Cyber-Laundering

Dr. Nathalie RÉBÉ
Financial Crimes and AML Consultant, Luxembourg
reben@caramail.fr

Abstract

The aim of this chapter is to help the reader gain understanding of the various money laundering practices using technology and discover the way they may be utilized by criminals to finance their illegal endeavors. The author will discuss international compliance and regulatory mechanisms, as well as international countermeasures to deter cyber-laundering.

Index terms: Cyber-laundering, Financial Crimes, Internet Regulations, Virtual Asset / Currencies

1. Introduction

Our interconnected world offers new and innovative ways to transfer and disguise funds that represent new money laundering concerns. The internet includes extensions of established payment systems, as well as new payment methods, which operate differently from traditional monetary transactions. As criminals have always been agile in adopting new methods and technologies to circumvent laws, they now take advantage of technological innovation and globalization to further expand their illicit businesses. By conquering and controlling the "cyber space", they can anonymously exploit new opportunities to evade the system and make high value transactions without paper trails or legal accountability. With the use of such methods, they can manage to stay one step ahead of law enforcement.

To comprehend the functioning of online unlawful financial activities, we will discuss how services can be abused, and describe the numerous ways to launder money and assets online. We will also review cyber-laundering risk factors, suspicious activities, and regulatory loopholes, such as weak or inefficient regulations, privacy concerns, jurisdictional conflicts, or law enforcement issues. In the end, recommendations and conclusions will be provided, along with current and future problematics related to cyber-laundering matters.

2. How online financial services can be abused?

Money laundering is the concept of converting illegally obtained money, to make it look like it was legitimately obtained. Cyber-laundering, can then simply be defined as the practice of money laundering carried out online. The internet can be used to launder money through multiple methods and at all stages of the money laundering process, namely the placement, layering or integration phases. Criminals can easily disguise their transactions, convert them into cash, they later on deposit in banks. Virtual currencies and assets can also be created and exchanged via a decentralized network of computers, to avoid financial institutions or governments' oversight.

Since the internet is the perfect platform for commerce, financial criminal activities can easily occur online, as transactions fall outside existing regulatory definitions. Therefore, cyber-laundering, is often related to cybercrimes such as: the sale of control substances, the sale of illegal items such as

firearms, tax evasion, terrorism financing, computer crimes, human trafficking, child exploitation, scams, fraud, extortion, etc.

3. Ways to launder money and Assets online

There are three main cyber-laundering typologies [1]:

- Internet payment services (such as mobile payments, micro payments or digital precious metals);
- Store value cards and smart cards;
- Online banking.

Additionally, cyber-laundering methods comprise crypto dark pools, over the counter purchases, crypto mining, art, NFT, crypto ATM, and physical to digital goods translation. While these techniques are quite famous ways to launder money, online gambling, gaming, auctions, and virtual worlds and assets are also starting to be known from the general public.

4. Risk Factors

The evolution of technology has allowed criminals to transfer large sums of dirty money via the internet. There are quite a few money laundering risk factors associated with new technologies. They include anonymity, the speed of the transactions, untraceable transactions, the cross-border nature of the internet, and third-party funding [2]. Since the internet crosses geographical border, online activities involve several jurisdictions, mutual legal assistance treaties issues, and the ability to transfer unlimited value.

Nowadays, it is nearly impossible to follow an account access and utilization, as it is possible to conduct transactions online from public terminals, and with high-level encryption. The anonymity online services provide also permits to avoid personal "face to face" contact, and to fulfill the "know your customer" compliance principle.

5. Suspicious Transactions

Cyber-launderers generally benefit from compliance detection and reporting inefficacy. As technology providers are unable to properly identify and authenticate parties, there is an obvious lack or inadequacy of audit trails, record keeping, and suspicious transaction reporting regarding online financial activities.

There are known "*red flags*" which can help recognize potential illicit online financial behaviors. These specific indicators can be classified into categories, such as: the size and frequency of transactions; transactions' patterns (irregular, unusual, or uncommon); the sender or beneficiary suggest criminal activity; the source of funds or wealth, relationship to criminal activities; or geographical risks [3].

6. Regulations

There are many organizations dedicated to preventing and stopping money laundering and cyber-laundering activities such as the United Nations, the European Union, the European Commission, the Financial Action Task Force, the International Monetary Fund, the Financial Crime Enforcement Network, the European Banking Authority, the Basel Institute, and the Egmont Group which established the Financial Intelligence Units. In such effort, several countries and international institutions have introduced robust legislations, recommendations, and policies.

Although Australia, the European Union, and the United Kingdom have created regulations concerning virtual currency, most countries do not have their own cyber-laundering legislation. In the European Union, the most famous tools to combat cyber-laundering are the Fifth [4] and Sixth [5] Anti-Money Laundering Directives implemented by its Member States. There are many legal instruments related to cyber-laundering, however they often rely on money laundering and counter-terrorism financing offences.

Other international policies concern cyber-laundering activities, including: the 2006 Anti-Money Laundering and Counter-Terrorism Financing Act [6]; the Bank Secrecy Act [7]; the 2018 Clarifying Lawful Overseas Use of Data (CLOUD) Act [8]; the International Convention for the Suppression of the Financing of Terrorism [9]; the 2020 Lawful Access to Encrypted Data (LEAD) Act [10]; and the 2001 USA PATRIOT Act [11].

The OECD Financial Action Task Force's work carry a great importance in the fight financial crimes. Their main recommendations related to cyber-laundering are the following:

- 2013 Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments, and Internet-Based Payment Services [12];
- 2014: FATF report: Virtual currencies. Key definitions and potential AML/CFT risks [13];
- 2015: Guidance for a Risk-Based Approach to Virtual Currencies [14];
- 2019: Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers [15]; and
- 2021: Revised 2019 Guidance on Virtual Assets and Virtual Asset Service Providers [16].

7. Privacy concerns

Data protection remains a key problematic in the anti-money laundering detection process. Various cyber-laundering methods are hard to keep track of, since each transaction cannot be recorded, as it would undoubtfully cost providers too much time, money, and data storage. While the level of recordkeeping of transactions and of ownership is important for the law enforcement process, detailed recordkeeping will most of the time decrease customer acceptance, because of privacy concerns.

The Financial Action Task Force 2019 "travel rule", requires "to obtain, hold, and transmit required originator and beneficiary information, immediately and securely, when conducting Virtual Assets transfers" [17]. However, a few recent regulations raise questions about recordkeeping's privacy concerns. Data protection laws considerably differ in various jurisdictions. For example, the European Union General Data Protection Regulation [18] has significant requirements to protect the privacy of EU persons. It requires compliance with safeguards for the protection of personal data from "technology enabled EU financial marketplace". There is also potential for conflict with other laws such as the CLOUD Act [19].

8. Jurisdiction

In some jurisdictions, the degree of regulation varies depending on the type of online financial service provided. Whereas in other jurisdictions, the same services are simply not regulated. There can be regulated and unregulated entities. Providers are not necessarily required to obtain a license or register for the provision of certain financial online services in some countries. As a result, there are no legal money-laundering reporting requirements for such providers in these jurisdictions. Therefore, criminals often privilege the most advantageous forum. Such regulatory gap creates

loopholes which lead to unlawful behaviors, while making it difficult to investigate and prosecute cyber-laundering.

9. Law enforcement

Several cyber-laundering law enforcement issues have emerged. First, as the current enforcement mechanism relies on defined financial and geographic borders, determining competent jurisdictional authority in the case of financial cybercrime can be a difficult task. Second, existing supervisory regulatory regimes constantly require revision for each known or new typology, since technology is in perpetual evolution. Third, the speed and volume of online transactions make it difficult to identify and find felons. Fourth, it is complicated to ensure accurate and adequate records of the transactions and persons involved. Last, stored value cards are clearly more difficult to detect and track than physical currency.

10. Recommendations

In this chapter, we have seen numerous regulatory issues regarding online financial crimes. Recalling that several factors work in the favor of criminals, such as the anonymity provided by the internet, the asymmetry in regulations, and the lack of adequate legal obligations for online financial service providers. To further complicate matters, many online funds services are covered by privacy regulations such as which make it complex for governments to uncover details of transactions if users do not allow access.

In an attempt to fill these legal loopholes, various recommendations will now be issued:

First, governments should prohibit the cryptocurrency exchanges they regulate from clearing and settling transactions with unregulated exchanges.

Second, regulators should prohibit exchanges from buying and selling cryptocurrencies that are explicitly designed to evade controls.

Third, anti-money laundering verification and reporting requirements should be enhanced concerning prepaid cards, crypto ATMs, marketplaces, and crypto mining operations.

Fourth, there is a clear need to extend the classification of virtual asset service providers to other online activities, in order to extend the scope of actual legislations.

Last but not least, governments need to elaborate privacy and data sharing laws that are in adequacy with the detection and reporting of online financial crimes.

11. Conclusions and Problematics

Since the internet is designed to work internationally, it provides criminals the means to operate worldwide, using multiple currencies. The diminishing of international financial borders creates an additional challenge for law enforcement, as it makes it difficult to determine jurisdictional authority. Traditional law enforcement techniques and methods have therefore become less effective or even obsolete.

Moreover, there are presently too few statutes and regulations focusing on cyberlaundering matters, and they also rely on defined financial and geographic borders. Governments must then take into account the latest technological developments, along with cultural and cross-jurisdictional regulatory issues, while building new money laundering policies. Law enforcement, regulatory agencies, and the private sector clearly have a part to play in the policy-making process. They must get together to discuss issues of mutual concern, and develop effective and reasonable measures to prevent and detect online financial crimes without impeding the commercial and consumer advantages of new technologies.

Enhance cooperation and coordination efforts among nations are necessary to ensure that policies and standards to fight cyber-laundering activities are consistent with the actual threats encountered. To effectively investigate financial cybercrimes, and trace questionable electronic fund flows, regulators and law enforcement authorities require new tools and techniques. There is also a great need to find the appropriate balance between an individual's right to financial privacy and the legitimate need of law enforcement and regulatory authorities to prevent and detect crime.

References

[1]. Financial Action Task Force - FATF, (2012-2020). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, [online]. Available: www.fatf-gafi.org/recommendations.htm.

[2]. Financial Action Task Force - FATF, (2012-2020). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, FATF, [online]. Available: www.fatf-gafi.org/recommendations.htm.

[3]. Financial Action Task Force - FATF, (2020). Money laundering and terrorist financing. Red flag indicators associated with virtual assets [online]. Available: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf.

[4]. 5AMLD, (May 30, 2018). Directive (EU) 2018/843 of the European Parliament and of the Council, amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU, Official Journal of the European Union, 156, 43-74 [online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843.

[5]. 6AMLD, (October 23, 2018). Directive (EU) 2018/1673 of the European Parliament and of the Council on combating money laundering by criminal law, Official Journal of the European Union, 22-30 [online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L1673&from=EN.

[6]. Australian Government, (2006). Anti-Money Laundering and Counter-Terrorism Financing Act, Canberra, [online]. Available: https://www.legislation.gov.au/Details/C2020C00362.

[7]. United States Government, (1982). Bank Secrecy Act, [online]. Available: https://www.govinfo.gov/content/pkg/USCODE-2012-title31/pdf/USCODE-2012-title31-subtitleIV-chap53-subchapII-sec5311.pdf.

[8]. United States Congress, (2018). H.R.4943.- CLOUD Act, [online]. Available: https://www.congress.gov/bill/115th-congress/house-bill/4943.

[9]. United Nations, (1999). International Convention for the Supression of the Financing of Terrorism, [online]. Available: https://www.un.org/law/cod/finterr.htm.

[10]. US Congress (2020). S.4051 - Lawful Access to Encrypted Data Act, [online]. Available: https://www.congress.gov/bill/116th-congress/senate-bill/4051?r=1&s=1.

[11]. United States Government, (2001). Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, [online]. Available: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf.

[12]. Financial Action Task Force - FATF, (2013). Guidance For a Risk-Based Approach: Prepaid Cards, Mobile Payments, and Internet-Based Payment Services, the Financial Action Task Force (FATF), Paris, France, 1-47, [online]. Available: https://www.fatf-

gafi.org/media/fatf/documents/recommendations/Guidance-RBA-NPPS.pdf, accessed on April 7, 2021.

[13]. Financial Action Task Force - Financial Action Task Force - FATF, (2014). FATF report: Virtual currencies. Key definitions and potential AML/CFT risks [online]. Available: https://www.fatf-gafi.org/documents/documents/virtual-currency-definitions-aml-cft-risk.html.

[14]. Financial Action Task Force - FATF, (2015). Guidance For a Risk-Based Approach: Virtual Currencies, the Financial Action Task Force (FATF), Paris, France, 1-48, [online]. Available: https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf.

[15]. Financial Action Task Force - FATF, (2019). Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, the Financial Action Task Force (FATF), Paris, France, 1-59, [online]. Available: www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html.

[16]. Financial Action Task Force - FATF, (2021). March, Draft updated Guidance for a risk-based approach to virtual assets and VASPS, FATF/PDG (2020)19/REV1, Sixth draft - Public Consultation. FATF, Paris, France.

[17]. Financial Action Task Force - FATF, (22 February 2019). Public Statement - Mitigating Risks from Virtual Assets, FATF, [online]. Available: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html.

[18]. European Union, (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679).

[19]. US Congress, (2018). H.R.4943.- CLOUD Act, [online]. Available: https://www.congress.gov/bill/115th-congress/house-bill/4943.