New Payment Methods and Insufficiencies in their Regulatory Scheme

Angel L. Rodriguez Santiago

INTRODUCTION

Money laundering is the process by which individuals who generate money through illicit activities create the perception that their funds derive from legitimate sources. Generally, this entails mixing illegally acquired earnings with money that has been legally obtained. As a result, tracing the source can become difficult, allowing the money to continue through a complex network of transactions. If a person tries to their spend ill-gotten gains without first obscuring its origins, three outcomes are possible: (1) the individual may be liable for unpaid taxes on the earnings; (2) the money may be linked to a crime and the owner subject to prosecution; and/or (3) the money can be seized by the government, if it finds that it was illegally obtained. For these reasons, criminals and their organizations recognize that it is imperative to hide the sources of their illegally acquired money in order to spend it freely, without the risk of loss or prosecution.

By its nature, money laundering is an illegal activity carried out by criminals and occurs outside the traditional scope of economic and financial oversight. Along with other aspects of underground activity, estimates provide the only insight into the magnitude of the problem. The United Nations Office on Drugs and Crime (UNODC) conducted a study to assess the value of illicit funds generated by drug trafficking and organized crime and to investigate the extent to which these funds are laundered. The Report estimates that, during 2009, crime-generated profits amounted to 3.6% of global GDP, and 2.7% (or $1.6 trillion) of these earnings were laundered. The U.S. General Office concedes that, although "there is no way to determine the current amount of money being laundered," it estimates that approximately 100 billion dollars is laundered in the United States annually.

One of the most important reasons justifying this crime is not the act of money laundering itself, but rather its underlying purpose. Criminals launder money in order to have the ability to freely spend the

profits generated from their crimes. Organized crime, drug traffickers, and a wide variety of other criminals, are involved in criminal activities for profit. These same activities generate large amounts of cash money. To eliminate or significantly reduce such criminal activity, the law is responsible for eliminating the underlying cause for the crime, because the easy acquisition of money for expenses is the motivating factor.

New technologies, some of which are currently in various stages of development and testing, will facilitate money laundering. They make it easier to absorb funds into the financial system and to manipulate them in order to hide their origins and subsequent use without raising suspicions. These new methods include electronic cash, also known as "e-cash" or "cybercash," simple online transactions, stored value cards (SVC), smart cards, and online banking. These tools represent a new form of laundering—*cyber money laundering*.

Laundering money in cyberspace adds a new technological perspective to the issue because the money intersects with the much wider terrain of cybercrime. Cybercrime can be defined as an act that is criminal and punishable by law using an electronic device that performs logical or mathematical functions, for example, a computer. Based on this definition, cyberlaundering is *the use of a computer to perform a transaction or relationship involving property or benefits, tangible or intangible, derived from criminal activity*.

This Article aims to evaluate how these new technologies have impacted the traditional money laundering scheme, whether the U.S. legal and regulatory framework is properly addressing it, and if not, what changes or mechanisms should be implemented. Part I discusses different aspects of money laundering, such as its definition, methods, and legal framework. Next, Part II addresses the recent advent of cyberlaundering, its definition, stages, and new methods of payment. Part III then turns to the regulatory scheme for cyberlaundering in the United States to examine its effectiveness, its shortcomings, and alternative approaches that may be used to mitigate money laundering in the United States. In Conclusion, the Article considers the need to implement changes in the current legal and regulatory framework to improve the effectiveness of existing legislation.

I. MONEY LAUNDERING

Legend has it when the notorious Willie Sutton was asked why he robbed banks, he replied, because "*that's where the money was*."[1] He was establishing the obvious—a large part of criminal activity is motivated by financial gain. However, once the money is in the hands of the criminal, the individual has the task of finding a safe way to transfer, spend, or invest it, without alerting the police or tax authorities of the underlying crime. Money laundering solves these problems, and reinforces the key that, at the end of the day, crime pays.[2]

The actual practice of money laundering is as old as crime itself. Yet, the term itself was only recently coined. "Money laundering" first appeared in a newspaper in the 1970s during the Watergate scandal.[3] In turn, the first U.S. court to use the term in a published decision was the Second Circuit Court of Appeals in 1976.[4] Money laundering is also referred to as the "financial facilitation of criminal activity."

A. Definition

There is no universally accepted definition for what constitutes "money laundering." In a classical sense, money laundering refers to a series of acts aimed at concealing the source or possession of ill-gotten gains.[5] In other words, money laundering is the process by which the existence, illegal source, or illegal application of income is concealed

---

[1] Leonard Buder, *Willie Sutton Said It First: 'That's Where the Money Is'*, N.Y. TIMES, Aug. 26, 1979, at 147.

[2] *See generally* NICHOLÁS RODRÍGUEZ GARCÍA & EDUARRDO FABIÁN CAPARRÓS, LA CORRUPCIÓN EN UN MUNDO GLOBALIZADO: ANÁLISIS INTERDISCIPLINAR (2004).

[3] *See* THE WHITE HOUSE TRANSCRIPTS 146, 173 (Bantam Books) (1974).

[4] *See* United States v. Papa, 533 F.2d 815, 822 (2d Cir. 1976) (stating a witness, called "by the Government, gave testimony about a money 'laundering' service he performed for Papa whereby Papa was able to convert millions of dollars of small bills (street money) into large bills").

[5] ISABEL SÁNCHEZ GARCÍA DE PAZ, LA CRIMINALIDAD ORGANIZAD: ASPECTOS PENALES, PRROCESALES, ADMINISTRATIVOS Y POLICIALES 151 (Dykinson 2005) ("Money laundering consists of all those operations carried out to provide the appearance of legality to the assets derived from a crime (e.g. drug trafficking, terrorism, fraud etc.)")

and later disguised to appear legitimate.[6] However, federal statutes that criminalize money laundering proscribe a wide variety of transactions, many of which have nothing to do with the concealment of the proceeds from crime. For example, the mere expense of property derived from criminal activity can be classified as a crime for money laundering, even if the effort to hide or disguise the financial transaction is lacking.[7] Whereas, failing to file a currency transaction report (or "CTR") with a financial institution can give rise to money laundering, even if the subject earnings are derived honestly and not through illicit activities.[8] After the terrorist attacks of September 11, 2001, "money laundering" was expanded in its broadest sense to include economic financing of terrorist groups.

Some U.S. statutes and regulations contain unique definitions for money laundering, such as 18 U.S.C. § 1956, which typifies the laundering of negotiable instruments, and 18 U.S.C. § 1957, which concerns monetary transactions of property derived by illegal activities. Other examples include the Money Laundering and Financial Crimes Strategy Act of 1998[9] and the USA Patriot Act of 2001.[10] The 1998 Act raised the issue of a national strategy to combat money laundering and

---

[6] *See* PRESIDENT'S COMM'N ON ORGANIZED CRIME, INTERIM REPORT TO THE PRESIDENT AND THE ATTORNEY GEN., THE CASH CONNECTION: ORGANIZED CRIME, FINANCIAL INSTITUTIONS, AND MONEY LAUNDERING 5 (1984) (decrying "the virtual impunity with which organized criminal enterprises and their members and affiliates 'launder' the proceeds of their illegal activities through financial institutions in this country and abroad."); *see also* United States v. Heyman, 794 F.2d 788, 789 n.1 (2d Cir. 1986) (adopting the Commission's definition of "money laundering"); United States v. Cuevas, 847 F.2d 1417, 1419 n.2 (9th Cir. 1988); Cuellar v. United States, 553 U.S. 550 (2008) ("[T]aking steps to make funds appear legitimate is the common meaning of the term 'money laundering.'").

[7] *See* 18 U.S.C. § 1957 (2018) ("Whoever, . . . knowingly engages or attempts to engage in a monetary transaction in criminally derived property of a value greater than $10,000 and is derived from specified unlawful activity, shall be punished [by] . . . a fine . . . , or imprisonment for not more than ten years or both.").

[8] *See* 31 U.S.C. § 5324 (criminalizing the act of evading reporting requirements). The CTR is one of the key reports used to detect money laundering.

[9] Pub. L. No. 105-310, 112 Stat. 2941, 2942–47 (1998) (codified as amended in §§ 31 U.S.C. 5340–5342, 5351–5352)

[10] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered sections of 12 U.S.C., 15 U.S.C., 18 U.S.C., and 31 U.S.C.) [hereinafter USA Patriot Act].

other "related financial crimes," defined as (a) the illicit movement of cash or equivalent earnings into, out of, or through the United States, or (b) as defined under state or local law.[11] Meanwhile, the regulations that implement Section 314 of the USA Patriot Act, which established the exchange of information between financial institutions related to money laundering, vaguely define the act as "an activity criminalized by the 18 U.S.C. § 1956 or 1957, or an activity that would be criminalized by 18 U.S.C. § 1956 or 1957, if it occurred within the United States."[12]

B. Scope

The legislation that serves as a deterrent to money laundering is not confined to transactions involving money or cash. For example, many of the requirements for reporting and registering financial institutions also apply to traveler's checks, cashier's checks, money orders, promissory notes, bearer securities and other "monetary instruments."[13] Similarly, the criminal provisions of Title 18, which prohibit financial transactions involving gains from a specific criminal activity, apply not only to cash gains, but to other tangible and intangible assets, including checks, electronic transfers, real estate, automobiles and credits in a bank account.

1. How is money laundered?

Money laundering takes many forms, from simple bank deposits to complex international transactions. Techniques and

---

[11] See 31 U.S.C. § 5340(2) (2018), for a definition of money laundering and related financial crimes as:

> (A) means the movement of illicit cash or cash equivalent proceeds into, out of, or through the United States, or into, out of, or through United States financial institutions, as defined in section 5312 of title 31, United States Code; or
>
> (B) has the meaning given that term (or the term used for an equivalent offense) under State and local criminal statutes pertaining to the movement of illicit cash or cash equivalent proceeds.

[12] *See* 31 C.F.R. § 1010.505(b).

[13] STEVEN MARK LEVY, FEDERAL MONEY LAUNDERING REGULATION: BANKING, CORPORATE AND SECURITIES COMPLIANCE § 1.04 (2d ed., 2017).

methods are constantly evolving as criminals adapt to changes in federal law and regulatory schemes. In addition, because efforts to prevent money laundering in the United States have become more efficient, criminals move to financial institutions in other countries characterized by ineffective regulation and porous borders.

The basic process of transforming illicit funds into assets of legitimate appearance involves three different phases: (1) placement, where the funds are deposited in the financial system; (2) stratification, where the illicit origin is obscured through a series of transactions; and (3) integration, where legal origin is created for the funds, such as the investment in legal assets or the forgery of documents.[14]

a. Placement

This is the initial phase and consists of the introduction of money of illicit origin within the financial system, either through financial institutions or through other more novel means that we will analyze later. In this stage, the money generated physically moves from the scene of the crime and is deposited in financial institutions (usually through structured transactions) or converted into traveler's checks, money orders, or other assets or holdings (e.g. automobiles, houses). Thus, the money is placed within the legal financial trading system. The aforementioned stage is the riskiest for the washer because the funds are still close to their criminal origins. Much of the regulations in the United States are focused on this stage, focusing on, for example, and suspicious deposits.

b. Stratification

The objective of this stage is to erase the trace of the transfer so that it is not possible to link the final funds with the illicit origin of the transfer. At this point what is known as acting in "layers" is carried out, that is, carrying out many transactions of different amounts in order to blur the trace so that it cannot be detected later. Funds are transferred from account to account, institution to institution, country to country, or from one person or corporation to another, to further obscure their

[14] *Id.* § 2.02.

origin and hinder their audit. The funds are distanced from the underlying criminal activity via "layers" of financial transactions.[15]

The more numerous the transfer or "layers," the greater is the difficulty in identifying the washer. The launderer will proceed to mix illicit business profits with those of licit businesses, buy and sell movable and immovable assets with the illicit money, and buy financial instruments with the money already deposited in the bank. The idea is to create a network of transactions that distract the authorities from the moment in which the origin of the money was legitimized to insert it into the financial system.

c. Integration

The objective of this last phase, of integration, consists in achieving the legal acceptance and integration of criminal capital in a more definitive manner, being recorded by means of accounting and tax records, thus giving them legal form and appearance. Once the purpose is achieved, it is difficult to detect unless there is a large discrepancy between the employment, the business and the legitimate investments of a person or company due to the illegitimate assets.

It is in this phase in which the launderer increases his wealth with the proceeds of crime, pretending the lawfulness of the money that has been obtained illegally by re-entering the economy with commercial transactions that appear to be normal. For example, money can be used to purchase legitimate third-party assets. Likewise, fictitious invoices, loan documentation, financial statements or contracts can be created to provide an apparent legal source for them. At this point, the proceeds are available to the criminal to promote more criminal activities, acquire other assets, or sustain a lifestyle of luxury.[16]

C. Money Laundering's Legal Framework

The purpose of the federal anti-money laundering regulation is to recruit financial institutions in the fight against crime. Financial institutions have the obligation to report all suspicious activity and

[15] *Id.*
[16] *Id.*

large cash transactions, keep a record of transfers and purchases in cash of negotiable instruments, operate robust anti-money laundering programs and customer identification programs, and refuse to engage in transactions that involve criminal profits.[17] Next, we will discuss several of the most important legal statutes that regulate this crime:

1. Bank Secrecy Act

In 1970, Congress passed the Bank Secrecy Act (BSA) with the intent of assisting U.S. authorities to detect, investigate and prosecute financial crimes.[18] The BSA requires financial institutions to submit transaction reports and create a cash trail of client transactions. The idea is that, by following the money, the investigators could trace the crimes from which the money was derived and punish the criminals. Over the years, Congress expanded the BSA to include other types of financial institutions, such as casinos and brokerage firms.[19]

The BSA is codified as amended throughout scattered sections of 12 and 31 U.S.C. as follows: 12 U.S.C. § 1829b (retention of records by the insured depository institution); 12 U.S.C. §§ 1951-1959 (maintenance of financial records); 31 U.S.C. §§ 5311-5332 (registers and reports on monetary instrument transactions). Initially intended to target reports or records with "a high degree of usefulness in criminal, tax, or regulatory investigations," the BSA was amended following the terrorist attacks of September 11, 2001 to include reports and records useful in "the conduct of intelligence or counterintelligence activities, including analysis, to protect against of international terrorism."[20]

2. Comprehensive Crime Control Act of 1984

The Comprehensive Crime Control Act of 1984 (CCCA)[21] was a crime control measure that reviewed the federal sentencing system and bail and confiscation procedures. Chapter IX of the CCCA

---

[17] *Id.* § 3.01.

[18] Bank Secrecy Act of 1970 (BSA, Pub. L. No. 91-508, 84 Stat. 1114 (1970) (codified as amended in scattered sections of 12 U.S.C., 15 U.S.C., and 31 U.S.C.).

[19] *See* LEVY, *supra* note 13.

[20] *See* 31 U.S.C. § 5311.

[21] Pub. L. No. 98-473, 98 Stat. 2135 (1984).

stiffened the civil and criminal penalties of the BSA and amended other provisions of the BSA. Among other things, it also:

(1) increased the notification requirements for cross-border currency transport (CMIR) from $5,000 to $10,000 to focus the application of the law on relatively large transactions;[22]
(2) added subsection (b) to 31 U.S.C. § 5317, which authorizes border searches without search warrants for persons, vehicles and containers entering or leaving the United States;
(3) Increased the maximum civil penalty for a voluntary breach of BSA from $1,000 to $10,000;[23]
(4) increased the maximum penalty for a voluntary BSA violation of $1,000 for a misdemeanor of one year to $250,000 for a five-year offense;[24] and
(5) amended the Racketeer Influenced and Corrupt Organizations Act (RICO) to make a BSA Title II violation a felony under RICO.[25]

3. Money Laundering Control Act of 1986

The Anti-Drug Abuse Act of 1986 was a comprehensive law that contained 15 titles dealing with every facet of the war on drugs.[26] Title I, subtitle H, entitled "Money Laundering Control Act of 1986" (MLCA), strengthened the BSA and proscribed money laundering as a federal crime.[27] The MLCA closed an important gap that existed with respect to the notification of monetary transactions, by prohibiting the of "structuring" transactions for the purpose of evading CTR reporting requirements.[28]

The MLCA made money laundering a federal criminal offense by adding articles 1956 and 1957 to title 18 of the United States Code. These important provisions were based on evidence before Congress showing that no matter how many times the BSA was amended, or how

[22] *See* 31 U.S.C. § 5316(a) (2018).
[23] *See id.* § 5321(a).
[24] *See id.* § 5322(a).
[25] *See* 18 U.S.C. § 1961(1)(E).
[26] Pub. L. No. 99-570, 100 Stat. 3207 (1986).
[27] *See id.* §§ 1351–1367 (codified as amended at 18 U.S.C. §§ 1956–1957).
[28] U.S. GEN. ACCOUNTING OFFICE, MONEY LAUNDERING: THE U.S. GOVERNMENT IS RESPONDING TO THE PROBLEM, GAO/NSIAD-91-130, 13 (1991).

rigorously it applied, "only a substantial ban on the act of money laundering will deter and significantly reduce it."[29]

Section 1956 proscribes as a felony the act of to carrying out (or attempting to carry out) a wide range of financial transactions or cross-border transmissions of funds involving products of "specified unlawful activity" with the intention to promote said specific illegal activity or with the knowledge that the transaction was designed to conceal or conceal the profits or to evade the requirement to inform it.[30]

Section 1957 makes it a felony for any person to carry out or attempt to make a "monetary transaction" in which he or she is aware that it involves gains derived from a crime. The Public Ministry only has to prove the person tried to spend or spent money from a criminal activity of which he was aware or reasonably should have been aware.[31]

Section 1956 possesses more subjective elements than Section 1957. The former requires that it be shown that the defendant intended to promote the specific illegal activity that generated the proceeds of the laundering or had the knowledge that the transaction was designed to conceal or conceal the profits or to evade the requirement to inform them. The latter requires only the expenditure of money (or its intent) that the defendant knows has come from a criminal activity, the intention of spending being an objective criterion. Therefore, it is more convenient for the public prosecutor's office to charge the money launderer with Section 1957 because it requires proving fewer elements than Section 1956.

Section 1956 establishes a criminal penalty of $500,000 or twice the value of the assets involved in the transaction, whichever is greater, and a penalty of imprisonment of up to 20 years (compared to five years for most white collar crimes); and a civil penalty of $10,000 or the value of the transaction, whichever is greater. The maximum prison sentence for a violation of Section 1957 is 10 years. The prison term mandated by Section 1957 is less than that of Section 1956 because, as already mentioned, there are fewer subjective elements that must be proven.

With the adoption of sections 1956 and 1957, the United States became the first country in the world to establish money laundering as

---

[29] S. Rep. No. 99-433, at 3 (1986).
[30] 18 U.S.C. § 1956 (2018).
[31] *Id.* § 1957.

a crime. Other nations followed the example of the United States, promulgating similar laws. The MLCA was also the precursor to the 1988 U.N. Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, the first and most important anti-money laundering initiative at the international level.[32]

4. Money Laundering Prosecution Improvements Act of 1988

The 1988 Money Laundering Prosecution Improvements Act (MLPIA) focused on addressing some of the perceived weaknesses of the BSA.[33] The legislation sought to reinforce the BSA in several ways. First, the MLPIA expanded the definition of "financial institution" to include (1) businesses engaged in automobile, airplane, or boat sales, (2) persons involves in the real estate industry, (3) the United States Postal Services (USPS), and (4) any other businesses designated by the Secretary of the Treasury Department "whose cash transactions have a high degree of utility in criminal, fiscal or regulatory matters."[34] Second, Congress required sellers of bank checks, cashier's checks, traveler's checks and money orders to verify and maintain records of the identity of persons other than regular customers who purchase said instruments in amounts of $3,000 or more.[35] Third, it raised the civil liability to $10,000 for anyone who intentionally or grossly neglects the reporting requirements imposed by the BSA.[36] Lastly, the MLPIA added new offenses to the "specified unlawful activities" list,[37] and authorized undercover police officers to present themselves as figures from the underground world to catch the cleaners and money in operations (also known as "sting operations"), using money from public funds instead of actual illicit income.[38]

---

[32] *See* LEVY, *supra* note 13, § 29.02.

[33] Pub. L. No. 100-690, §§ 6181–6187, 102 Stat. 4181, 4354–59 (1988) (codified as amended in scattered sections of 12 U.S.C., 18 U.S.C., and 31 U.S.C. (2018)).

[34] *See* 31 U.S.C. §§ 5312(a)(2), 5312(a)(2)(T)–(U), (Z).

[35] *See id.* § 5325.

[36] *See id.*

[37] *See* 18 U.S.C. § 1956(c)(7).

[38] *See* 8 U.S.C. § 1956(a)(3). A "sting operation" is a deceptive law enforcement operation designed to catch a suspect in the act of committing a crime. In practice, either a police officer, law enforcement agent, or cooperating witness will play the

5. Annunzio-Wylie Anti-Money Laundering Act

The current U.S. regime against money laundering was largely incorporated via the Annunzio-Wylie Anti-Money Laundering Act.[39] Several of the elements the Act incorporated are the requirements that financial institutions present reports of suspicious activity (SARs), establish and maintain compliance programs to guard against money laundering, and maintain records of domestic and international funds transfers.[40] The Act also granted the authority to revoke a bank's letter and to terminate one's deposit insurance based upon the conviction of an offense for money laundering.

6. USA Patriot Act

Title III of the USA Patriot Act included several provisions to fight international money laundering through the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001.[41] Among the most important provisions are:

(1) *Customer Identification* – Section 326 requires the Treasury Department and appropriate regulators to issue regulations that establish standards to identify customers who open accounts at financial institutions.
(2) "*Shell Banks*" – Section 313(a) prohibits U.S. financial institutions from providing correspondent accounts in the United States to foreign banks that do not have a physical presence in any country (*i.e.*, "shell banks").[42]
(3) *Due Diligence in Correspondent and Private Banking* – Section 312 requires all national financial institutions that maintain a private bank account or a correspondent account in the United States for a non-US person to establish due diligence procedures

role of a criminal partner or potential victim and go along with the acts or omissions of a known suspect in order to gather evidence of the suspect's criminal conduct.

[39] Pub. L. No. 102-550, §§ 1500–1565, 106 Stat. 3627, 4044–74 (1992) (codified as amended in scattered sections of 12 U.S.C., 18 U.S.C., and 22 U.S.C. (2018)).

[40] *See* 31 U.S.C. § 5318(g), (h); *see also* 12 U.S.C. § 1829b(b)(2), (3).

[41] USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered sections of 12 U.S.C., 15 U.S.C., 18 U.S.C., and 31 U.S.C.).

[42] *See* 31 U.S.C. § 5318(j).

designed to allow the institution to detect and report cases of money laundering through those accounts.[43]

(4) *Exchange of Information* – Section 314 requires the Treasury Department to enact regulations that encourage the exchange of information between the government and financial institutions, and between financial institutions themselves, for the purpose of detecting and discouraging money laundering and terrorist acts.[44]

(5) *Anti-Money Laundering Programs* – Section 352 (a) amended Article 5318 (h) of the BSA to require all financial institutions to establish a program against money laundering.[45]

II. WHAT IS CYBERLAUNDERING?

As noted, cyber money laundering is the use of a computer to form a transaction or relationship involving property or benefit, tangible or intangible that is derived from a criminal activity.[46] It can also be defined as the process of using payment systems based on emerging technologies in money laundering schemes.[47] Emerging technologies have created the conditions for developing and transmuting traditionally used money laundering schemes to incorporate ingenious and innovative methods. The term was introduced almost two decades ago to describe money laundering using the new payment systems.[48]

Understanding the concept of cyber money laundering presupposes understanding how the traditional form of money laundering has evolved with new technologies. This phenomenon originated and heightened with the advent of the Internet, a platform that has served as a great utility for criminals to carry out their money laundering schemes. Current computers are designed to process data at

---

[43] *See id.* § 5318(i).

[44] *See* USA Patriot Act § 314.

[45] *See id.* § 352 (a).

[46] Daniel Adeoyé Leslie, *Legal Principles for Combatting Cyberlaundering*, *in* LAW, GOVERNANCE AND TECHNOLOGY SERIES, at 56 (Springer Int'l Publ'g Switz., Vol. No. 19, 2014).

[47] *Cyberlaunderers: A First Look*, Money Laundering L. Rep., Mar. 1997, at 1.

[48] Wendy J. Weimer, Note & Comment, *Cyberlaundering: An International Cache for Microchip Money*, 13 DePaul Bus. L. J. 199, 199 n.1 (2001).

high speeds due to advances in the field of microprocessor optimization and the increasing processing capacity of CPUs.[49]

The increasing capacities of computers and devices have catalyzed new ways to carry out money laundering schemes. However, the determining factor in cyber money laundering is the growing access to the Internet. According to the website Internet World Stats, as of August 31, 2019, there are approximately 4.5 billion Internet users in a world of 7.7 billion inhabitants.[50] That is, almost half of the world has access to the Internet.

A. Why Does the Internet Attract Money Launderers?

The mode and stages of cyber money laundering are the same as those of money laundering that we discussed in Chapter 1 of this writing. A process of *placement*, *stratification* and *integration* takes place using virtual platforms. The internet has the function of facilitating this process thanks to the following factors.

1. Anonymity

One of the most important factors in the use of the internet as the main vehicle for money laundering is the anonymity it confers on its users. Anonymity is a specific aspect of privacy. These new technologies can allow large-scale transactions to be carried out anonymously and for such transactions to be carried out without the participation of traditional financial institutions. This factor has always been in contention and is debated, since it directly conflicts with the fundamental right to freedom of expression and privacy of individuals.[51] The balance between the anonymity provided by the new technology and the right of the government to have knowledge of the transactional flow in the networks will be complicated by the desire of legitimate users of these technologies to maintain their right to privacy.

---

[49] *See* Leslie, *supra* note 46, at 55. A CPU is the "central processing device" of a computer. This component determines the velocity by which data is processed.

[50] *See* Usage and Population Statistics, INTERNET WORLD STATS, http://www.internetworldstats.com/stats.htm (last visited Aug. 31, 2019).

[51] *See* Leslie, *supra* note 46, at 59.

Anonymity in public areas is fundamental for a healthy democracy.[52] The Supreme Court of the United States has reiterated this notion in multiple instances.[53] Because anonymity is an important component of freedom of expression and intimacy, the debate about anonymity on the Internet is, to some extent, a debate about political and social freedoms in a democratic society.[54] Anonymity is a necessary component in the ability of people to form ideas outside the watchful eye of their neighbors.[55] The lack of anonymity threatens the ability of people to challenge dominant authority or paradigms. The vision of the minority and diverse thinking are the fuel that drives the engine of a pluralist society. The expansive democratic market of ideas will be reduced to a corner shop if people are not allowed to freely try all the products and contribute with new ones.[56]

The ability to maintain anonymity on the Internet poses challenges and questions that are not addressed in other situations. If everyone communicates anonymously in cyberspace, how can we achieve public policy objectives, such as protecting minors from harmful content, preventing financial fraud or preventing copyright infringement? The application of these policies is based on the ability to identify and punish the perpetrator. These problems will only get worse as we expand the uses of the internet and depend more on cyberspace. Certainly every "real world" activity that we export to cyberspace will have its own unique problems and challenges. Anonymity will only complicate these challenges. However, for the reasons stated above, anonymity is an essential tool to protect freedom

---

[52] *See* Hiram A. Melendez Juarbe, *La Constitución En Ceros y Unos*, 77 Rev. Jur. U.P.R. 45, 53 (2008).

[53] *See, e.g.*, Talley v. California, 362 U.S. 60 (1960); McIntyre v. Ohio Elections Comm., 514 U.S. 334 (1995); Watchtower Bible & Tract Soc'y of New York, Inc. v. Vill. of Stratton, 536 U.S. 150 (2002).

[54] *See* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 Iowa L. Rev. 497, 500–01 (1995) ("In democratic society, information standards reflect specific conceptions of governance. . . . For private interactions and the relationship between citizens, both law and practice set the balance between dignity and free flows of information.").

[55] *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stan. L. Rev. 1373, 1427 (2000).

[56] *See McIntyre*, 514 U.S. at 343.

of expression and actions carried out on the Internet, even when the responsibility is marginally diminished.[57]

The conception that we have of the right to privacy to expectations of privacy, secrecy, loneliness, or the idea that we do not have constitutional rights over the information that we decide to reveal to the public, as is the case of the doctrine of searches and searches,[58] we could ignore threats that modern technology presents to civil rights.[59] An example of this is the collection of transactions carried out by individuals on the Internet and outside cyberspace by private entities and the government, as well as the collection, accumulation and classification of this information with the purpose of creating public and private profiles.[60] Other examples are the technological mechanisms used by the government that have the effect of sacrificing privacy at the expense of the defense of other public interests: (1) electronic surveillance in public places; (2) facial recognition technology; and (3) government and private databases.[61]

2. Speed

The speed with which transfers are carried out is another of the main attractions of this medium. As already mentioned, the increasing processing capabilities of computers and devices have influenced the speed of transactions carried out in cyberspace.[62] They also allow launderers to move funds quickly within a country or across the world. In addition, they make the process less expensive.

3. Untraceable Transactions

As we will discuss later, many of the mechanisms used to launder money in cyberspace have processes to hide the track of

---

[57] Shawn C. Helms, *Translating Privacy Values with Technology*, 7 B.U. J. Sci. & Tech. L. 288, 305 (2001).

[58] DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (N.Y. Univ. Press 2004).

[59] Melendez Juarbe, *supra* note 52, at 60.

[60] *Id.* at 6.

[61] *Id.* at 13.

[62] *See* Leslie, *supra* note 46, at 56–57.

transactions, making it easier for money launderers to work.[63] Currently, by way of example, the structure of IPv4 allows users to create false return addresses in the data packets, making some communications virtually impossible to track.[64]

4. Ability to Transfer Unlimited Value

Some of the means used to launder money on the internet do not have a limit of value, holding any amount of cash.[65]

5. No Face to Face Contact

This is known as the depersonalization of financial operations. When we use any of the financial services available on the Internet, we actually use our computer and it is the software that connects to the bank's server. The whole process of placing orders or making requests and executing them is totally or partially automatic without the presence of a human factor. So, we can pretend to be someone else every time we access the bank through cyberspace. The server of the financial institution checks only two things: the login (e.g., the unique identification number) and the password, not the true identity of a client. If the information is correct (that is, the same as that stored in the server's memory), access is granted. As a result, it would be more difficult to detect and stop transactions related to money laundering activities.[66]

6. Cross-border activity

The address of the online service provider is usually different from where the servers are actually located, or from where these servers

---

[63] Sarah N. Welling & Andy G. Rickman*, Cyberlaundering: The Risks, the Responses*, 50 Fla. L. Rev. 295, 310 (1998).

[64] David P. Hamilton, *Making Net Less Vulnerable Not an Easy Task*, CHI. TRIB. (Feb. 21, 2000), https://www.chicagotribune.com/news/ct-xpm-2000-02-21-00022 10167-story.html.

[65] *See* Weimer, *supra* note 48, at 221 ("The cyberstream provides the perfect instrumentality to launder this money due to the speed of the transaction, its security by means of anonymity, and the unlimited amount that can be transferred.").

[66] *See id.* at 223.

are administered or from where the client accesses the Internet.[67] New payment technologies allow us to conduct business between different countries and, therefore, across several legal systems. This means that several jurisdictions will be involved in the event of a crime being carried out. Cooperation in applying legal regulations and sanctions to is one of the great challenges despite the existence of many international treaties and conventions.

B. Stages of Cyberlaundering

As discussed *supra* in Part I.B.1, the three stages of traditional money laundering are placement, stratification, and integration. Yet, cybernetic money laundering substantially alters these stages due to the configuration of the scheme and the factors mentioned in the previous chapter.

1. Placement

In traditional money laundering, this stage is characterized by having the money in cash, either by depositing them in a financial institution, smuggling cash or buying high-value products. In the case of cyber money laundering, cash can be deposited through an unregulated financial institution that issues smart cards or deposited by "smurfs" using ATMs with the deposit function.[68] However, in the case of cybercrime there is no need to go through this stage, given that the money or equivalent value already has an electronic form and exists in cyberspace.[69] Some examples of this are internet fraud, identity theft schemes and false financing opportunities. This stage is distinguished from traditional money laundering by the use of technological methods both to transmute cash into virtual value, and to store value of illicit activities carried out on the Internet.

---

[67] *See id.*

[68] "Smurfing" is the practice of depositing sums of cash in small amounts to avoid risk controls.

[69] *See* Wojciech Filipkowski, *Cyberlaundering: An Analysis of Typology and Techniques*, 3 INT'L J. CRIM. JUST. SCI. 15, 20 (2008).

2. Stratification

In traditional money laundering, stratification refers to the process by which the washer transfers funds obtained from illicit activity and placed in a financial institution to various accounts between different institutions to obscure its origins. This second stage of the traditional money laundering process is the one that benefits the most from online services. Cyberspace provides the money launderer with the most important tools in this stage: anonymity, speed and distance of criminal activity. For example, one can create many internet accounts that have the function of hiding the identity of the client in addition to not require recurring income, which becomes an important element when one uses students or unemployed people as "Smurfs", or open an account in a foreign bank, if the law allows it.[70] One can also collect bank accounts and control them through a personal computer; this is done by creating an extensive transactional track in a short period of time by means of instantaneous domestic transactions or in several jurisdictions, making it difficult for the authorities to follow the track.

3. Integration

The last stage is intended to make gains derived from criminal activity appear as legitimate. One of the most effective ways to do this is to establish an online service company. The offering of online services, whether true or false, provides legitimate income.[71] The service can be of games of chance or betting, among others, but the same will never be realized, there being no net earnings paid to the account. The payment would appear as profit on the books of the internet service company. Therefore, the owner's profits would appear as legitimate and the product of his own company.

C. New Payment Methods in the Cyberspace

Although there is not a universal definition of payments in cyberspace, they can be described as payments that facilitate the

[70] *See id.*
[71] *See* Leslie, *supra* note 46.

transfer of financial values via the internet.[72] The terms digital currency or electronic money only encompass a small fraction of the transactional universe provided by cyberspace. Technology has significantly altered the way we conduct business and transfer money. Despite these benefits, it should be remembered that the internet is a neutral technological instrument; it can be used for positive or negative activities. Consequently, the internet has provided space for money launderers to have access to agile and effective tools when laundering large amounts of capital. At the same time, transactions occur in anonymity and in an impersonal environment, restricting the investigative capacity of the authorities since they are devoid of the necessary information to detect illicit activities.

The Financial Action Task Force (FATF), an independent intergovernmental body aimed at developing and promoting an international financial system against money laundering, published in 2010 a study detailing the "New Methods of Payment" (or "NMP") used.[73] The NMP can be divided into the following methods:

1. Internet Payment Services

The term "internet payment services" is used to refer to (1) payment services that depend on the use of a bank account and the use of the internet as a mechanism to transfer funds to or from the bank account; and (2) payment services provided by non-banking institutions that operate exclusively on the Internet and are only indirectly associated with banks.[74] The second mode is the most exploited by the washers, since they use companies that provide electronic money ("electronic cash" or "e-cash") to their customers. This mechanism has the effect of replacing cash. The value is stored in a computer and transferred between different computers through the internet for the purchase and sale of products.

---

[72] *See* ROGER C. MOLANDER ET AL., CYBERPAYMENTS AND MONEY LAUNDERING. PROBLEMS AND PROMISE., CRITICAL TECH.INST., RAND (1998), https://www.rand.org/content/dam/rand/pubs/monograph_reports/1998/MR965.pdf.

[73] FINANCIAL ACTION TASK FORCE, MONEY LAUNDERING USING NEW PAYMENT METHODS (2010), http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf [hereinafter FATF REPORT].

[74] *Id.* at 99.

2. Stored Value Cards

The stored value cards (SVCs), also known as smart cards, prepaid cards or "e-purse," are cards that have "the capacity, through the use of a band magnetic, computer chip or other means, to deposit and withdraw value from the card so that the value is stored and removed from the card by the use of appropriate terminal devices by a merchant or other beneficiary."[75] They are usually low-value cards, such as phone cards, that allow money to be stored on the card and then removed without a third party acting as an intermediary. Theoretically, these cards can be programmed to store billions of dollars. However, many stored value card programs impose a limit on the amount of value that can be stored on an individual card.[76]

3. Mobile Payments

Mobile payments can be described as payments made through the use of services through mobile phones or other communication tools.[77] Payments are initiated by voice commands, text messaging protocols, or wireless application protocols (WAP). The latest technology in mobile payments is near field communication. Near-field communication (NFC) works by combining two electronic devices, usually a mobile device, such as a smartphone and a reader of some type. NFC technology always involves an initiator that generates a radio frequency field to feed a passive vessel. In terms of payment technology, the reader would be the initiator and the smartphone (containing the stored credit card information) would be the target.[78]

---

[75] Robert J. Egan, *Banking in Cyberspace: Smart Cards and Electronic Money*, PLI/CORP., Nov.-Dec. 1995, at 477.

[76] *See* FATF REPORT, *supra* note 73, at 72.

[77] *See id.*

[78] See Andrea Meola, *Mobile Payments Technology and Contactless Payments Explained*, BUS. INSIDER (Dec. 21, 2016, 3:13 PM), for a detailed explanation of the technology.

D. New Payment Methods and their Risks

The FAFT establishes that the NMP, like any product and financial service, can be abused for money laundering purposes.[79] However, when NMP providers are subject to anti-money laundering obligations and appropriately supervised for this purpose, transactions using the aforementioned mechanisms tend to be more transparent and help prevent corruption and other abuses. The lack of enforcement of these obligations, the lack of regulations aimed at dealing directly with cyberlaundering, and the ease with which new money-laundering methods are provided aggravate the situation and allow more money launderers to opt to use cyberspace every day.

The FAFT published in June 2013 a study entitled "Guidance for a Risk Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Services" (or "NMP Guides").[80] The purpose of the NMP Guides is to provide parameters for a risk-based approach when taking anti-money laundering measures and to regulate new payment methods, with special attention to prepaid cards, mobile payments and internet payment services.[81] The study took the recommendations of the report issued in 2010 and implemented a series of guidelines for the regulation of all those financial institutions included within its definition. The report details the risks of each of the new payment systems mentioned above:

1. Prepaid Cards

Prepaid cards were introduced to the market in the 90s as the alternative to debit and credit cards. They started as a device used to pay for goods and services where the issuer did not need to perform any analysis on the credit card holder's credit position, or deal with the costs of opening and further management of a payment account. Nowadays, many prepaid cards can be used to withdraw cash from

---

[79] *See* FATF REPORT, *supra* note 73, at 72.

[80] FINANCIAL ACTION TASK FORCE, GUIDANCE FOR A RISK-BASED APPROACH: PREPAID CARDS, MOBILE PAYMENTS AND INTERNET-BASED PAYMENT SERVICES (2013), http://www.fatf-gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf [hereinafter FATF GUIDANCE].

[81] *Id.* at 2.

ATMs, and some of them contemplate the possibility of transfers from person to person.[82]

The prepaid cards can be divided into two categories: either "open-loop" or "closed-loop." A closed-loop card, also referred to as a single-purpose card, is a credit card or gift card that a consumer can only use to make purchases at a single company. This type of card bears the logo of the company that issues it, indicating where it can be used, but the card lacks the logo of a payment processor, such as Visa or MasterCard, and cannot be used for general purchases.[83] Closed-loop prepaid cards are not subject to extensive analysis, as they have a very limited negotiability. This does not mean that they have a lower money laundering risk, but that in most cases they are not used as payment methods. To illustrate this modality, the FATF in its 2010 NMP report details a case in which three defendants were prosecuted for buying closed-loop prepaid gift cards with information from stolen credit card accounts. The defendants used the gift cards to buy merchandise, which they then returned to the store in exchange for new gift cards or sold the merchandise in cash. Because the new prepaid cards were not linked to the numbers on the stolen credit cards, they were not affected when the credit card theft was discovered.[84] On the other hand, open-loop cards are those in which we typically think when we think of a credit card and have the important payment processor logo indicating that it can be used in almost all parts of the world.

a. Open-loop Prepaid Cards

When we speak of open-loop prepaid cards we refer to credit cards, debit cards or gift cards that a consumer can use to make purchases anywhere a card is generally accepted. An open-loop card bears the logo of a major credit card company: Visa, MasterCard, American Express or Discover. These cards are much more useful than closed circuit cards, such as store gift cards or store credit cards, which

[82] *Id.* at 5.

[83] *See* Julia Kagan, *Closed Loop Card*, INVESTOPEDIA, http://www.investopedia.com/terms/c/closed-loop-card.asp-0 (last updated Apr. 11, 2019).

[84] *See* FATF REPORT, *supra* note 73, at 14.

can only be used in a single store or a small group of stores owned by the same company.[85]

Open-loop prepaid cards[86] are used to quickly move cash around the world using the ATM system for the withdrawal of funds, without requiring a face-to-face transaction. The global network (VISA, MasterCard) can limit the use of prepaid cards to certain jurisdictions or regions, but most business models of open-loop prepaid cards are designed to operate globally.[87] In addition, this payment method has the least use limit, since it is based on comprehensive infrastructures used for payment transactions, including the global ATM network and a high number of accepting merchants and points of sale (POS).[88] The Federal Reserve estimated that in 2006 there were about 13.3 billion dollars in purchases with prepaid open-loop cards compared to $ 2.4 billion in purchases with credit cards.[89]

b. Stored Value Cards

For prepaid cards there is a risk of anonymity that can occur when the card is purchased, registered, loaded, recharged, or used by the customer. This risk is related to the functionality of the card and the existence of prevention measures that we will discuss later. In addition, open-loop cards usually allow customers to make payments in domestic as well as foreign locations through a global payment network. This, added to the physical size of them, makes them vulnerable to the misuse that criminals can give them, since instead of cash they will become a method of physical exchange across the most attractive border. Another element is the risk of allowing the cash financing of prepaid cards. The criminals would wash the proceeds of the crime in cash through this function, inserting those profits into the legal financial system through prepaid cards.

---

[85] *See* Troy Segal, *Open Loop Card,* INVESTOPEDIA, https://www.investopedia.com/terms/o/open-loop-card.asp (last updated July 16, 2019).

[86] *See* FATF REPORT, *supra* note 73, at 115.

[87] *See id.* at 29.

[88] *See id.* at 30.

[89] *Id.* at 76.

2. Mobile Payments

The mobile payment system[90] available today is the product of an evolutionary process that began with the spread of the telephony industry around the world in the late 1990s. Mobile payments (also known as "m-payments") are generally defined as the use of a mobile phone to credit, send, receive or transfer money or digital value. Today, 1.5 billion people have direct access to financial services, but there are more than 5 billion cell phones. It is estimated that in the next five years there will be almost the same number of mobile subscriptions as there are people on the planet.[91]

Mobile payment systems establish relationships with their customers through agents, online or through the mobile payment system itself. The problem of anonymity arises when the mobile payment service is used or recharged. In addition, these services can be used to transfer funds globally, a function that appeals to criminals. Finally, mobile payment services allow accounts and transactions to be financed in different ways, including cash financing through different agents. The latter creates a high risk of money laundering because the origin of this type of transactions remains hidden. The 2008 World Bank report also provides four factors that increase the risk of this type of payment method: anonymity, speed and little supervision.[92]

3. Internet Payments Services

The internet opened the world of electronic commerce and established a series of payments based on cyberspace. The internet provides a series of services that allow customers to access accounts that can be used to transfer electronic money or the value they hold to other individuals or businesses that also have accounts from the same provider.[93] The term "Internet payment services" (IPS) is generally used to describe bank style transfers and other types of payment services offered by non-banking institutions that operate exclusively on the internet and are only indirectly associated to banks.

---

[90] *See* FATF GUIDANCE, *supra* note 80, at 6–7.
[91] *See id.* at 37.
[92] *See* FATF REPORT, *supra* note 73, at 13.
[93] *See id.* at 9.

IPS related to bank accounts make similar transfers to the operation of a bank, the only difference being that the client is in front of his computer and not in the bank's offices. Non-bank PHIs, such as the PayPal platform, offer clients a range of services to finance money transfers across national borders, online purchases or participation in online auctions.[94]

Online payment services, for the most part, do not incur face-to-face contact with the customer. This increases the possibilities of identity fraud or of clients who provide false information to cover up any illegal activity. On the other hand, online payment service platforms that allow financing from third parties with funds of unknown origin increase the risk of money laundering. Internet payment services that handle all aspects of the relationship between customers (e.g., registration, cash-in/cash-out and transactions) and are subject to anti-money laundering requirements present a lower risk than decentralized services.

E. Recommendations to Minimize Risks

The FATF issued a series of recommendations to address money laundering in emerging technologies and payment methods.[95] The measures are aimed at creating a balance between the need to avoid the misuse of these new technologies and provide customers with the easy use that characterizes and is largely the reason for using these mechanisms:

1. Customer Due Diligence

Customer due diligence (CDD) is an effective measure to mitigate the money laundering risks that the new payment methods represent. The CDD requires financial institutions to have an obligation to identify and verify the identity of their clients. The greater the functionality of the new payment method, the greater the need for a better CDD. Prepaid cards and mobile payment services are distributed

[94] COUNCIL OF EUROPE (COE), MONEYVAL, CRIMINAL MONEY FLOWS ON THE INTERNET: METHODS, TRENDS AND MULTI-STAKEHOLDER COUNTERACTION (2012), https://rm.coe.int/research-report-criminal-money-flows-on-the-internet-methods-trends-an/168071509a.

[95] *See* FATF GUIDANCE, *supra* note 80, at 23.

through a network of service providers that would use CDD measures during face-to-face interaction. ISPs usually establish their relationship with their customers through the internet and digital accounts are financed through the same channel. ISPs are forced to implement CDD measures using the internet.[96]

2. Value, Financial and Geographical Limitations

Setting limits to new payment methods can be an effective mechanism to mitigate money laundering risks as long as it is combined with other measures such as the monitoring of accounts and transactions and the reporting of suspicious transactions. Many of the prepaid card programs already contemplate setting limits on financing and storage limits to ensure they are not used for money laundering. In terms of mobile payment services limitations are imposed on the amount of money or value that can be stored in a mobile payment account; about the maximum value allowed in each transaction, including cash withdrawals; and in the frequency of transactions allowed per day, week, month or year. ISPs should be considered case by case, since the restrictions vary depending on the digital currency.[97]

3. Origin of Financing

Suppliers of new payment methods should consider the source of financing when measuring the risk of being used for money laundering. They should consider restricting the sources allowed for the financing of said product. If the individual wishes to add cash value to the new payment method, the service provider must require the person to identify if the cash exceeds a limit established for an individual account or the number of transactions per day.[98]

4. Record Keeping, Transaction Monitoring and Reports

Record keeping is one of the most important anti-money laundering efforts and provides support for police investigations. At a

[96] *Id.* at 21–22.
[97] *Id.* at 22–23.
[98] *Id.* at 24.

minimum, the transaction record must contain the information identifying the parties to the transaction, the accounts involved, the nature and date of the transaction, and the amount transferred. The electronic nature of the new payment methods provides a solid basis for effective transaction monitoring and monitoring. It is recommended that providers maintain transaction records and customer information for a minimum of five (5) years.[99]

With regard to mobile payments, the telephone number of the sender and the recipient and the information on the SIM card must be stored in the register. The record could also include information on the exact location of the sender and the recipient. Depending on the size and nature of the transaction, registration of the transaction can be an important component.

III. ANTI-MONEY LAUNDERING REGULATION OF NEW PAYMENT METHODS IN THE UNITED STATES

A. Current U.S. Regulation of NMPs

The regulation of NMP represents a challenge for the United States. While other countries have created specialized agencies to address the regulatory scheme that governs these innovative payment systems, the United States continues to use the legal concepts of traditional systems. This gap between recent payment systems and existing legislation causes the U.S. judicial system, using its power of judicial review, to be forced to establish new interpretations that include the new elements of the NMP.

Beyond several guidelines that we will discuss later, issued by FinCEN over the years, there are no statutes that reflect the new typologies of cyber money laundering. This represents a problem when assisting the investigative authorities to detect this type of crime. We will explain briefly the regulatory scheme against money laundering in the United States of each of the NMP discussed in the last chapter:

[99] *Id.*

1. Prepaid Cards

As mentioned in Part 1.C, the USA Patriot Act amended the BSA to direct the Secretary of the Treasury to prescribe regulations requiring financial institutions to establish procedures to verify the identity of their clients by confirming who the person is, keeping records and determining if the person or agency that wishes to open an account is considered a terrorist.[100] The BSA defines "financial institution" with applicability of Section 36 as:

> (A) An insured bank . . .; (B) a commercial bank or trust company; . . . (K) an issuer, redeemer, or cashier of traveler's checks, checks, money orders, or similar instruments; (L) an operator of a credit card system; . . . (Y) any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to, or a substitute for any activity in which any business described in this paragraph is authorized to engage; or (Z) any other business designated by the Secretary whose cash transactions have a high degree of usefulness in criminal, tax or regulatory matters.[101]

Although the statute does not expressly mention prepaid cards, it is broad enough to apply to businesses that participate in the issuance of such cards. FinCEN has acknowledged that prepaid cards were not contemplated in Section 326 when it was implemented in 2001 because the cards were so new that regulators were uncertain how they would be used to launder money.[102] Section 326 requires banks to establish CIP (customer identification programs) to banks, but not to other institutions involved in the prepaid card industry, including non-bank card marketing companies and credit card companies.[103]

---

[100] *See* USA Patriot Act § 326, 31 U.S.C. § 5318(l) (2018).

[101] 31 U.S.C. § 5312(a)(2) (2000).

[102] David Breitkopf*, Regulators Eye Payroll Cards*, AM. BANKER (New York), May 24, 2004, at 5.

[103] Julia S. Cheney & Sherrie L.W. Rhine, *Prepaid Cards: An Important Innovation in Financial Services*, 52 CONSUMER INT. ANN. 370, 372–73 (2006) (explaining the three main participants in most stored value business arrangements are banks, credit card companies, and nonbank card marketing services). The BSA expressly applies to banks (subsections (A) and (B) of 31 U.S.C. § 5312(a)(2)) and credit card companies (subsection (L)), and could reasonably apply to nonbank card marketing services via subsections (Y), (K) or (Z). *See* 31 U.S.C. § 5312 (2018).

The open loop prepaid cards discussed in Part II.D are regulated in the same way as closed-loop prepaid cards.[104] The regulation on prepaid cards has been revised to take into account the wide range of functions and the high risk for money laundering posed by open-loop prepaid cards. In 2006, the Board of Governors of the Federal Reserve issued a final rule amending Regulation E,[105] which implements the Electronic Funds Transfer Act,[106] to expand the definition of "account" regulation to include payroll cards.[107] Although this rule was intended to provide protection to consumers who use electronic methods to transfer their funds, it is an attempt to regulate this type of prepaid card variant. This distinction between the two modalities has not been effectively addressed, as we will discuss later.

On March 21, 2016, a group of federal agencies in charge of the banking industry in the United States[108] and FinCEN published a guidance document for issuing banks to implement joint regulations aimed at strengthening compliance with the requirements established in the customer identification program (CIP) under Section 326 of the USA Patriot Act with respect to prepaid cards.[109] The guidance clarifies that a bank must apply its CIP to cardholders of certain prepaid cards issued by the bank and other prepaid access devices that meet the criteria.[110] To comply with the criteria imposed, the bank must include

---

[104] *Id.* at 371.

[105] *See* Electronic Fund Transfers, 71 Fed. Reg. 51,437 (Aug. 30, 2006).

[106] Electronic Fund Transfer Act, Pub. L. No. 95-630, 92 Stat. 3728 (1978) (codified as amended in scatter sections of 15 U.S.C. (2018)).

[107] Payroll cards, or "payroll card accounts" are an alternative to direct deposit to payments by check. These cards are issued by the largest payment processors, such as Visa, and allow workers to use them in places that accept credit cards.

[108] The Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), and the Office of the Comptroller of the Currency (OCC).

[109] *See* Press Release, Interagency Guidance to Issuing Banks on Applying Customer Identification Program Requirements to Holders of Prepaid Cards, https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20160321a1.pdf; *see also* Customer Identification Programs for Banks, Savings Associations, Credit Unions and Certain Non-Federally Regulated Banks, 68 Fed. Reg. 25090 (May 9, 2003) (codified at 31 C.F.R. § 1020.220 (2011) (FinCEN); Procedures for Monitoring BSA Compliance, 12 C.F.R. § 21.21 (2014) (OCC); Suspicious Activity Reports, 12 C.F.R. § 208.62(b)(2) (2000); Procedure for Monitoring Bank Secrecy Act Compliance, 12 C.F.R. §§ 211.24(j)(2) (FRB), 326.8 (FDIC), 748.2 (NCUA).

[110] *See* 31 C.F.R. § 1020.100(c), (a).

procedures to open accounts that, at a minimum, include the name, date of birth, address and customer identification number; and procedures to verify the client's identity using documentary or non-documentary methods.[111] The guidance document also recommends banks to enter into elaborate and enforceable contracts with prepaid access providers that clearly establish the duties, rights and obligations of each party in a manner consistent with the guidelines.

In turn, in October 2016, the Consumer Financial Protection Bureau (CFPB) approved a rule granting consumers of prepaid cards greater protections.[112] The new rule requires financial institutions to limit consumers' losses when funds are stolen or cards are lost.[113] However, these rules were directed to the consumer and did not include anti-money laundering measures.

In short, the customer identification programs required of financial institutions under Section 326 of the USA Patriot Act of 2001 constitute the most important anti-money laundering mechanism of the prepaid card payment system.

2. Mobile Payments

There has been much uncertainty as to which laws, regulations or state or federal financial rules are applicable to mobile payment services. Although there is no federal agency that is responsible for the specific implementation of this type of payment, supervision falls on several. Agencies whose financial services regulations are applicable to mobile payments are the Federal Reserve, FinCEN and the CFPB.[114]

Many of the Federal Reserve's financial services regulations are written broadly enough to cover mobile payment services.[115] These

---

[111] FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL (FFIEC), BANK SECRECY ACT (BSA)/ANTI-MONEY LAUNDERING (AML) EXAMINATION MANUAL: CUSTOMER IDENTIFICATION PROGRAM 47, 48–49 (2015)

[112] See CFPB, *Prepaid Accounts Under the Electronic Fund Transfer Act (Regulation E) and the Truth in Lending Act (Regulation Z)*, RIN 3170-AA22, Docket No. CFPB-2014-0031, for a detailed summary of the new rule.

[113] *See id.* at 5–6.

[114] *The Future of Money: Where do Mobile Payments Fit in the Current Regulatory Structure?: Hearing Before the H. Subcomm. on Fin. Insts. and Consumer Credit and the H. Comm. on Fin. Servs.*, 112th Cong. (2012).

[115] *See id.* at 5–17.

regulations include GLBA,[116] Regulation P,[117] EFTA[118] and Regulation E,[119] TILA[120] and Regulation Z,[121] among others. When it comes to non-financial institutions that provide mobile payment services, everything will depend on the role of the institution in the transaction and the specific provisions of a particular statute or rule. However, the scope of existing Federal Reserve legislation for new mobile payment methods is still being determined.

For its part, FinCEN and its rules for prepaid access, which include mobile payments, are specifically designed to make money laundering difficult.[122] James Freis, Director of FinCEN, offered his testimony regarding the scope of BSA requirements and anti-money laundering to the institutions responsible for managing mobile payment services:

> FinCEN's regulations also have made it clear that the acceptance and transmission of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another person or location, by any means, constitutes money transmission, and that any person wherever located doing business wholly or in substantial part within the United States engaging in money transmission, regardless of any other business lines the person is engaged in—such as the provision of telecommunications services—would likely be a money services business under FinCEN's regulations, and as such must register and

---

[116] Gramm–Leach–Bliley Act (GLBA), Pub. L. No. 106-102, 113 Stat. 1338 (1999) (also known as the "Financial Services Modernization Act of 1999"). This law repealed the Glass-Steagall Act of 1933 to allow commercial banks, investment banks, brokerage firms, and insurance companies to consolidate with each other

[117] 12 C.F.R. pt. 1016 (2011). Regulation P regulates the treatment of non-public personal information of consumers by financial institutions subject to the oversight power of the Federal Reserve Board of Directors.

[118] Electronic Fund Transfer Act, Pub. L. No. 95-630, 92 Stat. 3728 (1978) (codified as amended in scatter sections of 15 U.S.C. (2018)).

[119] 12 C.F.R. pt. 1005 (2011).

[120] Truth in Lending Act (TILA) of 1968, Pub. L. No. 90-321, 82 Stat. 146 (codified as amended at 15 U.S.C. § 1601).

[121] 12 C.F.R. pt. 226 (2011). Regulation Z implements the TILA requirement that lenders make significant credit statements to borrowers for certain types of consumer loans.

[122] *The Future of Money*, *supra* note 114, at 1–2.

> comply with all the reporting, recordkeeping, and monitoring requirements applicable to a money transmitter.[123]

That is, mobile payments would be considered as a "money transmission," and this type of transaction is required to register with FinCEN and comply with the record keeping and reporting required by the agency in its prerogative to implement the BSA. In addition, he emphasized that a payment system that allows the transfer of funds from one mobile phone to another is subject to the FinCEN prepaid access regulations.[124] In addition, if the activities of a non-financial institution meet the requirements of "money services business" (MSB), these entities must register with FinCEN as MSB.

For its part, the CFPB states that under the Dodd Frank Act[125] the CFPB is required to regulate the financial products of consumers and services under the financial right of the consumer. The broad language of this statute covers mobile payment systems and services. In terms of implementation, the CFPB's Cards and Payments team is responsible for analyzing the new developments in mobile payment services.

Like prepaid cards, this type of payment is governed by the provisions of the BSA and USA Patriot Act and financial institutions that provide mobile payment services must comply with the CIP and the requirements of the BSA. Those non-financial institutions that provide mobile payment services will have to comply with the same requirements.

3. Internet Payments Services

As already mentioned, online payment services comprise a variety of services, including online banking, prepaid internet payment services and digital currencies. The internet payment services already mentioned in Part II.D.3 are mostly granted by MSB. Therefore, all

---

[123] *Id.* at 5.

[124] *Id.* at 9.

[125] Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 (2010). The Act was passed in response to the 2007–08 financial crisis and provided the most significant changes to financial regulation in the United States since the New Deal legislation following the Great Depression.

regulations concerning this figure have a substantial impact on this type of electronic transfers.

On July 21, 2011, FinCEN published an amended Final Rule definition and other regulations related to MSB. The amended regulations define MSB as:

> [A] person wherever located doing business, whether or not on a regular basis or as an organized or licensed business concern, wholly or in substantial part within the United States, in one or more of the capacities listed in paragraphs (ff)(1) through (ff)(7) of this section. This includes but is not limited to maintenance of any agent, agency, branch, or office within the United States.[126]

The Final Rule includes a person providing money transmission services, or any other person involved in the transfer of funds. Specifically, it defines money transfer services as:

> A person that provides money transmission services. The term "money transmission services" means the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means. "Any means" includes, but is not limited to, through a financial agency or institution; a Federal Reserve Bank or other facility of one or more Federal Reserve Banks, the Board of Governors of the Federal Reserve System, or both; an electronic funds transfer network; or an informal value transfer system.[127]

The regulation also stipulated that a person could be classified as a money transmitter from case to case subject to an analysis of facts and circumstances, and identifies circumstances around which the person's activities do not convert him or her into a money transmitter.[128] In turn, the regulation exempts from the status of money transmitter those people who only provide delivery services, communications or access

---

[126] 31 C.F.R. § 1010.100(ff).

[127] *Id.* § 1010.100(ff)(5)(i)(A).

[128] *Id.* § 1010.100(ff)(5)(ii). ("Facts and circumstances; Limitations. Whether a person is a money transmitter as described in this section is a matter of facts and circumstances.")

to data on the network used by money transmitters to supply their services.[129]

In 2013, FinCEN published a management brief that established that digital currency managers would be subject to the BSA and should register as an MSB.[130] The purpose of this legislation was to prevent virtual currency exchange methods from being used to launder money. The letter states that "currency" refers to the bill or currency of the United States or another country that is designated as a currency of legal effectiveness; that circulates; and it is commonly used and accepted as a method of exchange in the country that issued it. It also refers to digital precious metals and defines as a distributor a person:

> engaged within the United States as a business in the purchase and sale of covered goods and who, during the prior calendar or tax year (i) purchased more than $50,000 in covered goods; and (ii) received more than $50,000 gross proceeds from the sale of covered goods.[131]

The term "covered goods" of the definition of distributor established in the management brief includes precious metals. If a person acts both as a money transmitter and as a precious metals' distributor, he has to implement an anti-money laundering program to mitigate the risks as required by the BSA and the USA Patriot Act. Specifically, he would be required to submit reports related to the sale of instruments. Negotiable instruments, record keeping, and the maintenance of records related to negotiable instruments.

Virtual currencies, online gambling, online auctions, digital precious metals and other online securities exchange platforms can be classified as money transmitters and would be subject to the 2013 FinCEN guidelines. to register, keep records of the transactions that are carried out and the performance of reports. These mechanisms are the ones that would help the authorities to detect suspicious transactions and possible cyberlaundering schemes.

---

[129] *Id.* § 1010.100(ff)(5)(ii)(A). ("(A) Provides the delivery, communication, or network access services used by a money transmitter to support money transmission services.")

[130] DEP'T OF THE TREASURY, FIN. CRIMES. ENFORCEMENT NETWORK (FINCEN), FIN-2013-G001, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES 2 (2013), http://www.fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html.

[131] 31 C.F.R. § 1027.100(b).

B. What Should be the Regulatory Approach?

Regulatory anti-money laundering schemes can focus on those parties that benefit the most from money laundering, say criminals. The alternative to this approach is to focus on financial institutions, increasing the compliance costs of commercial entities that offer securities exchange services. The opinion of this author is that we must focus on financial institutions. New technologies have created a plethora of innovative business platforms that significantly facilitate money laundering. To begin the analysis, it is important to begin by discussing the challenges that hinder the regulation of new payment methods.

First, the Internet and the SMS network, like many of the new technologies, are tools of neutral value that can be used both for beneficial activities for society and harmful ones. The internet provides a great potential for economic and social growth, and such exponential growth should not be affected by anti-money laundering regulations that are too onerous. On the other hand, mobile payment platforms provide a highly efficient system considering the number of mobile devices that exist and the ease with which transactions are carried out.

Second, regulating specific technologies can be inefficient due to the accelerated pace in which new technologies are being developed. The first cell phone with NFC technology debuted in the market in 2010, the Samsung Nexus S, and today is used in the platform of Apple Pay and Android Pay in millions of mobile phones as one of the main payment mechanisms. This phenomenon, characterized by major technological changes in short periods of time, would force legislators to visit the regulations repeatedly to make sure they are technologically up to date. The immediate effect would be to aggravate the problem of money laundering by allowing washers to use business models based on poorly regulated technology and increase regulatory costs.

Finally, laws directed at specific technologies can create unfair competition among emerging technologies. The laws would have the effect of increasing operational costs by requesting greater requirements in the identification of clients or in the system of maintenance of reports, creating convenient conditions for other technologies that compete for the services offered. This could affect the development of the technologies concerned, preventing further growth and the development of new technologies that may be of use to society.

Some authors argue that the current regulatory approach is enough to discourage cyber money laundering. However, considering the proliferation of new technologies and increasing dependence on new payment methods, this concept has changed considerably in recent decades. The magnitude of the problem of cyber money laundering is intensified due to the factors mentioned in Chapter 2.2, namely: (1) anonymity; (2) speed; (3) non-traceable transactions; (4) ability to transfer unlimited value; (5) no face-to-face contact; and (6) cross-border activity. This coupled with a lack of resource allocation and proper focus leads to grim scenarios. One of these scenarios is found in the case of Liberty Reserve, one of the largest online money launderers in the world.

In 2015, U.S. prosecutors shut down the global currency exchange company Liberty Reserve and accused it of being the largest money laundering operation on the Internet in history, referring to it as the "bank of choice for the criminal underworld."[132] More than one million customers used the Costa Rican company to launder more than $ 6 billion. In addition to the drug traffickers, the illicit users of Liberty Reserve included a wide range of criminals, thugs and criminal organizations dedicated to credit and investment card fraud, identity theft, hacking and child pornography. The company never registered with FinCEN as MSB and operated from the outset outside the agency's regulatory framework.

The large sums laundered by Liberty Reserve and the varied range of illegal activities can illustrate the problem that may arise from not efficiently regulating new technologies and not imposing greater requirements on financial institutions or, as in this case, MSBs, dedicated to exchange of funds or values in cyberspace or mobile networks.

The USA Patriot Act through Section 326 requires the implementation of customer identification programs for financial institutions and other non-banking institutions that engage in the exchange of money. In turn, FinCEN requires financial institutions to register, and MSBs when they acquire the status of money transmitters. However, to this day, there are many non-financial institutions that are

[132] United States v. Budovsky, No. 13cr00368 (DLC), 2016 WL 386133 (S.D.N.Y. Jan. 28, 2016).

not registered with FinCEN, as was the case of the Liberty Reserve company.

Although the regulatory approach increases the demands and, therefore, the compliance costs of commercial entities that offer payment services in cyberspace or mobile networks, this must be accompanied by efficient implementation by the relevant federal agencies. FinCEN is the main agency in charge of implementing the BSA, and its performance in auditing financial and commercial institutions is vital. John A. Cassara, a FinCEN employee from 1996 to 2002, strongly criticized the way the agency operated during his work. In his opinion, FinCEN had too many supervisors and few employees, refused to participate in investigations of rival agencies, did very little with the millions of BSA files in their databases and spent taxpayers' money on poorly designed technology systems. In addition, Cassara argued that the vast majority of the analysis was not really analysis, but a process of data reorganization. The analysts verified the databases, organized the data, covered the product and sent it back to the client. The result was a large and heavy document with little process of data analysis, and the applicant ended up frustrated.[133]

Therefore, despite reaching an optimal regulatory framework and focused either to deter criminal actions by money launderers (through education or "outreach") or impose greater requirements on financial institutions in the implementation of the programs that are required by law, it is imperative that the agencies in charge contemplate efficient implementation systems. If Cassara's testimony is true, what would it be worth to impose greater identification requirements and increase the current standards if after receiving the data required by the BSA it is not analyzed properly? In fact, although the BSA authorizes FinCEN to impose fines of a civil nature against financial institutions and businesses or non-financial businesses for violations of the BSA or lack of implementation of the required regulations,[134] in rare cases the agency exercises this authority and generally addresses the issue of regulatory violations through education. However, the first step must be to address the regulatory framework, directing it to address the

[133] *See* JOHN A. CASSARA, HIDE & SEEK: INTELLIGENCE, LAW ENFORCEMENT, AND THE STALLED WAR ON TERRORIST FINANCE 161–75 (Potomac Books 2006).

[134] *See* 31 U.S.C. § 5321 (2018); *see also* 31 C.F.R. § 1010.820 (2016).

inadequacies of the legislation provided to address the issue of electronic money laundering.

C. U.S. Regulatory Deficiencies Regarding NMPs

Section 326 of the USA Patriot Act does not require MSBs and other non-financial entities in charge of providing prepaid card services, mobile payment services and online payment services to establish customer identification programs (CIP). Not requiring MSB to implement customer identification programs substantially increases the likelihood that they will be used as a vehicle for laundering. Clients would enjoy a higher degree of anonymity when making their transactions. As already discussed, anonymity is one of the most important cyberspace attractions for money launderers.

This has been partially corrected by the requirements imposed by FinCEN in the 2013[135] directive by requiring MSBs and other institutions that are classified as "money transmitters" to present documentation required by the BSA to financial institutions. This includes the presentation of CTRs and SARs for registration purposes and collaborating with the authorities to identify suspicious activities but does not impose the establishment of a CIP program. Establishing these programs in these commercial entities, while increasing operational costs, would provide greater tools to the authorities to detect money laundering.

D. How to Correct the Regulatory Deficiencies with NMPs

The regulatory model would be corrected by the application of new approaches, such as the imposition of greater responsibilities on intermediary institutions to enforce the law. In keeping with this vision, the figure of "gatekeepers" provides an innovative approach in the search for effective implementation of public policies and regulations by the state. "Gatekeepers" are private entities able to prevent or deter inappropriate behavior by denying cooperation to the wrongdoers.[136] Lawyers and accountants are natural gatekeepers for fraudulent

---

[135] *See* FIN-2013-G001, *supra* note 130.

[136] Reiner H. Kraakman*, Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy*, J. L., ECON., & ORG., vol. 2, no. 1, at 53 (Spring 1986).

transactions that require scrutiny and legal opinions to be carried out.[137] In addition, the creation of regulatory measures such as licensing requirements can create fenders. For example, the prescription system allows doctors and pharmacists to prevent the abuse of controlled substances.[138] The ultimate purpose of fenders is to deter and prevent the improper conduct of individuals or corporations that use their services.

The application of the law by third parties serves as a response when too many malefactors remain unresponsive to the range of existing legal penalties. Direct deterrence of criminal behavior through laws often fails because wrongdoers lack the ability or information to make compliance decisions based on self-interest.[139] This deterrence also fails because criminal behavior is often costly to detect or prosecute and the fact that there are limits to the levels of penalties that may be imposed.[140] Regarding this last point, an example would be the fact that we cannot impose a fine that exceeds the value of the net assets of a company or individual for carrying out illicit transactions.[141]

At present, one should aim to find the perfect balance between the direct application of the law and the application of law by third parties. If the imposition of measures to third parties may entail an additional cost in their operations, the responsibility arising from non-compliance with these measures is justified by the dissuasive power of the respective implementation. In this sense, we understand that fenders have a deterrent effect on criminal activity.

To impose greater responsibility on financial and non-financial institutions to serve as gatekeepers in the supervision of suspicious activities and the implementation of programs aimed at discouraging money laundering, it is necessary to follow the example of other countries that have adopted requirements of stricter compliance. Since 2011, users of prepaid cards in the United Kingdom have had to adhere to the Electronic Money Regulations (EMR) established by the Financial Conduct Authority (FCA) in order to ensure greater

---

[137] *Id.* at 54.
[138] *See* 21 U.S.C. § 829 (2018).
[139] *See* Kraakman, *supra* note 136, at 56.
[140] *Id.* at 59.
[141] *Id.* at 64.

transparency in the operations of the referred sector.[142] The most important changes proposed by the anti-money laundering regulation established in 2011 by the United Kingdom were:

> (1) All applicants requesting to be electronic money issuers will be required (within the services provided by an electronic money issuer is the issuance of prepaid cards) to provide descriptions of governance arrangements, internal control mechanisms, risk management procedures and money laundering controls that will be used when issuing electronic money or providing payment services.[143]
> (2) All electronic money issuers must comply with legal requirements to discourage money laundering, and to that end, applicants must provide a description of the internal control mechanisms they will implement to comply with the relevant anti-money laundering regulations.

These policies are aimed at imposing greater responsibility on companies that request to be registered as electronic money transmitters. Effective monitoring of these types of companies can help authorities detect money laundering in cyberspace. The EMRs require the companies to develop a plan to address the possible money laundering risks of their business model and ensure the implementation of internal procedures and policies communication mechanisms to mitigate money laundering. The requirements attack the core of the matter by imposing on companies that offer services that involve financial transactions with digital currencies, online services or mobile payments to establish a plan to detect and mitigate money laundering.

This contrasts with the focus of Section 326 of the USA Patriot Act and its most important mechanism for detecting money laundering: the customer identification program (CIP). While EMR regulations are responsible for discouraging money laundering from businesses by requiring them to evaluate their business model and establish anti-laundering policies, CIP has two important functions: (1) to make a customer"s money laundering process more complex to create and present false information about their person, and (2) provide

---

[142] *See* FIN. CONDUCT AUTH., THE FCA'S ROLE UNDER THE ELECTRONIC MONEY REGULATIONS 2011: OUR APPROACH (2013), https://www.fca.org.uk/publication/archive/emoney-approach.pdf.

[143] *See id.*

information to the authorities that may be of help in possible criminal investigations. In cyberspace, the effectiveness of the first function of the CIP is difficult to quantify because money launderers do not have to be face to face with the commercial entity at the time of the transaction. In many online platforms, providing false information is much easier, weakening the aforementioned function. This also affects the second function, because by facilitating the presentation of false information at the time of the transaction or creating an account, the information collected on many occasions will not be useful to the authorities to find the money launderers.

The EMR offers a different approach by requiring commercial entities to deal with virtual currencies and other types of online payments that evaluate their respective business models and identify mechanisms to prevent money laundering. This approach is of particular importance when evaluating NMPs. The constant evolution of technological systems makes it imperative that financial institutions and other providers of financial services, with greater knowledge in the new technologies' procedures, techniques, and internal mechanisms as a platform offered for the exchange of values, have a greater role in the fight against the laundering of cybernetic money. Requiring companies to create plans to avoid money laundering of different business models based on different technologies can be beneficial for federal agencies, which would use the plans presented as input when establishing rules.

Therefore, it is imperative to amend Section 326 of the USA Patriot Act to expressly include MSBs and other businesses engaged in the transmission of money; and implement a stricter money laundering program imposing greater responsibilities on the financial sector and other companies dedicated to providing services using the NMP. The only negative aspect of this approach is that many of the companies cataloged as MSB do not register with FinCEN.

The Liberty Reserve case is one of many recent cases related to money laundering using new payment methods by an unregistered company. In 2014, Judge Ellen L. Hollander ordered the seizure of $45 million dollars from E-Gold, Ltd., an online company dedicated to the peer-to-peer exchange of digital precious metals that pleaded guilty to money laundering in 2008.[144] In another case, Robert M. Faeiella or "BTCKing," an underground bitcoin exchanger, and Charlie Shrem,

[144] *See* United States v. E-Gold, Ltd., 550 F. Supp. 2d 82 (D.D.C. 2008).

formerly the CEO and Compliance Officer of a bitcoin exchange company, pleaded guilty in federal court in Manhattan for operating an unregistered MSB, in which they transmitted money with the intent to facilitate criminal activity (*e.g.*, drug trafficking) on the "Silk Road," a website that serves as a black market designed to allow its users to buy and sell drugs anonymously and beyond the reach of the law.[145]

These three cases have something in common: although the defendants were businesses dedicated to the transmission of money, none of the businesses were registered with FinCEN as MSB. Courts have reiterated on several occasions it is a potential crime to carry out business in the digital exchange of currencies without registering with FinCEN, even if the state in which it operates does not impose a similar requirement.[146]

This principle was recently confirmed in *United States v. Lord*, where the defendants unsuccessfully tried to withdraw their guilty pleas based on their failure to register with FinCEN.[147] In the aforementioned case, the plaintiffs (father and son) began operating a bitcoin business through the internet on a website called localbitcoins.com. At the beginning of 2014, a bitcoin broker warned them that they were required to register with FinCEN because they were dedicated to the exchange of virtual currencies. Although the defendants allegedly produced false representations that they had registered with FinCEN before the bitcoin broker, it was not until November 2014 that they registered with FinCEN.[148] By that time, they had already exchanged more than $ 2.5 million dollars.[149] This delay in the search was the cause of the charges against the defendants.[150]

In none of the cases mentioned were the companies registered with FinCEN as MSB. While the law establishes that companies or individuals dedicated to the transmission of money must register in a period not greater than 180 days since the business was established

---

[145] *See* United States v. Faiella, 39 F. Supp. 3d 544 (S.D.N.Y. 2014).

[146] *See id.* at 546 (finding "Faiella clearly qualifie[d] as a 'money transmitter'); *see also* E-Gold, Ltd., 550 F. Supp. 2d at 97 ("Because Defendants are money transmitters, when they engage in cash transactions, they are required to file reports under Section 5313; when they do not engage in cash transactions, they are not.").

[147] Crim. No. 15-00240-01/02, 2017 WL 1424806 (W.D. La. Apr. 20, 2017).

[148] *Id.* at 3–4.

[149] *Id.* at 4.

[150] *Id.*

since the approval of the Money Laundering Suppression Act of 1994,[151] many companies that establish operations to launder money in cyberspace omit this requirement to avoid submitting documents required by the BSA, including suspicious activity reports (SARs) and monetary transaction reports (CTRs).

This aspect is related to the implementation of the established regulations, not the scheme itself. Laws only become useful when they are properly implemented. The proper monitoring of the virtual platforms to exchange currencies and securities carried out by the agencies is vital for the programs and requirements established by the USA Patriot Act and the BSA to bear fruit. It is the duty of FinCEN and other agencies in charge of ensuring records to implement effective programs to detect virtual businesses that are operating outside of the registration required by law.

IV. CONCLUSION

New advancing technologies represent innumerable challenges to the agencies tasked with regulating money laundering in cyberspace. It is the duty of the legislature to adjust and update the existing law to cover any deficiencies that hinder effective regulation. Yet, the issue of money laundering only continues to grow using the new technology, and not just in the United States, but around the globe. Thanks to cyberspace, technology has fostered international platforms for money laundering that could never before conceived.

Congress should impose stricter requirements to the anti-money laundering program required of financial entities, and to extend it to all companies dedicated to the transmission of virtual money. In turn, mechanisms should be created to facilitate the detection of businesses that operate without registering. A combination of regulations aimed at imposing higher compliance requirements to combat money laundering on financial institutions, and an increase in the monitoring of mobile and online businesses that are dedicated to the exchange of securities, will help to deter and detect cyberlaundering.

---

[151] Pub. L. No. 103-325, §§ 401–413, 108 Stat. 2160, 2243–2255 (1994) (codified in scattered sections of 12 and 31 U.S.C.); *see, e.g.*, 31 U.S.C. § 5330(a)(1) (2018).

The adoption of models contemplating an imposition of liability on offenders is becoming more indispensable given the little effect the current regulatory scheme has in detecting money laundering. The crime of money laundering begins with the financial institutions used, and these entities possess both the greatest responsibility and ability to deal with the matter head on.