C. §1956 (2016).

13) *Id.*

14) Public Law 100-690. Available online at <https://uscode.house.gov/statutes/pl/100/690.pdf>. *History of Anti-Money Laundering Laws, supra* note 10.

increased the punishments for Bank Secrecy Act violations.¹⁵⁾ The law required Suspicious Activity Reports and identification verification for wire transfers. These reports gave the government more information about possible instances of money laundering. The government depended on transparency to stop cleaning of illicit funds. This law established the Bank Secrecy Act Advisory Group. This group's purpose was to advise the Secretary of the Treasury on how to receive reports required by the Bank Secrecy Act, help law enforcement investigate money matters and help the public understand how the government used those reports.¹⁶⁾

5. Money Laundering Suppression Act

The Money Laundering Suppression Act of 1994 increased the requirements for banking institutions compliance with the law.¹⁷⁾ They had to train their organizations to detect and report money laundering schemes. The federal government created specific requirements for banking compliance. Also, the law created a duty for these financial institutions to report any suspected money laundering schemes to the appropriate agencies.¹⁸⁾ The increase in compliance rules increased the burdens on financial institutions.

Additional requirements included the law requiring that Money Services Businesses (MSB) had to register the owner or controlling person and keep a list of businesses that may act as agents for the financial services offered by the MSB.¹⁹⁾ If the MSB operated without registering, the MSB had committed a federal offense. These laws were not focused on only banks, but also anyone trading or transferring funds. The Money Laundering Suppression Act encouraged State governments to adopt uniform laws related to MSBs so that there could be uniform application of these laws on a nationwide basis.²⁰⁾

15) Public Law 102-550. Available online at <https://uscode.house.gov/statutes/pl/102/550.pdf>. *History of Anti-Money Laundering Laws*, *supra* note 10.

16) FinCEN Charter, *The Bank Secrecy Act Advisory Group*, FinCEN.gov, <https://www.fincen.gov/sites/default/files/shared/charter.pdf>.

17) H.R. 3235 – 103rd Congress (1993-1994). Available online at <https://www.congress.gov/bill/103rd-congress/house-bill/3235/text>. *History of Anti-Money Laundering Laws*, *supra* note 10.

18) *Id.*

19) *Id.*

20) In the United States, there are federal and state-level laws. The federal government may create federal laws under

6. Money Laundering and Financial Crimes Strategy Act

The Money Laundering and Financial Crimes Strategy Act of 1998 required additional training for banks to identify acts of money laundering.²¹⁾ The Department of the Treasury and other agencies were required to develop a National Money Laundering Strategy. The government also assembled task forces to concentrate on areas where money laundering was common. These designated areas were referred to as “high-risk money laundering and related financial crime areas”.²²⁾ The law allowed these task forces to address problems based on geographic or industrial area. Today there are governments of particular concern to the United States government, such as North Korea and Cuba, where the government is fearful that people may use laundered money to support acts of violence or human rights violations.

7. USA PATRIOT Act

In 2001, after the September 11 attacks, the government became more concerned with terrorism and how terrorists were funding their enterprises. This led to the adoption of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act).²³⁾ Title III of this law concentrated on halting money laundering. The law increased the requirements for identifying financial institution customers and increased the penalties for those who financially supported terrorism. The law prohibited American banks from engaging with foreigner shell banks that lacked a physical presence in any country.²⁴⁾ Banks had to increase their due diligence procedures,

the powers granted to the federal government by the United States Constitution, but cannot force state governments to adopt law. State governments may create any laws as long as those laws are not prohibited by the United States Constitution. The federalist system of government is a complex topic beyond the scope of this article. *See generally, Printz v. United States*, 521 U.S. 898 (1997).

21) H.R. 1756 – 105th Congress (1997-1998). Available online at <https://www.congress.gov/bill/105th-congress/house-bill/1756/text>. *History of Anti-Money Laundering Laws*, *supra* note 10.

22) *Id.*

23) H.R. 3162 – 107th Congress (2001-2002). Available online at <https://www.congress.gov/bill/107th-congress/house-bill/3162/text>. *History of Anti-Money Laundering Laws*, *supra* note 10.

especially when it came to business with foreign banks and accounts. The law directed financial institutions to increase the amount information they provided to the government. The anti-money laundering laws expanded to cover all financial institutions and increased the related penalties.²⁵⁾ The government could take special measures against areas that were of primary concern. Banks had to respond to requests for information within 120 hours. Whenever banks wished to merge or be acquired, the federal banking agencies had to review the bank's anti-money laundering records. MSBs that did business with countries which FinCEN determined to be of "primary money laundering concern" could be subject to sanctions under Section 311 of the USA PATRIOT ACT.²⁶⁾ The government was very sensitive at the time to terrorists using laundered money to fund terrorist acts.

8. Intelligence Reform and Terrorism Prevention Act

The most recent law enacted in 2004 was the Intelligence Reform and Terrorism Prevention Act. The law required that the Secretary of the Treasury created regulations requiring banks to report cross-border electronic transmissions of funds, if the Secretary believed the reporting was necessary to fight money laundering and the financing of terrorism.²⁷⁾ The Federal Regulations gave the Secretary of the Treasury the power to request additional recordkeeping and to increase reporting requirements to fight money laundering, along with the other goals of the regulations.²⁸⁾ The Secretary of the Treasury had the authority to issue orders to the financial institution Chief Executive Officers.²⁹⁾ As the daily use of the internet grew to make people's lives easier, the government was making laws to keep up with those changes.

24) *Id.*

25) *Id.*

26) H.R. 3162 – 107th Congress, *supra* note 23. See also Jennifer Shasky Calvery, Director of FinCEN, *Remarks of Jennifer Shasky Calvery, Director, Financial Crimes Enforcement Network at the Florida International Bankers Association Anti-Money Laundering Conference* (February 20, 2014), <https://www.fincen.gov/sites/default/files/2016-08/20140220.pdf>.

27) S. 2845 – 108th Congress (2003-2004). Available online at <https://www.congress.gov/bill/108th-congress/senate-bill/2845/text>. *History of Anti-Money Laundering Laws*, *supra* note 10.

28) 31 C.F.R. §1010.370 (2019).

29) *Id.*

9. Summation of Anti-Money Laundering Laws

These laws showed the transition of America's anti-money laundering laws over the years and the efforts that the government has taken to combat money laundering. Besides the changes to the laws, there have been numerous expansions of definitions of terms by federal agencies which have authority to define those terms under the laws. The government has steadily increased the requirements for financial institutions to maintain good records of any money transaction and to know who their customers are. Banks must have robust anti-money laundering systems to ensure they can catch any suspicious transactions. Those who engage in transfers of money must also follow reporting and record keeping as the law requires, even if those businesses do not consider themselves to be MSBs. As described below, there have been further attempts to expand the Bank Secrecy Act to make sure no illicit funds are allowed into the American market, as well as expansion of the definition of money to include all forms of virtual currency.

III. Requirements on Transactions Related to Virtual Currency

The laws noted above were drafted to fight against money laundering and other illegal uses of money. The government's focus was on record-keeping, reporting, and registration. There were penalties in place to deal with the situations when financial institutions choose not to adhere to these laws. The penalties range from civil penalties and forfeitures to criminal sanctions and being barred from working with money after a conviction. FinCEN works with the laws and regulations to make sure institutions are making their disclosures, to make sure that individuals are not funneling ill-gotten gains through different financial institutions, and to keep an eye on money coming from suspected countries to the United States.

1. Record Keeping

The government requires that banks and other financial institutions keep certain records

of currency transactions. The purpose of these records is to prevent illegal activity and help investigations and proceedings.³⁰⁾ Even institutions engaged in “informal” money transfers must keep certain records as required by the federal government.³¹⁾ These records must meet the standards set out by the Secretary of the Treasury, which includes keeping the records for a period of time and verifying clients’ identities.³²⁾ Anyone doing business in the United States must maintain certain information, such as the identity and address of the entities involved in the transaction, their legal capacity, the identity of the real parties with interests and a description of the transaction.³³⁾ Whenever people transfer over \$10,000, institutions must keep track of that transaction.³⁴⁾ When banking institutions have all this information, it becomes more difficult to hide illegal activities.

Not only do financial institutions need to track large transactions, but individuals entering the United States must also report movements of large sums of currency. Whenever people transport money, either personally or through a third-party, that person must make a report if the amount is over \$10,000.³⁵⁾ People who travel often have most likely seen questions on customs forms regarding carrying over \$10,000 of cash or its equivalent across international borders. The reason for this question is linked to the laws and regulations previously discussed. The government also wants to know if people have control over foreign financial accounts.³⁶⁾ Whenever people file their tax returns, the IRS wants to know if the individual has control over that type of foreign account. People need to make reports on their control and transfers of large amounts of money and state the source of those funds so that the government can be confident that the person obtained the money through legitimate channels.

30) 31 C.F.R. §1010.301 (2019).

31) 31 U.S.C. §5312 (2011).

32) 31 U.S.C. §5313 (2017).

33) 31 U.S.C. §5314 (2017).

34) 31 U.S.C. §5316 (2017), 31 C.F.R. §1010.330 (2012).

35) 31 C.F.R. §1010.340 (2019). *See* 31 C.F.R. §1010.306 (2016).

36) 31 C.F.R. §1010.350 (2011).

2. Suspicious Activity Reports

The laws also state that certain organizations must report suspicious transactions which may be linked to illegal activity, such as money laundering schemes. If an institution meets the definition of Section 5312 as a financial institution, it must report suspicious transactions.³⁷⁾ Some of these organizations include insurance companies, dealers in mutual funds and securities, casinos, banks, and MSBs. These reports may also be referred to as Suspicious Activity Reports. This is a type of voluntary report system, but failure to comply may result in fines and other penalties.

3. Internal Anti-Money Laundering Policies

Financial institutions must create and maintain adequate anti-money laundering programs. The goal of these laws is to halt money laundering and the Secretary of the Treasury has the authority to review the records of any institution as described in the law.³⁸⁾ The law requires that financial institutions have internal policies to stop money laundering, have a compliance officer, perform employee training programs, and have an independent audit to test these programs.³⁹⁾ The programs must have policies and procedures to reasonably assure continuing compliance. The focus is on knowing with whom the MSB is doing business, keeping records and filing reports.⁴⁰⁾ FinCEN believes that the best way to prevent money laundering is having the institutions that may come into contact with criminals to learn how to recognize them and subsequently report any suspicious behavior.

Some ways to do this is through confirming customer identification, filing reports, maintaining records, and responding to requests for information from law enforcement. FinCEN has issued many reports and guidelines to help those involved in these businesses to understand their obligations under the law.⁴¹⁾ MSBs should assess their risk of money laundering and

37) 31 U.C.S. §5312 (2017), 31 C.F.R. §1010.320 (2019).

38) 31 U.S.C. §5318 (2017).

39) *Id.*

40) 31 C.F.R. §1022.210 (2011).

41) FinCEN Guidance, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual*

design their programs accordingly. They need to know their customers to understand any potential vulnerability to criminal activity.⁴²⁾ MSBs need to educate and train their employees and appoint a person to be in charge of compliance and have someone conduct an independent review to monitor and maintain the program.⁴³⁾ If MSBs carry out these steps, hopefully they can detect any hint of criminal behavior swiftly. FinCEN has many resources available to help businesses that have questions.

FinCEN and other agencies that combat money laundering are aware of off-shore issues related to finance, such as businesses with foreign shell banks and foreign countries which engage in suspicious behavior. Some criminals may attempt to hide their money from the American government by keeping it in foreign banks. American banks may not provide services to foreign shell banks, which include foreign banks that do not have a physical presence in the United States.⁴⁴⁾ The government wants to be able to go after the foreign bank's assets in the United States if the government discovers that the foreign bank or financial institution failed to comply with the regulations to combat money laundering. The Secretary of the Treasury may require banks to take extra precautions if the Secretary believes there are reasonable grounds to be concerned about money laundering activities occurring outside of the United States.⁴⁵⁾ Often directives come from the Secretary when there is an issue with a particular nation or geographic region. The main methods to protect against money laundering are keeping records of the parties involved with the money transaction.

4. Registration of Financial and Money Services Businesses

The Bank Secrecy Act requires all money transfers to register their businesses.⁴⁶⁾ The U.S. government created the law against unlicensed money transmitting businesses in 1992

Currencies, FIN-2019-G001, 9 (May 9, 2019), <https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf>.

42) *Id.*, 10.

43) 31 C.F.R. §1022.210 (2011).

44) 31 U.S.C. §5318 (2017).

45) 31 U.S.C. §5318A (2017).

46) 31 U.S.C. §5330 (2017).

and updated the law in 2006. This law states that anyone running or managing an unlicensed money transferring business may receive up to five years in prison.⁴⁷⁾ Transferring funds includes any type of transfer within the United States or abroad.

Anyone who receives more than \$10,000 in any form of currency, including electronic money, must file a report with the IRS.⁴⁸⁾ The law requires that the entity disclose information about the parties, the amount, the date of the transaction and any other required identifying information. MSBs must register, even if they are not licensed as MSBs in any state, with the Department of the Treasury.⁴⁹⁾ They must keep a list of agents, which means persons who perform any work for the MSB.⁵⁰⁾ The government appears to be concerned with how businesses operate and that those who meet the definition register with the government.

The government may determine that a business is a MSB if that business operates like one. If a store, such as Walmart, distributes money orders, but does nothing more, the government would not classify it as a MSB. If Walmart also paid over \$1,000 per person per day in checks or exchanged currency, then the regulations would require that it register as a MSB and register its agents. The government cares about how an entity operates, rather than how the entity defines itself.

Not all people who use an anonymizing service are engaged in money laundering, but many people who wish to launder illicit funds use those services. Whenever a person transfers funds and uses that type of service, because it is part of the money transfer, the whole transfer is subject to the rules related to MSBs.⁵¹⁾ The government would not automatically classify a provider of anonymizing software as a money transmitter. That means that a software provider would not be required to follow the regulations of the Bank Secrecy Act, but a person using that software could be operating as a money transferor.⁵²⁾ If a person attempts to use that type of software to hide the source of the money, the transmitter must still report that transaction as part of the Bank Secrecy Act requirements. The rules about registration are another way

47) 18 U.S.C. §1960 (2006).

48) 31 U.S.C. §5331 (2017).

49) 31 U.S.C. §5330 (2017).

50) *Id.*

51) FIN-2019-G001, 19, *supra* note 41.

52) *Id.*, 20.

to make sure those that transfer money provide the same type of information to the government as banks are required to.

5. Safe Harbor Rule for Information Sharing

Whenever financial institutions suspect some act of money laundering, the law encourages them to voluntarily share information. The law provides a safe harbor rule so that these organizations can share identifying information to fight money laundering.⁵³⁾ FinCEN has created a notice form on their website for reporters to use before sharing sensitive information. The safe harbor rule protects the financial institution that shares information from any liability related to sharing or failing to give notice of sharing information to the identified person or entity.⁵⁴⁾ The institution may also need to file a Suspicious Activity Report if there is reason to suspect money laundering if that entity is required to make that report by law.

6. Power to Request and Gather Information

To make sure that institutions are following the requirements, the government may engage in information gathering. One way is to issue summons to those with information at financial institutions.⁵⁵⁾ This means that anyone in charge of records or someone who works at the financial institution may be summoned to give testimony, be examined, and be required to produce records and books.⁵⁶⁾ FinCEN, the IRS and Customs and Border Protection may issue summons as part of an investigation.⁵⁷⁾ These tools of information gathering help the government fight money laundering and search deeper into unusual financial behavior.

As noted above, there is special vulnerability when transactions occur internationally. The Secretary of the Treasury may require specific financial institutions to file reports about certain transactions with particular foreign entities.⁵⁸⁾ Once the Secretary decides to investigate, it

53) 31 C.F.R. §1010.540 (2019).

54) *Id.*

55) 31 C.F.R. §1010.911 (2019).

56) *Id.*

57) 31 C.F.R. §1010.912 (2019).

may ask for specified information related to a transaction, which includes the name of the institution, the name of the maker, payee, and endorsers, if any.⁵⁹⁾ This information would allow the Secretary to investigate all the involved parties and see if any illicit behavior occurred.

7. Penalties for Non-Compliance

The law details numerous penalties for failure to comply with the Bank Secrecy Act. If a foreign entity has failed to comply with a summons or subpoena, no American financial institutions may engage in transactions or other relationships with those entities.⁶⁰⁾ Once an American institution receives notice that they must terminate a relationship with a foreign bank, they must do so within ten days. Failure to comply may result in a civil penalty of \$10,000 per day until the relationship is terminated.⁶¹⁾ There may not be much the government can do to punish the foreign institution because it may be outside of the United States' jurisdiction. However, the government has the authority to prevent financial institutions within the United States from transacting business with the noncompliant foreign institution.

There are civil penalties when individuals and institutions fail to keep required records. When a financial institution fails to make a report or keep adequate records, FinCEN has authority to issue civil penalties.⁶²⁾ Whenever anyone fails to report holding funds overseas over the amount of \$10,000 or fails to report a transaction, the government may take the entire amount of the transported currency.⁶³⁾ The penalty for a bank willfully failing to make required reports is the amount of the money involved in the transaction on any involved director or institution.⁶⁴⁾ If the amount at issue is less than \$25,000, then that amount is the minimum penalty. The maximum penalty is \$100,000.⁶⁵⁾ The same penalties apply when banks refuse to comply with requests for information or failure to report accounts. When

58) 31 C.F.R. §1010.360 (2019).

59) *Id.*

60) 31 C.F.R. §1010.670 (2019).

61) *Id.*

62) 31 C.F.R. §1010.810 (2014).

63) 31 C.F.R. §1010.820 (2016).

64) *Id.*

65) *Id.*

the sanctioned party did not act intentionally, but instead acted negligently, the penalty is \$500.⁶⁶⁾ Negligence means that the party acted carelessly or unreasonably, but not willfully. These penalties punish failure to adhere to report and recordkeeping requirements. There are additional penalties if an organization knowingly participated in money laundering schemes.

The court may also issue criminal penalties for willful violations of these laws and regulations. When banks fail to keep financial records as the laws require, the institution or people in charge may receive a year of jail time and a \$1,000 fine.⁶⁷⁾ When an entity fails to make reports related to foreign transactions and currency, the penalties may include five years of prison and a \$250,000 fine.⁶⁸⁾ If the actor also broke other American laws or was part of a pattern of illegal activity, the penalty increased to ten years of prison and \$500,000 in fines.⁶⁹⁾ Whenever a person willfully makes a false statement or representation, the government may punish that person with up to five years of jail and \$10,000 in fines.⁷⁰⁾ The government may assess civil and criminal penalties against a guilty party.

One example of FinCEN assessing civil penalties is a case against Eric Powers of California who exchanged virtual currency. He bought and sold Bitcoin and his activities met the definition of a money transmitter and a financial institution.⁷¹⁾ He converted Bitcoin into dollars by delivering currency in exchange for Bitcoin. He also engaged in online discussions related to anti-money laundering compliance and registration for MSBs.⁷²⁾ He even stated on the internet that he would help others avoid their anti-money laundering reporting and recordkeeping obligations.⁷³⁾ He engaged in transactions that were highly suspicious and never filed any reports related to those activities.⁷⁴⁾ Lastly, he failed to report currency transitions

66) See Table 1 for maximum penalties after 2019. 31 C.F.R. §1010.821 (2018).

67) 31 C.F.R. §1010.840 (2019).

68) *Id.*

69) *Id.*

70) *Id.*

71) In the Matter of: Eric Powers, United States of America Department of the Treasury Financial Crimes Enforcement Network, No. 2019-01, 3 (April 18, 2019), https://www.fincen.gov/sites/default/files/enforcement_action/2019-04-18/Assessment%20Eric%20Powers%20Final%20for%20Posting%2004.18.19_1.pdf.

72) *Id.*, 3.

73) *Id.*, 4.

74) *Id.*, 5-6.

over the amount of \$10,000 and it appeared that Mr. Powers had carried out many of those transactions without reporting them.⁷⁵⁾ Based on all these actions, FinCEN decided that Mr. Powers' actions were intentional, that he knew about his obligations under the Bank Secrecy Act, and he should pay a penalty.

Mr. Powers admitted to violating the Bank Secrecy Act and consented to civil money penalties.⁷⁶⁾ FinCEN decided to assess a penalty of \$35,350, but could have imposed a penalty of \$25,000 for each willful violation.⁷⁷⁾ Mr. Powers' operation was a MSB and he willful violated the "registration, program, and reporting requirements" of the law.⁷⁸⁾ Though FinCEN could have assessed more in penalties, they took into consideration his ability to pay, as well as his other forfeitures to other government agencies. The case of Mr. Powers exemplifies the type of penalties applicable to violations of these laws.

Another matter that triggered penalties occurred with Ripple Labs Inc. Ripple Labs Inc. sold their virtual currency without registering with FinCEN and designing an anti-money laundering program as required by BSA.⁷⁹⁾ XRP II later assumed the Ripple Labs business, which also included the sale of virtual currency, and failed to create an anti-money laundering program or to report suspicious activities. Because of this behavior FinCEN fined them \$700,000 as a civil penalty.⁸⁰⁾ FinCEN had the authority to investigate failures to follow the Bank Secrecy Act related to cryptocurrency and has been enforcing the law aggressively.

There is an additional penalty to stop individuals who had previously been involved with money laundering from ever working at a bank or financial institution. After a court has prosecuted a person for that type of involvement, that person may not have any control over a bank or other financial institution.⁸¹⁾ This law's purpose is obvious because once a person has failed to adhere to these rules and regulations; they may be untrustworthy to be in charge

75) *Id.*, 7.

76) *Id.*, 1.

77) *Id.*, 7.

78) *Id.*, 2.

79) Steve Hudak, *FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger*, FinCEN Release (May 5, 2015), <https://www.fincen.gov/news/news-releases/fincen-fines-ripple-labs-inc-first-civil-enforcement-action-against-virtual>.

80) *Id.*

81) 12 U.S.C. §1829 (2010).

of financial transactions again.

These laws only apply if the money transfer involves an entity located in the United States. If an entity fails to comply with these record-keeping requirements, that person may be subject to an injunction and civil and criminal penalties. Smuggling money into or out of the United States could result in five years in prison, forfeiture of the involved property and other civil penalties.⁸²⁾ Registration helps to keep the businesses honest and transparent. All these penalties are tools to encourage compliance with the anti-money laundering laws.

IV. Financial Crimes Enforcement Network (FinCEN) and Virtual Currency

FinCEN is a body that helps to enforce the laws related to banking and financial institutions. Their goal is to prevent criminal activity related to the misuse of funds. The Federal Regulations state that FinCEN has authority to enforce and ensure compliance with the rules related to banking and finance.⁸³⁾ There are other federal agencies that report to FinCEN on their specific areas.⁸⁴⁾ FinCEN works to prevent abuses of financial institutions and to fight money laundering.

1. FinCEN Guidance and Statements

FinCEN issued many statements, guidelines and speeches so that financial institutions are aware of their obligations under the law. During the past few years, there have been many statements clarifying that virtual currency is currency and anyone transferring these funds must follow the Bank Secrecy Act. In 2018, the director stated that the filings required by the Bank Secrecy Act are vital to prevent money laundering and other funding of illegal activities.⁸⁵⁾ The director stated that compliance with anti-money laundering regulations was

82) 31 U.S.C. §5332 (2017).

83) 31 C.F.R. §1010.810 (2014).

84) *Id.*

critical to preventing misuse of money. In 2011, the FinCEN amended the definition of money services businesses to include MSBs that accepted and transmitted virtual currency, among other substitutes for currency.⁸⁶⁾ Users of virtual currency are not subject to MSB record-keeping requirements, but any organization administering or exchanging these virtual funds is subject to FinCEN, as noted in a Guidance published by FinCEN in 2013.⁸⁷⁾ That means that ordinary people who purchase virtual currency do not have to follow the reporting requirements, but hubs and other transferors do need to keep records and report suspicious activity. When a person converts funds from virtual cash to physical money, that person is operating as an MSB and must adhere to the law.

The rules cover entities that transfer virtual currency between a seller and buyer. It does not cover people directly selling or purchasing virtual currency or entities that accept virtual currency in payment.⁸⁸⁾ FinCEN expects institutions that handle virtual currency money transmissions to comply with all reporting requirements. If a business attempts to conceal the source of the transmission of virtual currency, those businesses are money transmitters and must follow the Bank Secrecy Act regulations. FinCEN and the IRS work together to ensure compliance with the Bank Secrecy Act. Some issues involve “virtual currency trading platforms, administrators, virtual currency kiosks (or ATM) companies, crypto-precious metals dealers, and individual peer-to-peer exchangers.”⁸⁹⁾ These new entities which aid in transmitting virtual currency pose new forms of vulnerability for money laundering and FinCEN has been working with other government agencies to reduce or eliminate the money laundering risks. For example, people may be able to anonymously deposit cash into a virtual currency kiosk and have that money converted to cryptocurrency without providing adequate documentation of the depositor’s identity. This is precisely the type of matter FinCEN and

85) Kenneth A. Blanco, FinCEN Director, *Speech delivered at the 2018 Chicago-Kent Block (Legal) Tech Conference*, FinCEN Remarks (August 9, 2018), <https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-2018-chicago-kent-block>.

86) *See generally* 31 CFR §§1010, 1021 and 1022 and FR Doc. 2011-18309 (July 20, 2011), <https://www.govinfo.gov/content/pkg/FR-2011-07-21/pdf/2011-18309.pdf>.

87) FinCEN Guidance, *Application of FinCEN’S Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN-2013-G001 (March 18, 2013), <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>.

88) *Id.*

89) Kenneth A. Blanco, *supra* note 85.

other government bodies want to stop.

FinCEN has also stated that the Bank Secrecy Act's regulations related to MSBs also apply to transmissions of values that are a substitute for currency, specifically convertible virtual currencies.⁹⁰⁾ If a person acts as a broker or dealer in currencies and transfers money not a part of the transaction, that person must comply with the requirements of a MSB. Whether a person qualifies as a MSB depends on that person's activities, not their business status or the terms they use.⁹¹⁾ Once an entities' behavior meets the definition of a MSB, it must keep records, make reports and have an effective anti-money laundering program.⁹²⁾ Mr. Powers' situation above is an example of an entity that did not consider that he was a MSB, but FinCEN held him to that standard.

The U.S. Commodity Futures Trading Commission, FinCEN and the Securities Exchange Commission (SEC) work together to prevent money laundering and other misuses of financial institutions. The leaders of these three agencies issued a statement in October 2019.⁹³⁾ People, who engage in activities which involve digital assets, including cryptocurrency, must follow the Bank Secrecy Act. The joint statement emphasized the fact that just because the terms used by a financial institution do not match up with the language in the laws, does not mean that organization is exempt.⁹⁴⁾ The government looks at the economic reality and use of the funds, assets and transactions.

FinCEN went on to emphasize in a joint statement that even if a business is not a MSB or falls into some other category that must comply with the Bank Secrecy Act, the traded digital assets may be securities under the law and need to follow the regulations set by the SEC.⁹⁵⁾ All people who own or trade securities must register them and anyone trading them

90) FIN-2019-G001, *supra* note 41.

91) *Id.*

92) *Id.*

93) Heath Tarbert, Chairman, U.S. Commodity Futures Trading Commission (CFTC), Kenneth A. Blanco, Director, Financial Crimes Enforcement Network (FinCEN), Jay Clayton, Chairman, U.S. Securities and Exchange Commission (SEC), Public Statement: *Leaders of CFTC, FinCEN, and SEC Issue Joint Statement on Activities Involving Digital Assets*, SEC.gov (Oct. 11, 2019), <https://www.sec.gov/news/public-statement/cftc-fincen-secjointstatementdigitalassets>.

94) *Id.*

95) *Id.*

should pay attention to potential money laundering risks, according to the SEC.⁹⁶⁾ These statements, speeches, and guidelines clarify that anyone doing business related to cryptocurrency must make sure they are in compliance with the Bank Secrecy Act and other applicable laws.

2. FinCEN Investigations

FinCEN works with different United States law enforcement agencies, as well as international organizations, such as the Egmont Group, to combat money laundering. FinCEN is working with other nations to improve reporting requirements and help financial institutions recognize illicit financial activities.⁹⁷⁾ FinCEN investigates with authority from the law, but it also relies on voluntary disclosures through Suspicious Activity Reports and other reports submitted by financial institutions.

When private actors report suspicious activities, it helps FinCEN fight against misuse of virtual currency.⁹⁸⁾ One of FinCEN's powerful tools is sanctions that motivate changes in behavior. When entities must keep records and there is no anonymity, that helps prevent exploiting services and illegal behavior. There are critics who believe the reporting regulations may push virtual currencies outside the United States; however the Under Secretary David S. Cohen believed that increasing transparency would make virtual currencies more stable and encouraged their use in the United States because the average person may feel more confident about purchasing virtual currencies with the government oversight.⁹⁹⁾ Perhaps more government involvement may discourage those who wish to hide their activities, but government involvement may also decrease scams and other fraudulent transactions, which could increase confidence in virtual currency.

Cryptocurrency may be easier to exploit for money laundering because there is no administer

96) *Id.*

97) Kenneth A. Blanco, *supra* note 85.

98) *Id.*

99) David S. Cohen, *Remarks from Under Secretary of Terrorism and Financial Intelligence David S. Cohen on "Addressing the Illicit Finance Risks of Virtual Currency"*, U.S. Department of the Treasury (March 18, 2014), <https://www.treasury.gov/press-center/press-releases/Pages/jl236.aspx>.

serving as an intermediary between a buyer and seller.¹⁰⁰⁾ FinCEN identified and investigated Liberty Reserve which appeared to be heavily involved with money laundering. Liberty Reserve was a centralized virtual currency, which means that Liberty Reserve funds had to be converted and placed with a central repository.¹⁰¹⁾ FinCEN also investigated BTC-e, which had over 700,000 customers worldwide and was located outside of the United States.¹⁰²⁾ Even though it was a non-American company, FinCEN assessed \$12 million in civil penalties against one of BTC-e's administrators, Alexander Vinnik for money laundering.¹⁰³⁾ These investigations show the real risk that cryptocurrency poses, but also that FinCEN has the ability to discover illegal behavior and stop it.

Cryptocurrency is treated like cash. If people buy and sell with it, they are not required to maintain records, except for transactions over \$10,000. However, FinCEN is most interested in when virtual currency is converted from or to "real" money. The Under Secretary mentioned that FinCEN may need to conduct more oversight if virtual currency becomes more common, but that the current rules meet the requirements for safety.¹⁰⁴⁾ Individuals are not subject to the Bank Secrecy Act and other regulations of money transmitters if they engage in "mining" virtual currencies or buying and selling for investment purposes only.¹⁰⁵⁾ The law is limited to those transmitting or trading monetary instruments.

The government alleged Liberty Reserve laundering over \$6 billion, and FinCEN was concerned that other centralized virtual currencies processed similar volumes of transactions.¹⁰⁶⁾ The amount of transactions performed with virtual currencies has been much smaller than those seen in the Automated Clearing House Network and wire transfers processed by Bank of America.¹⁰⁷⁾ However, that does not mean that FinCEN should not be paying close

100) Jennifer Shasky Calvery, *Before the United States Senate Committee on Banking, Housing, and Urban Affairs Subcommittee on National Security and International Trade and Finance Subcommittee on Economic Policy*, FinCEN (November 19, 2013), <https://www.fincen.gov/sites/default/files/2016-08/20131119.pdf>.

101) *Id.*

102) Kenneth A. Blanco, *supra* note 85

103) *Id.*

104) David. S. Cohen, *supra* note 99.

105) Jennifer Shasky Calvery (2014), *supra* note 26.

106) *Id.*

107) *Id.*

attention to virtual currencies because of the ease of using this medium to use funds for illegal purposes, as noted by the FinCEN representative.¹⁰⁸⁾ There is concern that in the future, the importance of virtual currency may increase and more criminals may rely on virtual currency for their activities.

Law enforcement agencies work with FinCEN to investigate potential acts of money laundering. One way they do that is to request FinCEN gather information about suspected financial institutions.¹⁰⁹⁾ Law enforcement must give the names of the suspected entities and state that they have reasonable grounds to suspect the investigated person is engaged in money laundering.¹¹⁰⁾ FinCEN can ask a financial institution to check their records for any transactions involving suspected persons. FinCEN may also request information on their initiative if they believe a bank had some interaction with a suspected person or organization.¹¹¹⁾ A big part of FinCEN's investigative powers comes from requiring banks and other financial institutions to share information about their customers and others with whom they have some transaction. When FinCEN requests information, the banks must not disclose to others that there is an investigation.¹¹²⁾ FinCEN has the opportunity to complete their investigation without the suspects knowing they are being looked at and gives FinCEN a better chance of conducting a thorough search before any charges are brought or the suspect can move all of their funds and property outside of the United States.

V. International Issues

Virtual currency's appeal is tied to the ease of transferring it. However, that may be the largest risk associated with it in regards to money laundering. Because money can be transferred across the world as easily as sending an email, these matters often cross international borders. The American government has laws dealing with nations of particular concern, which include

108) *Id.*

109) 31 C.F.R. §1010.520(b) (2019).

110) *Id.*

111) *Id.*

112) *Id.*

North Korean and Iran. Other countries, such as Venezuela and Cuba, have used virtual currency to attempt to bypass American sanctions. Because of the global nature of virtual currency and money laundering, the American government works with other countries and international organizations to combat these problems.

The United States government has created special regulations requiring due diligence when an institution does business with a foreign company. A few of these countries include North Korea, Bank of Dandong and Iran. No American financial institution may allow a North Korean banking institution to open or maintain an account in the United States or process transactions involving North Korean banks.¹¹³⁾ The United States government requires that American banks perform special due diligence to prevent the occurrence of any transactions. This rule was put into place in 2016. The same prohibitions and special due diligence requirements apply to transactions involving the Bank of Dandong, Ltd. no matter the location of the bank branch, which was enacted in 2017.¹¹⁴⁾ The Bank of Dandong is a Chinese bank that the United States government suspected of helping North Korea launder money and avoid U.S. sanctions.¹¹⁵⁾ The special rules enacted in 2019 in regards to Iran are similar; however, the United States Department of the Treasury's Office of Foreign Assets Control may authorize transactions with particular accounts.¹¹⁶⁾ Transactions may only occur if the International Emergency Economic Powers Act authorizes it or does not prohibit it.¹¹⁷⁾ These nations are believed to pose special risk to the United States and the government created these laws so that financial institutions cannot be used as a tool of abuse.

The United States is concerned that countries which the United States has sanctioned will use cryptocurrency to avoid those sanctions. The United States has determined that the risk of mishandled or illicit funds is too high to allow business with these nations. In particular, the government has sanctioned Venezuela because of the lack of law enforcement and the

113) 31 C.F.R. §1010.659 (2016).

114) 31 C.F.R. §1010.660 (2017).

115) Agence France-Presse, *Chinese bank banned from operating in US over North Korea ties*, South China Morning Post (November 3, 2017), <https://www.scmp.com/news/china/diplomacy-defence/article/2118225/chinese-bank-banned-operating-us-over-north-korea-ties>.

116) 31 C.F.R. §1010.661 (2019).

117) *Id.*

multitude of questionable government action. Venezuela is the second-largest national market for peer to peer trading of Bitcoin and this country had recently created an oil-backed cryptocurrency called the Petro.¹¹⁸⁾ The issue is that Venezuela is already suffering from massive inflation, human rights violations and a fleeing population.¹¹⁹⁾ The United States' goal of sanctions was to encourage positive change instead of allowing the current president to remain in power and keep the same course of action. The Venezuela government appeared to be highly corrupt with little legal oversight of money transfers and anti-money laundering policies.

In Cuba, the people used cryptocurrency to avoid United States' sanctions which involve financial blockades. Some Cubans used the money to access the global market and to receive payment.¹²⁰⁾ Other organizations used cryptocurrency to provide foreign aid to those in need in Cuba.¹²¹⁾ The Cuban government had announced plans to attempt to use virtual currency to help the economy.¹²²⁾ There have been various viewpoints on Cuba, but the American government appears to be considered with human rights violations and the lack of oversight over financial systems and transactions, as seen in Venezuela. The United States had the authority to stop transactions with countries who had exhibited suspicious behavior and lack transparency in their transfer of money. As described above, the American government has the power to prohibit any American banks or financial institutions from transacting business with suspected nations.

Because of the global world of finance and the speed at which the internet allows funds to be transferred, different nations find it more effective to work together to fight money laundering. FinCEN has been working with an international organization called the Egmont Group to combat money laundering.¹²³⁾ The Egmont Group is a platform made of 164 different Financial Intelligence Units, which work together to stop domestic and international money

118) Samuel Haig, *Venezuelan Petro Against US Sanctions: History and Use of the Crypto*, Coin Telegraph (July 17, 2019), <https://cointelegraph.com/news/venezuelan-petro-against-us-sanctions-history-and-use-of-the-crypto>.

119) *Id.*

120) Samuel Haig, *Ordinary Cubans Embrace Cryptocurrency to Bypass Crippling Sanctions*, Cryptocurrency News, (September 13, 2019), <https://www.ccn.com/ordinary-cubans-embrace-cryptocurrency-to-bypass-crippling-sanctions/>.

121) *Id.*

122) *Id.*

123) Kenneth A. Blanco, *supra* note 85.

laundering.¹²⁴⁾ The groups work together by sharing information with each other, as well as other international organizations, such as the United Nations, G20 Finance Ministers and Financial Action Task Force (FATF).¹²⁵⁾ There are representatives from FinCEN on the steering group of Egmont.¹²⁶⁾ These groups share information and strategies to fight money laundering and prevent the transfer and use of illicit funds. FinCEN has also worked with other nations to improve reporting requirements and help financial institutions know what kinds of activity may signal illicit financial activities.¹²⁷⁾ Together these organizations have a stronger chance to catch money launderers and those who hope to hide the source of their illegally-earned money.

The United States government works with other nations to develop plans to stop money laundering and also has entered treaties and agreements to share information whenever a foreign nation suspects an individual or organization attempted to bypass the law. As noted above, one way to learn about money laundering schemes is by requesting information from banks and other financial institutions. When the United States has a treaty or other agreement with a foreign country allowing subpoenas, then the Secretary or Attorney General may issue a subpoena to foreign financial institutions for records.¹²⁸⁾ If the foreign entity fails to comply with any summons or subpoena issued by the Secretary or Attorney General, the United States government may inform all American banks to stop doing any business or hold any accounts for those non-complying institutions.¹²⁹⁾ If the American institution continues to do business with the foreign entity which is refusing to comply with the summons or subpoena, the government has the authority to punish that financial institution.

The United States is working with FATF, which is a group of nations that set global standards to combat money laundering. There is an attempt to create unity in the rules applied internationally.¹³⁰⁾ Members of FATF do not set actual laws. Instead, they have made

124) Egmont Group, *About*, <https://egmontgroup.org/en/content/about>.

125) *Id.*

126) Marko Stolle, *Information Exchange on ML/TF Working Group (IEWG)*, Egmont Group, <https://egmontgroup.org/en/content/information-exchange-mltf-working-group-iewg>.

127) Kenneth A. Blanco, *supra* note 85.

128) 31 C.F.R. §1010.670 (2019).

129) *Id.*

130) Steven Mnuchin, *Remarks of Secretary Steven T. Mnuchin FATF Plenary Session Orlando, Florida*, U.S. Department

regulations for the group members to follow and turn over rule-breakers to the government of a member state. One recent regulation is the “travel rule” which is meant to halt anonymous transactions of money over \$3,000, especially virtual currency like Bitcoin.¹³¹⁾ One person interviewed by Forbes believed it would be impossible for cryptocurrency transfers to comply with this regulation because of the required data.¹³²⁾ The Egmont Group, FATF and other international treaties and agreements are some ways that the United States has cooperated with other nations to stop the influx of illegal gained virtual currency.

VI. Proposed New Laws

It appears that virtual currency’s role in the financial world will only increase. Lawmakers in the United States are aware of the issues facing the world, such as sanctioned countries attempting to circumvent those sanctions, as well as criminals attempting to hide the illicit sources of their wealth. The American government appears to be focused on preventing illicit funds from being used to pay for acts of terrorism. There are also honest people who also wish to take advantage of this new currency and be a part of what some people view as the future of finance. The government has been considering different laws that help protect the public and ensure no misuse of cryptocurrency by criminals.

1. Virtual Currency Consumer Protection Act and U.S. Virtual Currency Market and Regulatory Competitiveness Act

One proposal is the “Virtual Currency Consumer Protection Act,” which would direct

of the Treasury (June 21, 2019), <https://home.treasury.gov/news/press-releases/sm713>.

131) Jonathan Chester, *Could The New Financial Action Task Force Regulation Be The End of Bitcoin?*, Forbes (August 1, 2019), <https://www.forbes.com/sites/jonathanchester/2019/08/01/could-the-new-financial-action-task-force-regulation-be-the-end-of-bitcoin/>. See generally FATF Report, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, FATF (June 2014), <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>.

132) *Id.*

various government agencies to consider how people manipulate the price of virtual currencies, which types of virtual currencies are vulnerable to manipulation, and the effects on investors.¹³³⁾ As noted above, there are government officials concerned about the effects of virtual currency on the American financial market and how virtual currency may affect the United States dollar. The government also wants to know the best methods to surveil these markets and make sure the regulations against money laundering and other money-based regulations are enforced.¹³⁴⁾ A congressional committee also introduced a Bill entitled “U.S. Virtual Currency Market and Regulatory Competitiveness Act,” which directs that federal agencies should investigate the effect, importance and economic impact of virtual currencies and ensure that the United States is competitive in this industry.¹³⁵⁾ This Bill’s focus is American competitiveness in the global virtual currency marketplace. This Bill would encourage the government to investigate the potential benefits of blockchain technology and may help the SEC feel more comfortable with bitcoin offerings on the stock exchange.

2. ILLICIT CASH Act

A recently proposed Bill is the ILLICIT CASH Act which is meant to work towards improving the laws related to anti-money laundering.¹³⁶⁾ This proposed law also focuses on increasing the effectiveness of some the rules already in place, by amending 31 U.S.C. §5311 et al. Some of the proposed laws include increasing information sharing between financial institutions, strengthening programs to fight money laundering, and increasing reporting requirements. The suggested law would expand the meaning of funds to include “value that substitutes for currency or funds.”¹³⁷⁾ The Bill recognizes that criminals are increasingly using

133) H.R. 922 – 116th Congress (2019-2020). Available online at <https://www.congress.gov/bill/116th-congress/house-bill/922/text>.

134) *Id.*

135) H.R. 923 – 116th Congress (2019-2020). Available online at <https://www.congress.gov/bill/116th-congress/house-bill/923/text>.

136) S. 2563 – 116th Congress (2019-2020). Available online at <https://www.congress.gov/bill/116th-congress/senate-bill/2563/text>.

137) *Id.*

virtual funds in relation to illicit activity and that law enforcement must have the tools to detect and stop those actions. The Bill also wants to study Chinese money laundering and how authoritative regimes use the financial system for their benefit.

VII. Conclusion

Cryptocurrency does not seem to be a flash in the pan and may be here to stay. Many Bills fail to become laws, but the fact that Congress is discussing these issues related to virtual currency may show that virtual currency is becoming increasingly important. The government needs to take action to ensure people are protected instead of merely blocking every attempt at using cryptocurrency within the United States. Lawmakers, especially those at FinCEN, are aware that people want to have access to virtual currency and may look to foreign nations if the rules and regulations in the United States are too stringent. The government's strategy in response to virtual currency was to expand the definitions of money, transactions and money service businesses. Doing so allowed the law to quickly expand to make sure regulations covered transactions involving cryptocurrency. The Bank Secrecy Act has been around since 1970, but is still in effect today. FinCEN appears to have quickly responded to the changing nature of money and has worked together with other international organizations to prevent money laundering and help nations form laws to handle new technology, such as anonymizing software. FinCEN has placed special emphasis on reporting and recordkeeping, which may be the strongest tools to fight use and importation of illicit funds. FinCEN and the United States government appear cautious as they approach this new form of money, but also seem to be drafting regulations so that Americans can use virtual currency and be a part of an innovative method of finance.

References

1. Statutes

12 U.S.C. §1829 (2010).

18 U.S.C. §1956 (2016).

18 U.S.C. §1960 (2006).

31 U.S.C. §5312 (2011).

31 U.S.C. §5313 (2017).

31 U.S.C. §5314 (2017).

31 U.S.C. §5316 (2017)

31 U.S.C. §5318 (2017).

31 U.S.C. §5318A (2017).

31 U.S.C. §5330 (2017).

31 U.S.C. §5331 (2017).

31 U.S.C. §5332 (2017).

Public Law 91-508. Available online at <https://uscode.house.gov/statutes/pl/91/508.pdf>.

Public Law 99-570. Available online at <https://uscode.house.gov/statutes/pl/99/570.pdf>.

Public Law 100-690. Available online at <https://uscode.house.gov/statutes/pl/100/690.pdf>.

Public Law 102-550. Available online at <https://uscode.house.gov/statutes/pl/102/550.pdf>.

2. Regulations

31 C.F.R. §1010 (2019).

31 C.F.R. §1021 (2011).

31 C.F.R. §1022 (2011).

FR Doc. 2011-18309 (July 20, 2011),

<https://www.govinfo.gov/content/pkg/FR-2011-07-21/pdf/2011-18309.pdf>.

3. Congressional Bills

- H.R. 3235 – 103rd Congress (1993-1994). Available online at <https://www.congress.gov/bill/103rd-congress/house-bill/3235/text>.
- H.R. 1756 – 105th Congress (1997-1998). Available online at <https://www.congress.gov/bill/105th-congress/house-bill/1756/text>.
- H.R. 3162 – 107th Congress (2001-2002). Available online at <https://www.congress.gov/bill/103rd-congress/house-bill/3162/text>.
- H.R. 922 – 116th Congress (2019-2020). Available online at <https://www.congress.gov/bill/116th-congress/house-bill/922/text>.
- H.R. 923 – 116th Congress (2019-2020). Available online at <https://www.congress.gov/bill/116th-congress/house-bill/923/text>.
- S. 2845 – 108th Congress (2003-2004). Available online at <https://www.congress.gov/bill/108th-congress/senate-bill/2845/text>.
- S. 2563 – 116th Congress (2019-2020). Available online at <https://www.congress.gov/bill/116th-congress/senate-bill/2563/text>.

4. Articles

- Agence France-Presse, *Chinese bank banned from operating in US over North Korea ties*, South China Morning Post (November 3, 2017), <https://www.scmp.com/news/china/diplomacy-defence/article/2118225/chinese-bank-banned-operating-us-over-north-korea-ties>.
- Kenneth A. Blanco, FinCEN Director, *Speech delivered at the 2018 Chicago-Kent Block (Legal) Tech Conference*, FinCEN Remarks (August 9, 2018), <https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-2018-chicago-kent-block>.
- Jennifer Shasky Calvery, *Before the United States Senate Committee on Banking, Housing, and Urban Affairs Subcommittee on National Security and International Trade and Finance Subcommittee on Economic Policy*, FinCEN (November 19, 2013),

<https://www.fincen.gov/sites/default/files/2016-08/20131119.pdf>.

Jennifer Shasky Calvery, Director of FinCEN, *Remarks of Jennifer Shasky Calvery, Director, Financial Crimes Enforcement Network at the Florida International Bankers Association Anti-Money Laundering Conference* (February 20, 2014), <https://www.fincen.gov/sites/default/files/2016-08/20140220.pdf>.

Jonathan Chester, *Could The New Financial Action Task Force Regulation Be The End of Bitcoin?*, *Forbes* (August 1, 2019), <https://www.forbes.com/sites/jonathanchester/2019/08/01/could-the-new-financial-action-task-force-regulation-be-the-end-of-bitcoin/>.

David S. Cohen, *Remarks from Under Secretary of Terrorism and Financial Intelligence David S. Cohen on "Addressing the Illicit Finance Risks of Virtual Currency"*, U.S. Department of the Treasury (March 18, 2014), <https://www.treasury.gov/press-center/press-releases/Pages/jl236.aspx>.

Egmont Group, *About*, <https://egmontgroup.org/en/content/about>.

FATF Report, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, FATF (June 2014), <https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>.

Financial Crimes Enforcement Network, *History of Anti-Money Laundering Laws*, <https://www.fincen.gov/history-anti-money-laundering-laws>.

FinCEN Charter, *The Bank Secrecy Act Advisory Group*, FinCEN.gov, <https://www.fincen.gov/sites/default/files/shared/charter.pdf>.

FinCEN Guidance, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies*, FIN-2019-G001 (May 9, 2019), <https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf>.

FinCEN Guidance, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, FIN-2013-G001 (March 18, 2013), <https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf>.

Samuel Haig, *Ordinary Cubans Embrace Cryptocurrency to Bypass Crippling Sanctions*, *Cryptocurrency News*, (September 13, 2019), <https://www.ccn.com/ordinary-cubans-embrace-cryptocurrency-to-bypass-crippling-sanctions/>.

- Samuel Haig, *Venezuelan Petro Against US Sanctions: History and Use of the Crypto*, Coin Telegraph (July 17, 2019), <https://cointelegraph.com/news/venezuelan-petro-against-us-sanctions-history-and-use-of-the-crypto>.
- Steve Hudak, *FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action Against a Virtual Currency Exchanger*, FinCEN Release (May 5, 2015), <https://www.fincen.gov/news/news-releases/fincen-fines-ripple-labs-inc-first-civil-enforcement-action-against-virtual>.
- Information Exchange Working Group (IEWG), Professional Money Laundering Facilitators, Egmont Group Bulletin (July 2019), <https://www.egmontgroup.org/sites/default/files/filedepot/external/20190701%20-%20IEWG%20Professional%20ML%20Networks%20Bulletin%20-%20final.v.pdf>.
- Internal Revenue Service, 4.26.5.2, *History of Bank Secrecy Act*, Internal Revenue Manual (10-03-2012). Available online at https://www.irs.gov/irm/part4/irm_04-026-005.
- Steven Mnuchin, *Remarks of Secretary Steven T. Mnuchin FATF Plenary Session Orlando, Florida*, U.S. Department of the Treasury (June 21, 2019), <https://home.treasury.gov/news/press-releases/sm713>.
- Press Release, *The Effect of Cryptocurrency on Money Laundering*, Market Watch (July 15, 2019), <https://www.marketwatch.com/press-release/the-effect-of-cryptocurrency-on-money-laundering-2019-07-15>.
- Marko Stolle, *Information Exchange on ML/TF Working Group (IEWG)*, Egmont Group, <https://egmontgroup.org/en/content/information-exchange-mltf-working-group-iewg>.
- Heath Tarbert, Chairman, U.S. Commodity Futures Trading Commission (CFTC), Kenneth A. Blanco, Director, Financial Crimes Enforcement Network (FinCEN), Jay Clayton, Chairman, U.S. Securities and Exchange Commission (SEC), Public Statement: *Leaders of CFTC, FinCEN, and SEC Issue Joint Statement on Activities Involving Digital Assets*, SEC.gov (Oct. 11, 2019), <https://www.sec.gov/news/public-statement/cftc-fincen-secjointstatementdigitalassets>.

5. Case Law

In the Matter of: Eric Powers, United States of America Department of the Treasury Financial Crimes Enforcement Network, No. 2019-01, 3 (April 18, 2019), https://www.fincen.gov/sites/default/files/enforcement_action/2019-04-18/Assessment%20Eric%20Powers%20Final%20for%20Posting%2004.18.19_1.pdf.

Printz v. United States, 521 U.S. 898 (1997).

[Abstract]

U.S.A. Anti-Money Laundering Approach to Criminal Use of Virtual Currency

Patricia Ruth McWilliam Lee*

The United States government has been combating money laundering for decades. The most central law related to anti-money laundering is the Bank Secrecy Act. The Financial Crimes Enforcement Network (FinCEN) is one of the main agencies in the fight against money laundering. In 2011, FinCEN amended the definition of Money Services Businesses to include virtual currencies. The law gives FinCEN authority to pursue actions against out-of-the-country entities as long as the financial institutions do business in the United States. FinCEN can seize property located in the United States.

FinCEN recognized that virtual currency could easily be used to launder money because of its anonymous nature. FinCEN works with different American agencies to combat illicit use of funds through registration requirements and encouraging financial institutions to report suspicious behavior. The United States, along with other international organizations, is working to stop criminal activity related to the use of cryptocurrency, especially as it appears that cryptocurrency is increasing in popularity and use worldwide. The government notes that they wish to encourage the use of cryptocurrency and other virtual currencies, but will fight against money laundering to hide illegal activity or enjoy the benefits of illicit behavior.

[Key Words] anti-money laundering, Bank Secrecy Act, cryptocurrency, Financial Crimes Enforcement Network (FinCEN), Internal Revenue Service (IRS), money laundering, money services business, virtual currency

* Associate Attorney at the Law Office of David J. McWilliam in South Carolina, USA, and Former Associate Professor at Konkuk University Law School

