

Money Laundering in the United States: A Review of Current Regulations and Threats

Grace Hutchinson

A Senior Thesis submitted in partial fulfillment  
of the requirements for graduation  
in the Honors Program  
Liberty University  
Spring 2024

Acceptance of Senior Honors Thesis

This Senior Honors Thesis is accepted in partial fulfillment of the requirements for graduation from the Honors Program of Liberty University.

---

Jamie Stowe, D.B.A.  
Thesis Chair

---

Charlene Geisler, Ph.D.  
Committee Member

---

James H. Nutter, D.A.  
Honors Director

---

Date

**Table of Contents**

- Abstract ..... 4
- Money Laundering in the United States: Comparison of Detective, Preventative, and Enforcement Measures to Other Countries ..... 5
  - Background ..... 5
  - Definitions ..... 6
  - Money Laundering Steps ..... 7
  - Anti-Money Laundering in the United States ..... 7
    - Relevant Parties and Regulations ..... 8
      - Financial Action Task Force ..... 8
      - Financial Crimes Enforcement Network ..... 9
      - Currency and Foreign Transactions Reporting Act of 1970. .... 9
      - Money Laundering Control Act of 1986 ..... 10
      - Anti-Money Laundering Act of 2020 ..... 11
        - Corporate Transparency Act of 2021 ..... 11
  - International Threats and Vulnerabilities ..... 13
    - Professional Money Laundering ..... 13
    - Trade-Based Money Laundering ..... 14
    - Global Art Market ..... 15
      - Freeports ..... 17
      - Cryptocurrency ..... 17
  - Domestic Threats and Vulnerabilities ..... 19
    - Corruption ..... 19
    - Casinos and Gambling Platforms ..... 20
    - Professional Services ..... 21
- Current Prevention Techniques in the United States ..... 21
- Current Detection Techniques in the United States ..... 22
  - Whistleblowers ..... 23
  - Benford’s Law and Machine Learning Methods ..... 24
- US AML Recommendations ..... 25
  - Workload Changes in FinCEN ..... 25
  - Industry-Tailored Money Laundering Resources ..... 26
  - Mandating Risk Assessments ..... 27
- Conclusion ..... 28
- References ..... 29

**Abstract**

Money laundering is the act of hiding illegally obtained money in the financial system. There are three stages of money laundering: placing, layering, and integration. In the United States, the Bank Secrecy Act, monitored by the Financial Crimes Enforcement Network (FinCEN), requires companies to establish an anti-money laundering (AML) compliance program and to exercise customer due diligence as preventative measures. The US government can detect money laundering through Suspicious Activity Reports, Currency Transaction Reports, and whistleblower tips. However, AML threats and vulnerabilities such as Professional Money Launderers, cryptocurrency, and the global art market allow criminals to continue to launder money through and within the United States. By decreasing the workload for FinCEN, developing resources for professional services and other industries, and requiring a risk assessment and technology component, the US can expand their territory in the fight against money laundering.

## **Money Laundering in the United States: Comparison of Detective, Preventative, and Enforcement Measures to Other Countries**

In today's era, the act of laundering money involves over \$2 trillion dollars per year (*Money laundering*, n.d.). In the United States, the Financial Crime Enforcement Network (FINCEN) is the main government department that oversees the enforcement the Bank Secrecy Act, which is the main regulation towards money laundering. Once money has entered the financial system, it is almost impossible to detect; however, some methods of prevention are through anti-money laundering (AML) policies and Know-Your-Client policies. To detect money being laundered, Suspicious Activity Reports (SARs) and Currency Transaction Reports (CTRs) are reported to FinCEN. As AML threats and vulnerabilities persist on international and domestic fronts to the US, reducing the workload for FinCEN, providing resources for professional services and other industries, and mandating a risk assessment and technology component will allow for the US to combat money laundering through different avenues.

### **Background**

A widespread definition of money laundering did not arise until the 1970s, during the investigation into the Watergate Scandal when the term was used by the media (Seagrave, 1995). The Committee for the Re-Election of the President (nicknamed CREEP) had moved around \$500,000 of designated campaign funds to pay burglars to commit perjury on behalf of President Nixon (Kelly, 2020). However, the concept of concealing and mixing illegally obtained money into the financial system has existed for at least 2,000 years (Seagrave, 1995). At the time, regional governments in China banned commercial trading, and thus, Chinese merchants who had earned money from commercial trading laundered their earnings to prevent their arrests. These merchants converted the money into assets that were easily transportable, then moved the

assets into a different region in order to invest it into their businesses. The types of easily transportable assets may have changed over the years, but this technique of moving the money to a different jurisdiction is still used today.

### **Definitions**

While concealing and mixing illegally obtained money into the financial system is a simple definition of money laundering, FinCEN defines money laundering as the act of “disguising financial assets so they can be used without detection of the illegal activity that produced them” (FinCEN, n.d.f., para. 1). Financial assets are highly liquid assets such as cash, gift cards, stocks, and bonds (Tretina & Curry, 2022). Money laundering primarily deals with the concealment of these highly liquid assets, not personal or real property (Albrecht et al., 2019). Personal and real property may be a method to conceal cash or cash equivalents; however, they are not assets that are being concealed. Additionally, while businesses record assets on their books, individuals and groups launder financial assets, not businesses (*Money laundering*, n.d.). However, businesses may be used to conceal the financial assets in their books or on site (if the business is a physical location).

The Financial Accounting Standards Board official defines an asset as having “a present right of an entity to an economic benefit,” where an economic benefit is the “the capacity to provide services or benefits to the entities that use them” (*Statement of financial accounting concepts No. 8*, 2021, p. 5). In general, this means that the right (or ownership of something) grants the entity the ability “to sell, transfer, license, or exchange” it (*Statement of financial accounting concepts No. 8*, 2021, p. 9). Assets can include cash, inventory, short-term investments (such as stocks and bonds), property, intangible assets, and long-term investments (Napoletano & Curry, 2021). As time continues, some assets lose value due to physical

deterioration, wear-and-tear, or obsolescence and lack of adaptability. These assets that lose value are considered depreciable assets, such as buildings, vehicles, and furniture.

### **Money Laundering Steps**

The three steps to successfully launder money through the financial system are placement, layering, and integration (Schneider & Windischbauer, 2008). First, the money must be placed into the financial system. An example of this would be to “deposit currency to bank accounts abroad” to make it appear as if foreign income was made or through smurfing, which is when small amounts are deposited over time to appear inconspicuous (Schneider & Windischbauer, 2008, pp. 394-395). Second, the money must be layered to hide its origins. This is usually accomplished by multiple transactions with intermediaries and transactions between various accounts in different locations. The purpose of layering the funds is to confuse any criminal investigation by complicating the audit trail and making it virtually impossible to trace where the money went. Thirdly, the money must be integrated, and is returned to the criminal legally so they may make use of it. This stage may involve converting the money into assets such as real estate, art, jewelry, etc. The integration stage makes it extremely difficult to determine if money was legally or illegally obtained without “proper documentation as evidence from the previous stages” (Šarkauskaitė, 2023, para. 16).

### **Anti-Money Laundering in the United States**

AML regulations originated after organized crime in the US became a key focus by the media during the 1960s (Von Lampe, n.d.). Many of these organizations hid their proceeds from the government to avoid paying taxes. On October 15, 1970, President Nixon signed the Organized Crime Control Act of 1970, which was geared towards “elimination of the infiltration of organized crime and racketeering into legitimate operations in interstate commerce” (9-

110.000 - *Organized crime and racketeering*, n.d., para. 2). While this act was to reduce or eliminate organized crime from operating legitimately, it did not address how legitimate institutions could detect or prevent organized crime from moving money through the business. Thus, on October 26, 1970, Nixon signed the first anti-money laundering act (*Anti money laundering history*, 2022). Because of criminals' avoidance to report the illegally obtained money to the Internal Revenue Service, the US government currently classifies money laundering as tax fraud (the most common tax fraud) (Albrecht et al., 2019). The United States relies on various parties, regulations, prevention techniques, and detection techniques to combat money launderers, but international and domestic threats and vulnerabilities continue to persist.

### ***Relevant Parties and Regulations***

Since the first law pertaining to laundering money was passed in 1970, many amendments and additions have been passed over the years (FinCEN, n.d.b.). Since the establishment of the Financial Action Task Force, 166 financial intelligence units (FIUs) have emerged internationally and distribute financial intelligence through the Egmont Group, a global sharing platform (Lagerwaard & Goede, 2023). FIUs investigate and combat money laundering in their respective countries and other FIUs. The United States' FIU is the Financial Crimes Enforcement Network, who enforces the Bank Secrecy Act and related regulations (FinCEN, n.d.g.).

**Financial Action Task Force.** At the Group of Seven (G7) summit from July 14 to July 16, 1989, leaders from the United States, United Kingdom, Canada, France, Germany, Italy, and Japan strove to develop a financial action task force from the summit countries and other interested countries to fight money laundering by providing guidance and monitoring of current financial institutions (*Economic declaration*, 1989). The Financial Action Task Force (FATF)



provides FATF Recommendations, which are considered the international standard for AML policies (Jin & Wang, 2021). Additionally, the FATF notes countries that they determine have substantial weaknesses in their AML policies. They also are a platform for countries to share strategies and challenges in implementing AML regulations.

**Financial Crimes Enforcement Network.** In the 1990s, drug trafficking and other threats to the United States were being target by US intelligence efforts (FinCEN, n.d.a.). However, due to a lack of sufficient intelligence analysis on financial vulnerabilities and threats and a lack of “resources to support financial investigations,” the US created FinCEN under the Department of the Treasury (FinCEN, n.d.a., para. 4). FinCEN works to protect the financial system from illegal use, fights money laundering, and encourages national security by collecting, analyzing, and dissemination financial intelligence to decision makers (FinCEN, n.d.g.). FinCEN is guided by and upholds the Currency and Financial Transactions Reporting Act of 1970 and their primary goal is to “follow the money” (FinCEN, n.d.g., para. 7). In 2020, the International Consortium of Investigative Journalists and BuzzFeed News published a large number of FinCEN documents detailing various transactions and suspicious activity over two decades (Lopez-de-Silanes et al., 2023). A subsequent review of the documents demonstrated that many companies over filed SARs, thus reducing the effectiveness of FinCEN. So, despite FinCEN’s efforts to ensure anti-money laundering regulations are up-to-date, public opinion believes that they are receiving too much intelligence and are unable to accurately determine true suspicious activity (Collin, 2020).

**Currency and Foreign Transactions Reporting Act of 1970.** In 1970, in an effort to combat organized crime funding, the Currency and Foreign Transactions Reporting Act was passed (FinCEN, n.d.b.). This act, along with its amendments, other statutes, and any subject

matter related is referred to as the Bank Secrecy Act. It requires US financial institutions to assist US government agencies such as the IRS, the Drug Enforcement Administration (DEA), and the Federal Bureau of Investigation (FBI) in their efforts to combat money laundering. Financial institutions are required to report daily transactions over \$10,000 (Currency Transaction Reports) and to report any suspicious activity (Suspicious Activity Reports) that may constitute money laundering, tax evasion, or other illegal activities. Additionally, these institutions are required to establish an anti-money laundering/countering the finance of terrorism (CFT) program (FinCEN, 2021b). The company specific program is to monitor and ensure BSA compliance and to include a risk portion to direct the company to give more attention to high risk activities and customers. Failure to abide by this act may lead to subsequent lawsuits and investigations.

Since the BSA came into effect, it has allowed law enforcement agencies to prosecute and seize millions of dollars' worth of property and cash from illegal sources (FinCEN, 2021a). SARs and CTRs have been used from county level agencies all the way to national level agencies to further their investigations. However, there are some weaknesses associated with the act. From an internal control level, there is a lack of documentation of due diligence that many financial institutions have (Pogach, 2016). When monitoring transactions and reporting suspicious activity, many financial institutions have "outgrown their monitoring systems" (Pogach, 2016, para. 3). Additionally, some institutions may purchase monitoring systems but neglect to customize the settings for their environment.

**Money Laundering Control Act of 1986.** While the Currency and Foreign Transactions Reporting Act of 1970 attempted to stop the flow of illegal funds by "requiring financial institutions to comply with currency reporting requirements," the Money Laundering Control Act of 1986 (MCLA) gave federal authorities legal ways to target organized crime efforts to conceal

money (Driggers, 2011, p. 930). The MCLA “established money laundering as a crime” and included additions to the BSA (FinCEN, n.d.a., para. 4). MLCA targets criminal offenders directly by prohibiting money laundering and transacting funds derived from a predicate crime (Driggers, 2011). Regarding the predicate crime, the US does not need to trace the money back to the crime, they only need to be able to conclude that the funds were illegally derived. Additionally, the criminal does not need to know where the funds came from and only needs to know that the funds were illegally derived.

**Anti-Money Laundering Act of 2020.** Division F of the National Defense Authorization Act for the year 2021 is the Anti-Money Laundering Act of 2020 (AMLA) (Rosen & Miller, 2022). The AMLA is the largest effort in the US since the Currency and Foreign Transactions Act of 1970 to strengthen anti-money laundering regulations and to detect of financial crime activity. The act established new transparency requirements for public and private companies (the Corporate Transparency Act of 2021), mandated a review of current regulatory framework, encouraged anti-money laundering partnerships domestically and internationally, strengthened BSA whistleblower provisions, and worked to “expand the BSA’s regulatory scope” to include “value that substitutes for currency” (Rosen & Miller, 2022, para. 2).

**Corporate Transparency Act of 2021.** The Corporate Transparency Act (CTA), passed in 2021 by the US Congress, mandated that as of January 1, 2024, small businesses must disclose ownership information for individuals that have beneficial ownership of the company (FinCEN, 2024). Beneficial ownership means any individual who owns at least 25% of the company or who has substantial control over the company’s decisions. Any businesses created by filing a document with the secretary of state or equivalent state offices are required to submit Beneficial Ownership Information (BOI) directly to FinCEN. However, the CTA does not incentivize lying

when submitting beneficial ownership, thus launderers and criminals may still have opportunities to work around the law (Azrilyant, 2021).

In previous years, limited liability corporations (LLCs) could be established anonymously by individuals as a shell company to protect the owners' personal assets and to complete transactions such as international wire transfers (Azrilyant, 2021). International wire transfers allow for the movement of billions of dollars of illicit funds, thus establishing an LLC anonymously was beneficial to criminals (Singh, 2018). LLCs are also simpler to create than corporations or partnerships and the company's profits and losses are passed through to the owner, thus avoiding being taxed at the corporate tax rate percentage. Because of the CTA, a new preventative measure to eliminate anonymous beneficial ownership is now in place and small businesses (such as LLCs) are supposed to be a much smaller vulnerability to the US (Azrilyant, 2021).

### **International and Domestic Money Laundering**

In the United States, international money laundering is considered "transporting or attempting to transport funds in or out of the US with the intent to promote 'specified unlawful activity' or with knowledge that the property involved represents the proceeds of unlawful activity" (*Money laundering control act [MCLA] overview*, n.d., para. 3). Domestic money laundering is "conducting or attempting to conduct financial transactions involving the proceeds of 'specified unlawful activity' knowing that the proceeds are criminally derived" (*Money laundering control act [MCLA] Overview*, n.d., para. 2). Thus, the difference between international and domestic money laundering is that domestic money laundering is money that is known to be criminally derived that is being moved within the US, and international money laundering is money that does not have to be known to be criminally derived (intentionality of

the funds is included) and is moved in or out of the US. As the US continues to use these definitions to investigate and prosecute money launderers, there continues to exist various threats towards the US that are considered international and domestic.

### ***International Threats and Vulnerabilities***

Over time, the risks of global money laundering have continued to rise with the “average global ML/TF risk level increasing from 5.25 in 2022 to 5.31 in 2023 (where 10 is the maximum risk)” (*Basel AML index 2023*, 2023, p. 6). The effectiveness and compliance with FATF Recommendations have improved significantly over the years, but countries still have issues investigating suspicious activity (*Report on the state of effectiveness and compliance with the FATF standards*, 2022). Countries with the weakest measures affect the success of global standards regarding illicit finance (Jin & Wang, 2021). Theoretically, many countries have extensive AML procedures in place (*Basel AML index 2023*, 2023). However, these procedures are not as functional as predicted. For example, technology compliance with FATF Recommendation has dropped 20% since 2021. Other global risks regarding “financial transparency and standards; public transparency and accountability; and political/legal risks” also prohibit the success of AML recommendations (*Basel AML index 2023*, 2023, p. 5).

**Professional Money Laundering.** While money laundering can be accomplished by individuals or groups on their own, Professional Money Launderers (PMLs) are third-party actors who “help criminals launder the proceeds of crime,” usually for a fee (*Professional money laundering*, 2018, p. 11). They also generally “operate on a large scale” and move funds transnationally (*Professional money laundering*, 2018, p. 11). While PMLs may consist of one person (an individual PML), they can also be PML organizations or networks, which are usually two or more PML organizations. PMLs know the money they are moving is illegitimate and are

concerned mostly with getting the money to its destination. In terms of advertising, they usually maintain their reputation by word-of-mouth, but have also been seen to have advertisements on the Dark Web. Operationally, the criminal will transfer the illicit funds to the PML, who will then layer the funds to avoid detection, then they will move the funds back to the criminal to be used.

One particular type of PML are Chinese Money Laundering Organizations (CMLOs), who use “black market foreign exchange” transactions where they match individuals looking to sell a certain currency (typically U.S. dollars) to those that wish to purchase a certain currency (such as Pesos) (*National money laundering risk assessment*, 2022, p. 23). CMLOs are typically wealthy Chinese nationals who launder money on behalf of drug trafficking organizations (Kato, 2022). These Chinese organizations have become popular in recent years because Chinese nationals purchasing the currency are looking to avoid China’s regulations regarding exporting capital. Because these organizations are so vast and primarily operate in the black market, the only regulations that currently exist regard the black market in general.

**Trade-Based Money Laundering.** Trade-Based money laundering is an example of using a business to conceal assets or move money through the business (*Money laundering*, n.d.). Trade-Based money laundering is disguising illegally obtained funds “through legitimate trade transactions” (*Trade-Based money laundering: A global challenge*, 2023, para. 3). Because trade transactions can include commodities, products, or services, and is worldwide, it was identified that unchecked trade-based money laundering caused an overestimate of the amount of money that is laundered each year (*Trade-Based money laundering: A global challenge*, 2023). According to a study by Global Financial Integrity that looked at known trade-based money laundering cases between 2011 and 2021, \$60 billion was identified as laundered funds. Over- and under-invoicing goods, misrepresenting goods being shipped, multiple invoices of goods,

over- and under-shipping phantom shipments, and using information value transfer systems are all potential methods to disguise money (*Trade-Based money laundering: A global challenge*, 2023).

Most merchandise can be used to launder money through trade transactions, but the most common types of merchandise used are transportation vehicles, metals and minerals, agricultural products, and textiles (*Trade-Based money laundering: A global challenge*, 2023). High-value, low-volume and low-value, high volume merchandise are the most vulnerable to trade-based money laundering (*Trade-Based money laundering: Assessing vulnerabilities in economic sectors and products*, 2023b). Generally, products that are not likely to draw suspicion, such as clothing, cosmetics, etc. are used to launder proceeds. Supply-chain functions involved with moving goods are vulnerable to laundered funds because they are potentially easier and cheaper to set up than moving high-value products through an intermediary. An example of trade-based money laundering using supply chain functions is an organization that creates a legitimate transaction to ship cosmetics and when the transaction is approved, the organization's illegal funds are shipped instead. While Know Your Customer and due diligence requirements are being established, more stringent and easily implementable procedures may improve preventing and detecting trade-based money laundering.

**Global Art Market.** During the integration stage, criminals and terrorists find ways to introduce the illegal funds as legal, sometimes through the purchasing and selling of art (Hufnagel & King, 2020). Since art is not depreciable, criminals may purchase artworks as a way to store illicit funds, as a status symbol, or as a medium of exchange for bribes or payments (*Money laundering and terrorist financing in the art and antiquities market*, 2023). However, rather than a crime being committed “against” art, moving money using art is committing a

crime “through” art (Hufnagel & King, 2020, p. 131). One example of art being used in money laundering occurred in 2018, where criminal charges allegedly stated that *Personnages 1965* by Pablo Picasso was involved in a money laundering scheme. As of 2022, the global art market had an estimated value of \$68 billion (McAndrew, 2023). The secondary market, which is art that is resold or not sold by the artist or a representative, makes up 80% of the art market’s value. “The absence of artists and their representatives in the transaction” makes the secondary market more vulnerable to money laundering than the primary market (*Money laundering and terrorist financing in the art and antiquities market*, 2023, p. 11).

Regarding how sales of art are conducted, 40% of sales are conducted at art fairs, 30% of sales are conducted in international public auction houses, and 20% of sales are conducted online (*Money laundering and terrorist financing in the art and antiquities market*, 2023). At art fairs, the art fair organizers are not subject to collecting beneficial ownership identities, provenances of the art, or the source or methods of paying for art. International public auction houses pose an AML risk because they are also not subject to the same requirements, and because suspicious cross-border sales may make it difficult for law enforcement officials to investigate properly. Online sales are a risk because of difficulties verifying identities and sources of funds, and because there is diversification in online sales channels that have the potential to leave no physical trace. Despite these vulnerabilities, some countries are beginning to implement “certain market participants to register and to apply measures including customer due diligence, keeping records, and reporting of suspicious transactions” which, if implemented fully, may reduce some of the vulnerability associated with the art market (*Money laundering and terrorist financing in the art and antiquities market*, 2023, p. 20).



**Freeports.** Freeports are secure storage facilities that are often used to store art and other valuable objects and are located within free trade zones or as tax-free zones near major transport locations (*Money laundering and terrorist financing in the art and antiquities market*, 2023). Any art that is sold and then shipped to a freeport is not subject to sales taxes until the item leaves the location (Gilmour, 2022). Additionally, items that are sold within a freeport are also not subject to a value-added tax (Korver, 2020). While there are tax benefits to storing items in freeports, there are also ownership benefits where beneficial ownership can be disguised by listing the owner as a company or legal entity without the true identity ever being provided, regardless of the current guidelines mandating beneficial ownership information (Zarobell, 2020). It is because of anonymous ownership, tax benefits, and the security of the freeport make them an international vulnerability to the fight against money laundering.

Current regulations regarding freeports, such as the Geneva freeport in Switzerland and the Luxemburg freeport in Luxemburg, are considered sufficient by their respective governments (Ebnetter, 2023). However, particularly in Switzerland, the only requirement is that the name and address of the owner needs to be listed on the inventory list, despite the fact that the freeport contains an estimated 1.2 million artworks valued in total at \$100 billion. In Luxemburg, the government requires that freeports act as “AML-gate keepers” and are required to report suspicious transactions and complete due diligence to identify the beneficial owner (Korver, 2020, p. 2). While these efforts are moving towards similar requirements that financial institutions must uphold, the art market as a whole is in need of stricter regulations (Gilmour, 2022).

**Cryptocurrency.** In 2008, the first digital currency, Bitcoin, was launched (Teichmann & Falker, 2021). Digital currency, now deemed cryptocurrency, uses “blockchain-based,

decentralized systems and can be spent using an electronic software or hardware wallet” (Teichmann & Falker, 2021, p. 92). Blockchain allows the transaction to be present anonymously in a public ledger, which extinguishes the need for a third-party to manage the transaction. Cryptocurrency is traded more in countries that have financial restrictions, such as Palestine or Venezuela, but is also becoming increasingly popular in the United States. In theory, cryptocurrency would be monitored by the public. However, \$24.2 billion in cryptocurrency was involved in illicit activity in 2023, according to a report by Chainalysis, a blockchain data platform (*The 2024 crypto crime report*, 2024). Bitcoin, the most popular cryptocurrency, was used to launder over \$2.5 billion between its launch in 2008 to 2020 (Teichmann & Falker, 2021).

Cryptocurrency as a method to launder funds only makes up about one percent of total laundered funds (Kolmar, 2023). Many criminals and organizations prefer other methods such as wire transfers and trade-based money laundering. Some PMLs are known for using cryptocurrency, and most cryptocurrency that is tracked leads to a small number of organizations (*Crypto money laundering rises 30%, report finds*, 2022). While cryptocurrency as a layering method may not be popular now, but it is estimated that more organizations and criminals will use it in the future.

In the United States, virtual asset corporations are mandated to have an AML compliance program, and this includes mixer corporations, which mix the funds together to disguise the original source (Lemire, 2022). Included in this list are decentralized financial institutions (DeFi). Decentralized financial institutions are “virtual asset protocols and services that purport to allow for some form of automated peer-to-peer (P2P) transactions, often through the use of self-executing code known as ‘smart contracts’ (code deployed on blockchain) based on

blockchain (distributed ledger) technology” (*Illicit finance risk assessment of decentralized finance*, 2023, p. 1). Some of these institutions choose to not comply with the BSA through collection of Know Your Customer information, which opens an avenue for launderers to take advantage of (Bhasker et al., 2023). Additionally, misunderstandings about how AML obligations apply to DeFi services lead to exploitation of the institutions (*Illicit finance risk assessment of decentralized finance*, 2023).

### ***Domestic Threats and Vulnerabilities***

Around \$300 billion is laundered through and within the United States, which is around 15% to 30% of money that is globally laundered (Kolmar, 2023). Additionally, around 90% of laundered funds go undetected even though 90% of money laundering offenders are indicted. Threats such as corruption, gambling platforms, and professional services are considered current domestic threats and vulnerabilities in the US as they usually do not involve international transactions (*National money laundering risk assessment*, 2022).

**Corruption.** Corruption is one of the main predicate crimes associated with money laundering (*The top 3 crimes driving money laundering*, 2022). This refers to bribes and theft by public officials. It is estimated that the global cost of corruption is \$2.6 trillion dollars, where \$1 trillion is from bribes alone (*Global cost of corruption at least 5 per cent*, 2018). Laundering money is favorable to corrupt officials and organizations who steal or receive funds (Mugarura, 2016). While the World Bank and the International Monetary Fund work to encourage good governance and control measures, corruption and money laundering has continued to spread throughout many countries due to “bad governance which has been exploited” (Mugarura, 2016, p. 82).

Corruption is present in every country (Tanzi, 1998). Transparency International Index assesses the perception of corruption in each country by its citizens and generally correlates with the actuality of corruption in a given country. Nicaragua is perceived as the most corrupt country, whereas New Zealand is perceived as the least. While corruption has the potential to affect the global economy and occurs in all countries, it is generally considered a domestic issue specific to the country. In each country, corruption “reduces public revenue, increases public spending,” and increases income inequality, thus inhibiting economic growth (Tanzi, 1998, pp. 27-28). Additionally, since each country is unique, the fight against corruption is unique to each individual country and reform of the country itself is required.

**Casinos and Gambling Platforms.** Despite various efforts to implement AML requirements in casinos in the US, compliance in the sports betting and online gaming industry is limited due to their online capacity, platforms, and large number of cash transactions (*National money laundering risk assessment*, 2022). Gambling companies must maintain AML guidelines such as customer verification, but online gambling platforms are permitted to use other methods to verify a customer’s identity, which are not as substantive as physical casinos. Casinos have large amounts of cash move through every day, and even with SARs being reported for large transactions, illegal funds are still able to move in and out using such techniques as “chip walking” (*National money laundering risk assessment*, 2022, p. 56). Chip walking is when criminals exchange large amounts of cash for chips at one or more casinos, travels to other casinos, gambles for a short time, then exchanges the chips for cash in what appears to be legitimate winnings. Another method of chip walking is to give the chips to another person in another casino for them to exchange back into cash. Chip walking is the “second most selected activity on the SAR form” and these are filed the most in Nevada, Louisiana, California, New

Jersey, and Pennsylvania (*National money laundering risk assessment*, 2022, p. 56). While suspicious activity is being reported, casinos and gambling platforms are a vulnerability in the US and are one of the major focuses by FinCEN.

**Professional Services.** Complicit professionals who abuse their positions to help criminals launder funds are a threat to US anti-money laundering efforts (*National money laundering risk assessment*, 2022). Unwitting professionals also pose a threat in not recognizing the signs of suspicious activity (*Basel AML index 2023*, 2023). This threat partially arises in their supervision. Many professional services firms are considered non-compliant with current AML regulations and do not exercise proper due diligence in collecting customer identities and reporting activities. In the US, attorneys are not required to have comprehensive AML regulations as they are not considered a financial institution (*National money laundering risk assessment*, 2022). Because of this, the legal profession has the potential to be exploited by criminals. Other professional services, such as accounting firms and real estate firms, are subject to comprehensive AML regulation, but most firms are not technologically compliant (*Basel AML index 2023*, 2023).

### **Current Prevention Techniques in the United States**

Money can be laundered through financial institutions that may not be aware of its occurrence (FinCEN, n.d.c.). While AML laws exist mostly to help detect illegal funds moving in and out, §103.125 of title 31 of the Code of Federal Regulations (CFR) in the US lists various ways that a money services business can help prevent money laundering in their business. A money services business is any business that offers services such as money orders, check cashing, etc., and conducts more than \$1,000 in daily money services, or provides monetary transfers. Thus, 31 CFR 103.125 applies to financial institutions.

One method of prevention that is stated in 31 CFR 103.125 is that a money services business must have and maintain an AML compliance program (FinCEN, n.d.c.). This program must be in writing and must list the risks that the business may have based on their “location, size, nature, and volume of the financial services provided” (FinCEN, n.d.c., p. 10). Additionally, the program must incorporate education of employees in high-risk areas, the possibility for an independent review, and procedures in place that allow employees to reasonable comply with US laws.

Another method that financial institutions can incorporate is to establish relationships with customers (FinCEN, n.d.c.). This is sometimes known as Know Your Client (Spenner, 2019). A study by Capital Preferences demonstrated that various techniques to collect information from customers increased growth within the company and employees were able to provide more adequate services. By allowing increased disclosure of customer identification, financial institutions can reduce the risk of organized crime and terrorism from using the money services business (FinCEN, n.d.c.). Some businesses may incorporate a customer identification or verification policy that will be compliant with state and federal laws and allow employees to report suspicious activity. This policy can also encourage the timely reporting of suspicious activities to prevent additional laundering.

### **Current Detection Techniques in the United States**

Money laundering is difficult to detect from an open-source and external auditor’s perspective (Albrecht et al., 2019). Thus, regulations exist to help financial institutions detect and report suspicious activity that could potentially be laundered money. 12 CFR 21.11 states that a national bank must file a SAR with FinCEN if there is insider abuse discovered or suspected, a transaction of \$5,000 or more has been processed through the bank and the bank suspects illegal

activity, or if there are multiple transactions totaling more than \$25,000 and the bank suspects a violation of laws (*12 CFR ch. 1*, n.d.). Additionally, the SAR must be reported within 30 days of the initial detection of facts. This law is designed to review many transactions through national banks. However, this does lead to over 140,000 SARs reported each month (FinCEN, n.d.d.).

The Bank Secrecy Act mandates that financial institutions must report to the Internal Revenue Service (IRS) any transaction that occurs in a single day that is over \$10,000 (also know as CTRs) (FinCEN, n.d.e.). In the 1990s, large transactions were used by fraudsters to launder money, thus the Bank Secrecy Act led to increased disclosure and reporting by financial institutions to detect money laundering (Doppelt, 1990). These reports, along with SARs, are used by federal agencies (and state and local if reported to them) to ascertain the possibility that money is being laundered, however the large volume of reports may hinder timely investigations.

### ***Whistleblowers***

Similar to most fraud schemes, the most common way that tax fraud (thus money laundering) is detected is through whistleblowers, tips, and complaints (Albrecht et al., 2019). As a part of the AMLA of 2020, whistleblower provisions were revised to be comparable to the Dodd-Frank Act of 2010, established by the Securities and Exchange Commission (Rosen & Miller, 2022). Whistleblowers who report suspected acts of money laundering or terrorist financing are protected from retaliation from their employers and may be eligible for compensation (Occupational Safety & Health Administration [OSHA], 2022). While SARs are reported more often, whistleblowers more often have better “insight and access to information about economic crimes that are difficult to detect like money laundering” (*Money laundering and the laws that apply*, n.d., para. 6). Additionally, in the US, non-US citizens are able to report suspicious activity, and if the report leads to prosecution, can receive compensation for their

efforts. However, a literature review by Mehrotra et al. noted that the more specific a company's policy regarding whistleblower protection, the less likely that employees will submit suspicious activity due to management discouragement (2019).

### ***Benford's Law and Machine Learning Methods***

In 2018, a company in Spain was investigated for being involved with a money laundering scheme (Badal-Valero et al.). Over 600 suppliers were moving money in and out of this company, and investigators needed to determine which suppliers were potentially involved in the scheme. A group of researchers applied Benford's Law and various machine learning techniques to determine potential fraudulent suppliers. Benford's Law, discovered by Frank Benford in 1948, is a logarithmic law that states that "the frequency distribution of leading digits in many real-life collections of numbers is not uniform" (Badal-Valero et al., 2018, p. 24). It is present in most data sets and can be used to detect irregularities in transactional data.

The study used calculations of p-values of individual fit to compare to Benford's Law (Badal-Valero et al., 2018). The closeness of fit to Benford's Law would help classify the supplier as fraudulent or legal. Then, four machine learning methods were analyzed to help classify: ridge logistic regression, neural networks, decision trees, and random forests. Ridge logistic regression was used to "classify instances between two categories" (Badal-Valero et al., 2018, p. 27). In the study, neural networks were used to predict fraudulent suppliers, decision trees were used to better classify the data, and random forests were used as an addition to decision trees because they provide more accuracy and ease of use.

While neural networks were determined to have the best performance, random forests were noted to be the best approach (Badal-Valero et al., 2018). However, when comparing similarities of identified fraudulent suppliers between each method, it was recommended to



investigate suppliers that appeared in at least two machine learning methods. Thus, instead of having to investigate 600 suppliers, Spanish investigators may only need to investigate about 12. Badal-Valero et al. concluded that the potential usefulness of Benford's Law and machine learning techniques as a way to detect anomalies in data sets (as demonstrated by their study) may help future investigators discover fraud. However, Benford's Law does not detect fraud, only irregularities in data sets. The methods used by Bada-Valero et al. would need to be altered and customized depending on the organization, potential type of fraud, and other factors, which may prohibit the implementation of Benford's Law as a reliable detection technique.

### **US AML Recommendations**

As money laundering continues to be a prevalent issue in the United States, with multiple international and domestic threats and vulnerabilities present, a few recommendations may be beneficial to the United States (Albrecht et al., 2019). By removing some of the workload from FinCEN, the agency can refocus their efforts on implementing and analyzing emerging patterns in money laundering schemes to create new regulations. Working to educate professional service groups and providing them with resources specific to their industry may encourage due diligence and understanding of the severity of laundering money. Lastly, mandating a risk assessment and technology component to the money service industry and other industries at risk will allow each company to determine where they should focus their AML efforts.

### ***Workload Changes in FinCEN***

FinCEN receives over 1.7 million SARs each year, with that number expected to increase (FinCEN, n.d.d.). However, FinCEN employs less than 400 people, which means on average, each employee reviews over 4,000 SARs each year (Collin, 2020). Additionally, while all US financial institutions are required to report to FinCEN, other countries that use the US dollar to

conduct transactions may also file SARs with FinCEN. One recommendation to ease the load on FinCEN is to outsource SARs to other US government departments or contracting companies. Another recommendation is to permit government employees to work in FinCEN for a period of time. Some intelligence agencies, such as the Defense Intelligence Agency, allow their employees to work at other agencies and organizations for up to two years to learn and use skills to broaden their skillset and practice their “tradescraft” (Defense Intelligence Agency, n.d., para. 7). By working to provide current government employees in other organizations with opportunities to contribute to the fight against money laundering, unity between government agencies will strengthen and FinCEN employees will also have more time to focus their efforts on other threats.

### ***Industry-Tailored Money Laundering Resources***

Regarding industries that must be compliant with the BSA, industry-tailored education on money laundering may help companies submit quality SARs and develop custom AML compliance programs to the specific company. In the Netherlands, the number of SARs submitted has decreased over the years, but there has been an increase in convictions of money-laundering offenses (Collin, 2020). This suggests that the quality of SARs in the Netherlands has increased. One way to work towards quality SARs is educating companies and employees on what signs to look for. All licensed professionals (lawyers, accountants, real estate professionals, etc.) are required to continue their education each year (Milian, 2021). Since many professional services do not exercise proper due diligence (possibly because of a lack of education), providing Continuing Professional Education (CPE) courses for professionals that talk about due diligence and money laundering red flags in the specific industry may help with the quality of SARs being received by FinCEN. While this may seem very broad, by having scenario situations tailored to

the specific industry and practical applications of AML in the industry will help professionals understand the risks that money laundering poses to their industry and applicable steps to report suspicious activity.

Another recommendation for FinCEN to provide to financial institutions and relevant parties is to create an industry-specific AML resource document along with benefits for complying with AML requirements (Collin, 2020). If a simplistic list of AML resources exists for companies, it is not well designed or easy for a typical individual to understand. Including information such as what should be included in a SAR, industry-specific red flags, and general information on how criminals may be moving money through the industry can provide institutions with ideas on how they can improve their AML program and a reference that employees can use in their everyday work.

### ***Mandating Risk Assessments***

In terms of focusing efforts on specific industries, the money services industry receives the most SARs per year (FinCEN, n.d.d.). However, that does not mean that other industries should be ignored. With many companies being technologically noncompliant, requiring a risk assessment instead of suggesting one and requiring a technological component will provide FinCEN and companies with information on what the company can focus their AML efforts on. A technology component that incorporates machine learning techniques and Benford's Law, such as what the study by Badal-Valero et al., may be beneficial for the money services industry and any industry that involves financial transactions (2018). Included in the money services industry are DeFi services, which are largely noncompliant because many institutions do not understand how AML compliances apply to them. In the art and antiquities industry, art fairs are not required to collect beneficial ownership information or provenances of artworks. Online gambling

platforms are not required to have extensive customer identification systems (*National money laundering risk assessment, 2022*). Advertising to these industries and creating regulations specifically tailored towards those institutions comparable to what other industries are required to have will help to alleviate misunderstandings in the industry. For example, since physical casinos are required to collect customer identification, online gambling platforms can require an identification document to verify information.

### **Conclusion**

Money laundering involves large amounts of money, and there are numerous threats to the United States' efforts to combat money laundering on an international front and a domestic front. Some ways to prevent money laundering are to have AML policies in place and to implement Know Your Client rules so that employees can learn to spot money laundering before it can grow. Some ways to detect money laundering are through Suspicious Activity Reports and Currency Transaction Reports as mandated by the Bank Secrecy Act. As the US shifts their focus to specific threats such as cryptocurrency, restructuring the workload of FinCEN, new regulations and education of current industries subject to AML compliance can work to reduce criminals' abilities to launder funds. While these recommendations will never fully eliminate the risk of money laundering, once established, the US can focus their efforts on convicting money launderers and work with the FATF and other countries to combat money laundering on a global scale.

### References

*12 CFR ch. I (1–1–14 Edition)*. (n.d.). Government Publishing Office.

<https://www.govinfo.gov/content/pkg/CFR-2014-title12-vol1/pdf/CFR-2014-title12-vol1-sec21-11.pdf>

*The 2024 crypto crime report*. (2024, February). Chainanalysis.

[https://www.pensamientopenal.com.ar/system/files/Documento\\_Editado1686.pdf](https://www.pensamientopenal.com.ar/system/files/Documento_Editado1686.pdf)

*9-110.000 - Organized crime and racketeering*. (n.d.). US Department of Justice.

<https://www.justice.gov/jm/jm-9-110000-organized-crime-and-racketeering>

Albrecht, W. S., Albrecht, C. O., Albrecht, C. C., & Zimbelman, M. F. (2019). *Fraud examination* (6<sup>th</sup> ed.). Cengage Learning, Inc.

*Anti money laundering history: 1970 to 2022*. (2022, November 7). Comply Advantage.

<https://complyadvantage.com/insights/us-anti-money-laundering-act-aml-history/>

Azrilyant, J. (2021). Shell game: How the corporate transparency act aims to end the illicit use of shell companies, where it fails, and what to do about it. *Public Contract Law Journal*, 51(1).

[https://link.gale.com/apps/doc/A696172654/LT?u=vic\\_liberty&sid=summon&xid=14d7f1ef](https://link.gale.com/apps/doc/A696172654/LT?u=vic_liberty&sid=summon&xid=14d7f1ef)

Badal-Valero, E., Alvarez-Jareno, J. A., & Pavia, J. M. (2018). Combining Benford's Law and machine learning to detect money laundering: An actual Spanish court case. *Forensic Science International*, 282, 24-34. <https://doi.org/10.1016/j.forsciint.2017.11.008>

*Basel AML index 2023: 12th public edition* (2023). Basel Institute on Governance.

[https://index.baselgovernance.org/api/uploads/Basel\\_AML\\_Index\\_2023\\_12th\\_Edition\\_879b07b7b2.pdf](https://index.baselgovernance.org/api/uploads/Basel_AML_Index_2023_12th_Edition_879b07b7b2.pdf)

- Bhasker, S., Grady, M. P., & Mosley, K. G. (2023). Cryptocurrency and anti-money laundering enforcement and regulation. *Criminal Justice*, 38(2).  
[https://link.gale.com/apps/doc/A759873238/LT?u=vic\\_liberty&sid=summon&xid=6b8dfd9d](https://link.gale.com/apps/doc/A759873238/LT?u=vic_liberty&sid=summon&xid=6b8dfd9d)
- Collin, M. (2020, September 25). *What the FinCEN leaks reveal about the ongoing war on dirty money*. Brookings. <https://www.brookings.edu/articles/what-the-fincen-leaks-reveal-about-the-ongoing-war-on-dirty-money/>
- Crypto money laundering rises 30%, report finds*. (2022, January 26). BBC.  
<https://www.bbc.com/news/technology-60072195>
- Defense Intelligence Agency. (n.d.). *Career development*. US Department of Defense.  
<https://www.intelligencecareers.gov/dia/career-development>
- Doppelt, A. B. (1990). Telltale signs of money laundering. *Journal of Accountancy*, 169(3).  
<https://www.ojp.gov/ncjrs/virtual-library/abstracts/telltale-signs-money-laundering>
- Driggers, A. (2011). Money laundering. *American Criminal Law Review*, 48(2).  
[https://repository.library.georgetown.edu/static/flexpaper/template.html?path=/bitstream/handle/10822/1080991/aclr\\_vol0048\\_no0002.pdf?sequence=2&isAllowed=y](https://repository.library.georgetown.edu/static/flexpaper/template.html?path=/bitstream/handle/10822/1080991/aclr_vol0048_no0002.pdf?sequence=2&isAllowed=y)
- Ebnetter, C. (2023, July 27). Unlocking the secrets of the Geneva Freeport: A haven for priceless art and tax evasion. *The Swiss Times*. <https://theswisstimes.ch/unlocking-the-secrets-of-the-geneva-freeport-a-haven-for-priceless-art-and-tax-evasion/>
- Economic declaration*. (1989, July 16). G7 Research Group.  
<http://www.g8.utoronto.ca/summit/1989paris/communique/index.html>
- Financial Crimes Enforcement Network. (2021a, June 24). *FinCEN recognizes the significant impact of bank secrecy act on law enforcement efforts*. Department of the Treasury.

<https://www.fincen.gov/news/news-releases/fincen-recognizes-significant-impact-bank-secrecy-act-data-law-enforcement>

Financial Crimes Enforcement Network. (2021b, December 15). Review of bank secrecy act regulations and guidance. *The Federal Register*, 86(238).

<https://www.govinfo.gov/content/pkg/FR-2021-12-15/pdf/2021-27081.pdf>

Financial Crimes Enforcement Network. (2024). *Beneficial ownership information reporting*.

Department of the Treasury. [https://www.fincen.gov/boi-faqs#B\\_2](https://www.fincen.gov/boi-faqs#B_2)

Financial Crimes Enforcement Network. (n.d.a.). *BSA timeline*. US Department of the Treasury.

<https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act/bsa-timeline>

Financial Crimes Enforcement Network. (n.d.b.). *History of anti-money laundering laws*. US

Department of the Treasury. <https://www.fincen.gov/history-anti-money-laundering-laws>

Financial Crimes Enforcement Network. (n.d.c.). *Money laundering prevention: A money*

*services business guide*. Department of the Treasury.

[https://www.fincen.gov/sites/default/files/guidance/msb\\_prevention\\_guide.pdf](https://www.fincen.gov/sites/default/files/guidance/msb_prevention_guide.pdf)

Financial Crimes Enforcement Network. (n.d.d.). *SAR filings by industry*. US Department of the

Treasury. <https://www.fincen.gov/reports/sar-stats/sar-filings-industry>

Financial Crimes Enforcement Network. (n.d.e.). *The bank secrecy act*. Department of the

Treasury. <https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act>

Financial Crimes Enforcement Network. (n.d.f.). *What is money laundering?* US Department of

the Treasury. <https://www.fincen.gov/what-money-laundering>

Financial Crimes Enforcement Network. (n.d.g.). *What we do*. US Department of the Treasury.

<https://www.fincen.gov/what-we-do>

Gilmour, P. M. (2022). Freeports: Innovative trading hubs or centres for money laundering and tax evasion? *Journal of Money Laundering Control*, 25(1), 63-71.

<https://doi.org/10.1108/JMLC-01-2021-0002>

*Global cost of corruption at least 5 per cent of world gross domestic product, Secretary-General tells security council, citing world economic forum data.* (2018, September 10). United Nations. <https://press.un.org/en/2018/sc13493.doc.htm>

Hufnagel, S., & King, C. (2020). Anti-money laundering regulation and the art market. *Legal Studies*, 40(1), 131-150. <https://doi.org/10.1017/lst.2019.28>

*Illicit finance risk assessment of decentralized finance.* (2023, April). US Department of the Treasury. <https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf>

Jin, M., & Wang, Z. (2021). Research on the relationships between FATF assessment effectiveness, compliance and money laundering risk. *2021 International Conference on Computer, Blockchain and Financial Development (CBFD)*, 15–536.

<https://doi.org/10.1109/CBFD52659.2021.00113>

Kato, N. (2022, March 16). *U.S. Treasury identifies ongoing and emergent money laundering risks and vulnerabilities.* JDSupra. <https://www.jdsupra.com/legalnews/u-s-treasury-identifies-ongoing-and-1810996/>

Kelly, M. (2020, May 14). *The history of CREEP and its role in the Watergate Scandal.* Thought Co. <https://www.thoughtco.com/what-was-creep-105479>

Kolmar, C. (2023, March 29). *20 money laundering statistics [2023] facts about money laundering in the U.S.* Zippia. <https://www.zippia.com/advice/money-laundering-statistics/#:~:text=In%20fact%2C%20there%20is%20tons,and%20%242%20trillion%20each%20year>



Korver, R. (2020). *Money laundering and tax evasion risks in freeports and customs warehouses.*

Special Committee on Financial Crimes, Tax Evasion, and Tax Avoidance.

<https://www.europarl.europa.eu/cmsdata/155722/5%20->

[2002%20EPRS\\_Freeparts%20in%20the%20EU\\_exec.sum.pdf](https://www.europarl.europa.eu/cmsdata/155722/5%20-2002%20EPRS_Freeparts%20in%20the%20EU_exec.sum.pdf)

Lagerwaard, P., & Goede, M. (2023). In trust we share: The politics of financial intelligence sharing. *Economy and Society*, 52(2), 202-226.

<https://doi.org/10.1080/03085147.2023.2175451>

Lemire, K. A. (2022, September 26). *Cryptocurrency and anti-money laundering enforcement.*

Reuters. <https://www.reuters.com/legal/transactional/cryptocurrency-anti-money-laundering-enforcement-2022-09-26/>

Lopez-de-Silanes, F., McCahery, J. A., & Pudschedl, P. C. (2023). Corporate governance and value preservation: The effect of the FinCEN leak on banks. *Law and Contemporary Problems*, 85(4), 247-298.

<https://web.p.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=0&sid=af9510c8-d6f3-4a8d-bd63-a4f904e6d8d9%40redis>

McAndrew, C. (2023). *The art market 2023: A report by Art Basel & UBS.* Art Basel.

<https://theartmarket.artbasel.com/download/The-Art-Basel-and-UBS-Art-Market-Report-2023.pdf>

Mehrotra, S., Mishra, R. K., Srikanth, V., Tiwari, G. P., & Kumar, E. V. M. (2020). State of whistleblowing research: A thematic analysis. *FIIB Business Review*, 9(2), 133-148.

<https://doi.org/10.1177/2319714519888314>

Milian, J. (2021, December 3). *Continuing education requirements in the US: An overview.*

Ascend. <https://ascend.thentia.com/united-states/continuing-education-requirements-us/>

*Money laundering.* (n.d.). United Nations Office on Drugs and Crime.

<https://www.unodc.org/unodc/en/money-laundering/overview.html>

*Money laundering and the laws that apply.* (n.d.). National Whistleblower Center.

<https://www.whistleblowers.org/money-laundering-and-the-laws-that-apply/>

*Money laundering and terrorist financing in the art and antiquities market.* (2023, February).

Financial Action Task Force. <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Money-Laundering-Terrorist-Financing-Art-Antiquities-Market.pdf.coredownload.pdf>

*Money laundering control act (MLCA) overview.* (n.d.). Willkie Compliance.

<https://complianceconcourse.willkie.com/resources/anti-money-laundering-us-money-laundering-control-act/>

Mugarura, N. (2016), Uncoupling the relationship between corruption and money laundering crimes. *Journal of Financial Regulation and Compliance*, 24(1), 74-89.

<https://doi.org/10.1108/JFRC-01-2014-0002>

Napoletano, E., & Curry, B. (2021, March 10). What are assets? *Forbes*.

<https://www.forbes.com/advisor/investing/what-are-assets/>

*National money laundering risk assessment.* (2022, February). U.S. Department of the Treasury.

<https://home.treasury.gov/system/files/136/2022-National-Money-Laundering-Risk-Assessment.pdf>

Occupational Safety and Health Administration. (n.d.). *Whistleblower protection for reporting money laundering.* US Department of Labor.

<https://www.osha.gov/sites/default/files/publications/OSHA4176.pdf>

Pogach, S.R. (2016, August 8). *Common issues and problems in BSA enforcement actions*.

National Association of Federally-Insured Credit Unions.

<https://www.nafcu.org/compliance-blog/common-issues-and-problems-bsa-enforcement-actions>

*Professional money laundering*. (2018, July). Financial Action Task Force. [https://www.fatf-](https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Professional-Money-Laundering.pdf.coredownload.pdf)

[gafi.org/content/dam/fatf-gafi/reports/Professional-Money-Laundering.pdf.coredownload.pdf](https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Professional-Money-Laundering.pdf.coredownload.pdf)

*Report on the state of effectiveness and compliance with the FATF standards*. (2022, April).

Financial Action Task Force. <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Report-on-the-State-of-Effectiveness-Compliance-with-FATF-Standards.pdf.coredownload.pdf>

Rosen, L.W., & Miller, R.S. (2022, September 27). *The Financial Crimes Enforcement Network (FinCEN): Anti-Money laundering act of 2020 implementation and beyond*.

Congressional Research Service. <https://crsreports.congress.gov/product/pdf/R/R47255>

Šarkauskaitė, Ž. (2023, August 2). *What is integration in money laundering?* Swiss Money.

<https://swissmoney.com/what-is-integration-in-money-laundering/>

Seagrave, S. (1995). *Lords of the rim: The invisible empire of the overseas Chinese*. Putnam's Sons.

Singh, P. (2018, February 24). *LLC, limited liability companies as shell companies for money*

*laundering*. LinkedIn. <https://www.linkedin.com/pulse/llc-limited-liability-companies-shell-money-laundering-singh/>

- Spenner, P. (2019). Do you really know your client? *Journal of Financial Planning*, 32(4), 16-17. <https://go.openathens.net/redirector/liberty.edu?url=https://www.proquest.com/trade-journals/do-you-really-know-your-client/docview/2206003509/se-2?accountid=12085>
- Statement of financial accounting concepts No. 8: Conceptual framework for financial reporting.* (2021, December). Financial Accounting Standards Board. [https://viewpoint.pwc.com/dt/us/en/fasb\\_financial\\_accou/statements\\_of\\_financ/con\\_8\\_conceptual\\_fra/assets/con8chapter4.pdf](https://viewpoint.pwc.com/dt/us/en/fasb_financial_accou/statements_of_financ/con_8_conceptual_fra/assets/con8chapter4.pdf)
- Tanzi, V. (1998, May). *Corruption around the world: Causes, consequences, scope, and cures.* International Monetary Fund. <https://www.imf.org/external/pubs/ft/wp/wp9863.pdf>
- Teichmann, F. M. J., & Falker, M. (2021). Money laundering via cryptocurrencies – potential solutions from Liechtenstein. *Journal of Money Laundering Control*, 24(1). <https://www.emerald.com/insight/content/doi/10.1108/jmlc-04-2020-0041/full/html>
- The top 3 crimes driving money laundering.* (2022, January 11). Napier AI. <https://www.napier.ai/post/predicate-crimes-money-laundering>
- Trade-Based money laundering: A global challenge.* (2023a, February 2). Global Financial Integrity. <https://gfintegrity.org/report/trade-based-money-laundering-a-global-challenge/>
- Trade-Based money laundering: Assessing vulnerabilities in economic sectors and products.* (2023b, October 2). Financial Crime Academy. <https://financialcrimeacademy.org/trade-based-money-laundering/#:~:text=A%20wide%20range%20of%20economic,launders%20to%20launder%20the%20money.>
- Tretina, K., & Curry, B. (2022, December 1). *9 types of investment assets.* Forbes. <https://www.forbes.com/advisor/investing/types-of-investment-assets/>

Von Lampe, K. (n.d.). *The concept of organized crime in historical perspective*. Organized Crime Research. <http://www.organized-crime.de/lauhtm01.htm>

Zarobell, J. (2020). Freeports and the hidden value of art. *Arts*, 9(4), 117.  
<https://doi.org/10.3390/arts9040117>