International Journal of Legal Information 51.1, 2023, pp. 69–76. © The Author(s), 2023. Published by International Association of Law Libraries
doi:10.1017/jli.2023.13

Smurfing in Electronic Banking: A Legal Investigation of the Potential for Transnational Money Laundering

Abhishek Thommandru

Abstract

Money laundering is a serious crime that is often associated with organized crime, terrorism, and other illegal activities, often by transferring them through a series of financial transactions and institutions. In this study, the researchers focused on detecting a specific type of money laundering called "smurfing", which involves breaking up large amounts of money into smaller transactions. The growing market for banking services and the intense competition among banks has led to a shift towards electronic banking. This shift is driven by changes in the way that customers use banking services and the advancements in technology. Electronic banking offers several benefits, such as faster transaction processing and the ability to avoid waiting in line at physical branches. However, it also carries risks, including the potential for electronic payment systems to be used for money laundering. With the development of technology, money laundering can now be done through online betting and casino platforms, as well as through the buying and selling of cryptocurrencies. This article aims to explore the ways in which electronic payment systems, online gambling, and cryptocurrencies can be used to launder illegally acquired money.

Keywords: Money Laundering, Electronic Banking, Smurfing, Cryptocurrency, Illicit Money, crime

Introduction

The term "smurfing", also known as structure, is a common method of money laundering, which involves dividing large amounts of money into smaller amounts to avoid being detected. Criminals often use smurfing to deposit illicit funds into bank accounts in a way that makes it appear as though the money was obtained legally. Banks are required to report any cash transactions over a certain threshold to the government in order to help identify and prevent money laundering.[1] In the United States Banks, for example, the Financial Crimes Enforcement Network (FinCEN) is the authority which is watchdog and banks have a duty to report any cash transactions over $10,000. This is known as a Currency Transaction Report (CTR).[2] To avoid triggering a CTR, criminals may use sophisticated smurfing methods to disburse large sums of money into smaller fragmented amounts and deposit them into different remote and safe bank accounts. For example, a criminal may take $100,000 in cash and deposit it into ten different bank accounts in amounts of $9,000 each. This would allow the criminal to avoid triggering a CTR and make it more difficult for law enforcement to trace the illicit funds. Smurfing is often used in conjunction with other methods of money laundering, such as trade-based money laundering or the use of shell companies. It can be difficult for law enforcement to detect and prosecute cases of smurfing, as it often involves multiple individuals and financial institutions. To combat smurfing and other forms of money laundering, banks and

[1] Hinde, Stephen. "Smurfing, swamping, spamming, spoofing, squatting, slandering, surfing, scamming and other mischiefs of the World Wide Web." *Computers & Security* 19.4 (2000): 312-314.

[2] Network, Financial Crimes Enforcement. "Financial Crimes Enforcement Network." (2007).

other financial institutions have implemented a number of measures, such as the use of transaction monitoring systems and customer due diligence procedures. These measures help to identify suspicious activity and prevent illicit funds from being deposited into bank accounts. Despite these efforts, smurfing remains a common and effective method of money laundering. It is important for law enforcement agencies, banks, and other financial institutions to continue working together to identify and prevent this crime.

The electronic payment system is a regulated network that allows individuals to connect their bank accounts and transfer funds electronically.[3] This system allows for the quick transfer of large amounts of money across borders and continents, making it challenging to track the source of the electronic transfer and the flow of funds. According to Tomić, Todorović, and Jakšić (2017), electronic payment systems are susceptible to the misuse of funds, including for money laundering.[4]

The advancement of technology has contributed to the growth of electronic payment systems and the ways in which money laundering can be carried out through these systems. While account-to-account transfers are still the most common method, online gambling, betting, and electronic money, particularly cryptocurrencies, have become increasingly popular for money laundering.[5] Electronic transfers are heavily regulated in many countries, with a requirement for banks to identify their customers before allowing electronic money transactions. However, online betting and electronic money may not be as strictly regulated in some countries, making it easier for criminal organizations to exploit these systems. In countries where there are no laws regarding the identification of people making electronic money transfers or reporting large fund transfers, the central idea of money laundering is derivation the techniques of shifting from cash to electronic money or digital money.

This research examines how electronic payment systems, smurfing/ mules, and electronic money can be misused to launder illegally obtained funds. The study aims to identify the ways in which these new improvised methods can be used for money laundering. The final section investigates measures to prevent and protect against the use of electronic payment systems for money laundering. The conclusion summarizes the key findings of the research and suggests areas for further study.

DEFINITION AND HISTORY OF SMURFING

Smurf was a free-to-use web application by Microsoft in 1995, that allowed users to send and receive money via mail, telegram and even fax. It was used as part of the "X-word" technology, which helped people to make anonymous payments and transfer funds without revealing who they were or where the payment was coming from. Smurfing has now become an important form of money laundering. This type of fraud involves using illegal means to send and receive money through personal accounts. These fraudsters use various methods to ensure that their transactions are made without suspicion.[6]

The term "smurfing" was originally used to describe the practice of breaking up large sums of money into smaller amounts in order to avoid detection by law enforcement. The term is thought to have originated in the 1980s, when drug traffickers in Colombia began using networks of individuals to deposit small amounts of drug proceeds into bank accounts in order to avoid detection. As the practice became more widespread, law enforcement agencies began using the term "smurfing" to describe this method of money laundering[7]. In 1986, the U.S. Congress passed the "Money Laundering Control Act", which made it a federal crime to engage in money laundering or to assist others in doing so. The act specifically targeted the practice of smurfing and made it illegal to structure financial transactions in order to avoid reporting requirements. In the decades since the Money Laundering Control Act was passed, smurfing has continued to be a common method of money laundering. Criminals have used smurfing

[3] Krzysztof, W. O. D. A. "Money laundering techniques with electronic payment systems." *International&Security. An International Journal* (2006): 27-47.

[4] Todorović, Violeta, Milena Jakšić, and Nenad Z. Tomić. "BANK REGULATIONS IN MODERN FINANCIAL ENVIRONMENT." *Facta Universitatis. Series: Economics and Organization* (2017): 217-230.

[5] Calafos, Michael W., and George Dimitoglou. "Cyber Laundering: Money Laundering from Fiat Money to Cryptocurrency." *Principles and Practice of Blockchains*. Springer, Cham, 2023. 271-300.

[6] Singh, Ashish, and Kakali Chatterjee. "Cloud security issues and challenges: A survey." *Journal of Network and Computer Applications* 79 (2017): 88-115.

[7] Albrecht, Chad, et al. "The use of cryptocurrencies in the money laundering process." *Journal of Money Laundering Control* 22.2 (2019): 210-216.

https://doi.org/10.1017/jli.2023.13 Published online by Cambridge University Press

to launder money from a variety of illegal activities, including drug trafficking, human trafficking, and terrorism financing.

ROOTS OF MONEY LAUNDERING

The term "bleaching money" is thought to have originated in the United States during the Prohibition era of the early 1930s, when criminals would use various methods to "clean" the proceeds of their illegal activities, such as selling illegal alcohol.[8] By different methods that criminals may use to launder money, for example, deposit it in a bank that does not need information about the source of the funds, or using it to buy luxury branded goods that can be resold at a lower than market price in order to introduce the dirty money into legal financial flows.

Al Capone, one of the most infamous American gangsters, was known to have laundered approximately $1 billion through various business ventures as early as 1931.[9] Illegal organizations often employ skilled accountants to facilitate money transfers to do so in order to conceal and invest in clearly legitimate business enterprises. Mayer Lansky, for example, laundered money from illegal casinos (estimated at $1 billion) into Swiss bank accounts, then invested the funds in businesses in Cayman Islands, Caribbean Islands, South America and Hong Kong. Despite his involvement in money laundering for the mafia over a period of 50 years, Lansky was never convicted of these crimes, highlighting the challenge of tracing money laundering transactions. Another well-known case of money laundering is that of "Pablo Escobar", whose fortune was estimated at $9 billion in 1989.[10] This wealth was generated through the sale of narcotics and laundered through various financial institutions.

It involves using various financial transactions to transform illegally obtained money into legal flows (OECD, 2019). Money laundering is a crime that can have serious consequences and can harm a country's economic growth. It is often used to finance terrorist activities and is considered a major global threat.[11] According to Lucian (2010),[12] money laundering involves three stages: the initial deposit or purchase of assets, the use of complex financial transactions to conceal the origin of the funds, and the creation of the appearance of legality through fake invoices or the acquisition of luxury goods.[13] The Financial Action Task Force (FATF) is a global organization promoting the fight against money laundering, identifies three primary methods by which criminal organizations transfer money for the purpose of laundering and integrating it into legal financial systems[14]. These methods include using the financial system, moving physical cash, and transferring goods bought illegally by trade.

According to a 2011 report by the United Nations Office on Drugs and Crime (UNODC), an estimated $2.1 trillion was laundered globally in 2009, equivalent to approximately 3.6% of the world's gross domestic product. Of this amount, around 70% is believed to have been laundered through financial systems. Research by Walker (1999) suggests that 46.3% of laundered money originates in the United States, and 18.9% returns to the United States following the laundering process.[15]

There are some common methods that criminals may use to launder money, including fake invoicing, false lawsuits, layering, and reverse money laundering.

1. False invoices are used to sell goods and art works at substantially higher prices than the estimated value. The seller then returns the goods or works of art to the original owner, who refunds the buyer the difference, minus a commission. This allows the seller to appear as though they have made a legitimate profit, while actually using the sale as a way to launder money.

[8] Bartlett, Herbert Franklin. "A student harvest-work program at West Springfield (Mass.) High School" (1943).

[9] Kumar, Praveen. "Money Laundering in India: Concepts, Effects and Legislation." *International Journal of Research* 3.7 (2015).

[10] Rockefeller, J. D. *The Life and Crimes of Pablo Escobar*. JD Rockefeller, 2016.

[11] Simser, Jeffrey. "Money laundering: emerging threats and trends." *Journal of Money Laundering Control* (2013).

[12] Lucian, Radulescu Dragos. "The concept of money laundering in global economy." *International Journal of Trade, Economics and Finance* 1.4 (2010): 354.

[13] Vitvitskiy, Sergij S., et al. "Formation of a new paradigm of anti-money laundering: The experience of Ukraine." *Problems and Perspectives in Management* 19.1 (2021): 354-363.

[14] Balani, Henry, Joshua J. Lewer, and Mariana Saenz. "Trade based money laundering in select Asian economies: a comparative approach using the gravity model." *Southwestern Economic Review* 44 (2017): 15-26.

[15] Anderson, Jack. "Match fixing and money laundering." *International Sports Betting*. Routledge, (2018). 65-78.

https://doi.org/10.1017/jli.2023.13 Published online by Cambridge University Press

2. False lawsuits involve paying illicit funds into a bank account in a jurisdiction with strict banking secrecy laws, such as the Cayman Islands. The person who paid the funds then initiates a lawsuit against the bank, and in the settlement, the bank pays the investment amount to stop the litigation.
3. Layering involves opening a fake company in a smaller country and using it to open a bank account. The person then contracts with the bank for money laundering services, and sends the bank cash through another client. The client then transfers the money, minus a commission, to the fake company's account.
4. Reverse money laundering involves stealing goods, such as luxury items, and selling them to launder money. The sale profits are invested in other countries' banks. Through banks controlled by money-laundering organizations, new banknotes will be issued with the amount invested, and the country whose currency is being used prints and delivers the banknotes to the launderer's-controlled banks.

How smurfing works in money laundering

Financial crimes have been on the rise in recent years as many wealthy individuals, especially financial institutions have turned into money launderers. This has been triggered by a range of factors such as globalization and an increase in human trafficking where people are exploited to earn huge sums of capital. One way this happens is through illicit financial flows where banks or other financial institutions siphon off billions of dollars from their customers. There are two methods that these criminals use to launder money; one being bank laundering and another through informal settlement schemes. With regard to bank laundering, it involves the process whereby a customer pays his bank for withdrawals from deposits he/she kept with the bank. These withdrawal amounts are then transferred into accounts under the account holder's name. Another method which facilitates money laundering is informal settlement where bank owners take payments from depositors as well as remitting them to themselves. The term smurfing was first used by Frank Baumgartner to refer to the illegal flow of funds emanating from illegal transactions which were not reported to law enforcement authorities.[16] When banks or any other financial institution allows this form of funding they are often termed as money launderers. Most fraud rings involve fraudulent activities such as stock manipulation, insider trading, and corporate espionage among others.

Despite the fact that banks and other financial institutions have a duty of ensuring that their clients do not engage in unauthorized and unlawful activities they should be careful when engaging partners with whom they do business. For example, if one bank wants to engage with another, it may offer to provide security details whereby it is clear that the person they want to engage will not go against the set rules. Failure to undertake necessary measures when engaging with such partners can be classified as money laundering. As mentioned earlier most cases involving financial crimes may not be reported since they are usually hidden from detection. It is also argued that some fraudsters may want to hide the identity of their victims. This is because they are afraid of being caught. To avoid such eventualities, financial institutions should consider undertaking several checks before engaging with their business partners. If the risks involved are too high, then money laundering cannot be the right option. Banks and other institutions should keep in mind that in order to protect themselves they should seek the services of qualified personnel to carry out due diligence on possible clients. Apart from providing enough protection to customers it is also important to ascertain that there are effective controls placed in place which detect illegal activities perpetrated by financial crimes.

On the whole, money laundering has negative implications to society and the economy as it is characterized by losses, increased costs of running the economy, and loss of jobs for those affected since they would have to be relocated to secure job areas. Consequently, the question of whether this practice should be allowed to continue arises. Smurfing is done by entering some amount of information and then sending out the details including money. Usually, two fraudsters will meet up in person and talk over plans for sending transactions. They will enter names, addresses and credit card numbers in order to be able to get cash for these payments without getting the knowledge of anyone. Once this is done an agreement is signed where one party gives the other both the name of their account and an email address where they can check if the transaction is indeed legitimate. The fraudulent group pays all the fees related to this transaction and then sends out a receipt for processing and transferring the money. If the bank finds out about this, all of its checks and balances would instantly reflect that there was a crime

[16] Mutňanský, Michal, and Zuzana Vincúrová. "Detection of unusual financial transaction." *Creative and Knowledge Society* (2017).

https://doi.org/10.1017/jli.2023.13 Published online by Cambridge University Press

being committed. However, most banks do not see anything wrong with such a move because they are usually unaware of the scam.

HOW LAUNDERS GET BENEFITS OF SMURFING

Smurfing has been very useful when it comes to sending and receiving money among many others. But there still exist loopholes in which hackers may use to initiate scams that involve money laundering. Therefore, it is very crucial that all companies, organizations and governments come together in order to curb the vice so as to prevent criminals from exploiting the technology to commit criminal acts. This should be done without much hassle because in the long run, the citizens of any nation benefit since they are assured of security when making large purchases.

With this kind of activity becoming more rampant today, as well as those in the future, there is a need to understand how to deal with such issues at hand. This way we shall reduce the chances of our loved ones and ourselves falling victim to these fraudsters. As such the government should formulate strict laws that would ensure that proper measures are taken in case of any suspicions from individuals carrying out these activities in public places. For instance, the police force should have enough power to investigate and arrest individuals involved in such activities without fear. There is also a lot of fraud that goes on in the world where people are not willing to disclose their identities, especially when they are involved in drug trafficking and human trafficking. This, therefore, creates a loophole where such individuals find themselves taking advantage and committing crimes in order to support their families. Some of them may even be aware of such activities but fail to act as a cautionary measure to prevent them from doing it, knowing very well that they will not get caught.

CHALLENGES OF DETECTING AND PREVENTING SMURFING

There are several challenges that law enforcement and financial institutions face in detecting and preventing smurfing, a common method of money laundering. Some of these challenges include:

1. Complexity: Smurfing often involves multiple individuals and financial institutions; it is difficult to track the flow of illegal funds making it difficult to track the flow of funds. Thus, makes it challenging for law enforcement to detect and prosecute cases of smurfing.
2. Lack of reporting: Financial institutions are required to report suspicious activities to the authorities. But in some cases, they may not be aware that they are dealing with illicit funds. This can make it difficult for law enforcement to detect and prevent smurfing.
3. Evolving techniques: Criminals are constantly adapting and evolving their techniques for money laundering, including smurfing. This means that law enforcement and financial institutions must stay up-to-date on the latest methods and technologies in order to effectively detect and prevent smurfing.
4. Limited resources: Law enforcement agencies often have limited resources and may not have the capacity to investigate every case of suspected money laundering. This can make it difficult to detect and prevent smurfing, especially if the case is complex or involves multiple parties.

COMPARATIVE ASPECTS OF LAW ENFORCEMENT IN INDIA, UK & AUSTRALIA

One challenge is the use of multiple individuals to deposit small amounts of illicit funds into multiple bank accounts. This makes it difficult for law enforcement and financial institutions to detect the activity, as it is often spread out over many different accounts and transactions. Another challenge is the use of shell companies and other legal entities to hide the true ownership of assets. Criminals may use these entities to launder money and make it appear as though the funds were obtained legally. A third challenge is the lack of transparency in certain financial centers, such as the Cayman Islands and the British Virgin Islands, which can make it difficult for law enforcement and financial institutions to trace the movement of illicit funds. To combat these challenges, law enforcement and financial institutions in India and the UK have implemented a number of measures, such as transaction monitoring systems, customer due diligence procedures, and anti-money laundering regulations. These measures help to identify suspicious activity and prevent illicit funds from being deposited into bank accounts. Despite these efforts, smurfing remains a significant challenge for law enforcement and a common method of money

https://doi.org/10.1017/jli.2023.13 Published online by Cambridge University Press

laundering in India and the UK. It is important for these agencies and financial institutions to continue working together to identify and prevent this crime.

But interestingly launders adopted Cuckoo smurfing in Australian borders where syndicates are dedicated syndicates of organized criminals who help other criminals (usually but not necessarily exclusively drug dealers) to move illicit cash. In this smurfing many innocent people were trapped and been questioned and arrested by authorities based on "Lordianto v Commissioner of the AFP; Kalimuthu v Commissioner of the AFP [2019] HCA 39, is the culmination of numerous cuckoo smurfing cases under the Proceeds of Crime Act 2002".[17]

It is important to remember that a single indicator may not be sufficient to identify instances of Cuckoo Smurfing. Instead, providers should use a combination of indicators and conduct further monitoring, including:

- Determining if there is no apparent relationship between the third party and the account holder
- Investigating whether deposits received are related to remittance and whether the account holder is aware of the details of the overseas and/or Australian remittance business
- Engaging with overseas counterparts and attempting to gather more information about the source of overseas funds (where possible)
- Retaining video footage or images of third-party depositors to identify patterns and assist law enforcement efforts
- If a provider believes that an account is being used for Cuckoo Smurfing, they should conduct additional monitoring and consider whether to file a Suspicious Matter Report with AUSTRAC.

International Perspective - Money laundering prevention measures

The European Union's anti-money laundering directive, adopted in year 1991, was the first to define money laundering. This directive, which was based on the 1988 United Nations Convention, requires all member countries of the UN to combat money laundering, with a particular focus on money earned from the sale of drugs.[18] The directive imposes a number of obligations on financial institutions to prevent money laundering, including the requirement to identify and record all clients and to report any suspected money laundering transactions to national authorities.

Banks are the first line of defense against money laundering through electronic payment systems. By identifying and recording all clients and monitoring financial transactions that may be related to money laundering, banks can proactively work to prevent this crime. In addition, countries with strong regulations and measures in place to prevent money laundering can discourage criminal organizations from attempting to launder money through their financial institutions.

In 2018, the Fifth European Union Directive against money laundering was adopted, identifying cryptocurrencies as a potential method of money laundering.[19] As a result, member states were required to ensure the registration and licensing of all cryptocurrency exchange services. This would impose an obligation on these services to maintain records of their clients and allow financial institutions in the country to exercise control over them. These measures aimed to reduce anonymity when purchasing cryptocurrencies and, in turn, reduce the likelihood of money laundering. Preventing money laundering is a global concern, as it can have far-reaching impacts on the stability of the financial system and the integrity of the global economy. There are several organizations that have been established specifically to address this issue. One of the most well-known is the Financial Action Task Force on Money Laundering (FATF). Established in 1989 by the International Monetary Fund, this organization consists of 39 members, including 37 countries and two regional organizations. The FATF works to provide recommendations for the fight against money laundering, terrorism financing, and the proliferation of weapons of mass destruction. It helps national regulators establish legislation that can effectively combat money laundering, and conducts research into money laundering techniques and prevention measures. Through its efforts, the FATF aims to contribute to the stability of the global financial system. Another important global organization in the fight against money laundering

[17] Yuile, Andrew. "Courts and parliament: Judgments: High court judgments." *LAW INSTITUTE JOURNAL* 94.1/2 (2020): 44-45.

[18] Van Ha, Thai. "The Development of European Union Legislative Framework against Money Laundering and Terrorist Financing in the Light of International Standards." *Technium Soc. Sci. J.* 18 (2021): 185.

[19] Frick, Thomas A. "Virtual and cryptocurrencies—regulatory and anti-money laundering approaches in the European Union and in Switzerland." *Era Forum*. Vol. 20. No. 1. Springer Berlin Heidelberg, 2019.

https://doi.org/10.1017/jli.2023.13 Published online by Cambridge University Press

is the Global Task Force to Combat Money Laundering (GTF-AML). The organization cooperates with FATF, World Bank, International Monetary Fund and United Nations Drugs and Crime Agency (UNODC), Interpol and other organizations lead the fight against money laundering. The GTF-AML focuses on increasing transparency around the origin of money and preventing the use of money laundering to finance terrorism.

In Serbia, the Law on "Prevention of Money Laundering and Terrorist Financing" has been enacted to prevent and detect money laundering and terrorist financing.[20] One of the main measures outlined in this law is the requirement for financial institutions to "know their customer" and monitor their business activities. This means that when opening an account or conducting large financial transactions, financial institutions must identify the customer and ensure that the funds being transferred are not derived from illegal activities. In Serbia, this requirement applies to transactions of more than 15,000 Euros in Dinars for non-customers.

The Law on Digital Property in Serbia also regulates the trading of digital currencies, such as cryptocurrencies. However, the use of cryptocurrencies is still largely unregulated and is considered to be in a "gray area," as the potential for abuse and illicit activities involving cryptocurrencies is still being explored.

One of the main ways to combat money laundering is to identify the parties involved in a financial transaction, including both the sender and the recipient. However, the use of cryptocurrencies can pose a challenge in this regard, as the anonymity of these digital assets makes it difficult to track and monitor financial transactions. As a result, countries that have not yet developed regulations for dealing with cryptocurrencies may be particularly vulnerable to money laundering activities. The lack of oversight and transparency in the cryptocurrency market can make it a target for criminals seeking to launder money.

CONCLUSION

One of the main innovations in smurfing has been the increasing use of electronic payment systems. Criminals can now use electronic payment systems to transfer large sums of money across borders quickly and easily, making it easier to launder money. Another development in smurfing has been the increasing use of "layering" to conceal the origin of funds. Layering involves transferring money through multiple accounts or transactions in order to make it more difficult to trace the origin of the funds. Criminals may use a combination of traditional and electronic payment systems to accomplish this. In addition to these developments, there has also been a rise in the use of virtual currencies, such as Bitcoin, for money laundering purposes. Criminals can use virtual currencies to transfer funds anonymously, making it more difficult for law enforcement to trace the origin of the money. Electronic payment systems are particularly vulnerable to abuse because they can transfer large amounts of money to other countries' accounts and the possibility of layered transfers to conceal the origin of funds. The regulation of these systems can be limited in some countries, and existing regulations may not be adapted to newer forms of money laundering such as smurfing and betting or electronic money. While global organizations work to implement measures to prevent money laundering, the effectiveness of these efforts ultimately depends on national legislation and the implementation of regulations. One of the most effective measures for preventing money laundering is the identification of the ordering party and the recipient of financial transactions. Identifying these parties in electronic transactions can help to identify potential money laundering and trigger further monitoring of their transactions. As technology continues to advance, it has an impact on the ways in which money laundering can occur. One example of this is the use of cryptocurrency, which allows for anonymous transactions and makes it harder for organizations to combat money laundering. These digital currencies can be used to trade on exchanges or purchase goods, making it difficult to identify the parties involved in the transaction. This makes it more challenging to fight against money laundering, as well as organized crime and terrorism, which often rely on these methods to move and hide illicit funds. The increasing prevalence of cryptocurrency for buying goods and services, including through the "dark web," also presents additional dangers. While the purchase of cryptocurrency through the internet may be somewhat limited, it can be more readily obtained and used through the "dark web," where it may be used to buy illegal weapons or to rent services such as hacking or hitmen. The rapid development of electronic payment systems has brought many benefits, but it has also presented a new challenge for organizations that work to prevent money

[20] Paunović, Nikola. "Terrorist financing as the associated predicate offence of money laundering in the context of the new EU criminal law framework for the protection of the financial system." *EU and comparative law issues and challenges series* (ECLIC) 3 (2019): 659-683.

https://doi.org/10.1017/jli.2023.13 Published online by Cambridge University Press

laundering and terrorist financing. These systems can be misused to facilitate anonymity in the commission of these crimes, making it more difficult for anti-money laundering and anti-terrorist financing agencies to combat them. Additionally, electronic payment systems can be used to purchase illegal goods, further contributing to the problem. As technology continues to evolve, it is important for agencies to stay vigilant and adapt their strategies to address these challenges.

https://doi.org/10.1017/jli.2023.13 Published online by Cambridge University Press