South Carolina Journal of International Law and Business

Volume 19 | Issue 2 Article 8

2023

INTERNATIONAL RISE OF CRYPTOCURRENCY: A COMPARATIVE REVIEW OF THE UNITED STATES, MEXICO, SINGAPORE, AND SWITZERLAND'S ANTI-MONEY LAUNDERING (AML) REGULATION

Michael G. Lindsay

INTERNATIONAL RISE OF CRYPTOCURRENCY: A COMPARATIVE REVIEW OF THE UNITED STATES, MEXICO, SINGAPORE, AND SWITZERLAND'S ANTI-MONEY LAUNDERING (AML) REGULATION

Michael G. Lindsay

INTRODUCTION

In his July 2022 address to the G20 Summit in Bali, Indonesia, Financial Action Task Force (FAFT) President T. Raja Kumar directly addressed the "failure" of G20 members and other countries to "lead by example" in regulating money laundering across the global financial market.[1] According to President Kumar, less than 12% of surveyed countries are enforcing the FAFT's 'travel rule'—guidance that encourages the application of customer due diligence (CDD) and know your customer (KYC) mechanisms.[2] The failure to implement timely and proportional anti-money laundering (AML) regulations, warned President Kumar, exposes countries and financial markets to fraud, money laundering, and terrorism—"failure to [implement these regulations] will allow criminals to profit from these gaps, at the expense of governments and their people."[3]

The Financial Action Task Force, an international body that offers financial guidance on the increased risks associated with money laundering, is comprised of thirty-seven member jurisdictions and two regional jurisdictions.[4] As with most other international bodies, these FATF members bring different perspectives, policies, and opinions on how to minimize money laundering risks—including those associated with cryptocurrencies. For example, China has instituted an outright ban on the sale of cryptocurrencies through initial coin offerings.[5] In comparison, Japan embraces cryptocurrencies by classifying several companies as "registered cryptocurrency exchange operators."[6] Once given this designation, companies are required by Japan's Financial Services Agency to "build a 'strong' computer system to support the cryptocurrency and check the identity of users to prevent money laundering."[7] In recent years, this crypto policy led to Japan's recognition of Bitcoin as legal tender.[8] Hence, each country has a

[1] T. Raja Kumar, President, Fin. Action Task Force, FATF President at the G20 Finance Ministers and Central Bank Governors' Meeting, 15-16 July 2022 (Jul. 16, 2022) (transcript available at https://www.fatf-gafi.org/en/publications/Fatfgeneral/Speech-g20-fmcbg-july-2022.html) (accessed 25 Oct. 2022).
[2] *Id.*
[3] *Id.*
[4] *FATF Members and Observers*, FIN. ACTION TASK FORCE (last visited 25 Oct. 2022), https://fatfgaf.org/about/membersandobservers/index.html. The current membership, as of 25 Oct. 2022, of the FATF includes Argentina, Australia, Austria, Belgium, Brazil, Canada, China, Denmark, European Commission, Finland, France, Germany, Greece, Gulf Cooperation Council, Hong Kong, Iceland, India, Ireland, Israel, Italy, Japan, the Republic of Korea, Luxembourg, Malaysia, Netherlands, New Zealand, Norway, Portugal, Russia, Saudi Arabia, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom, and United States.
[5] SETH C. ORANBURG, A HISTORY OF FINANCIAL TECHNOLOGY AND REGULATION: FROM AMERICAN INCORPORATION TO CRYPTOCURRENCY AND CROWDFUNDING 140 (Oxford Univ. Press, 2022). This statement was jointly extended by the China Securities Regulatory Commission, China Banking Regulatory Commission, People's Bank of China, and the China Insurance Regulatory Commission, explaining that this constitutes "illegal fund-raising activity." Initial Coin Offerings (ICOs), by definition, are "transactions in securities according to the SEC and fall under relevant securities laws."
[6] *Id.*
[7] *Id.*
[8] *Id.*

unique and tailored approach to how it regulates cryptocurrencies within its jurisdiction. This is where the problem lies.

In recent years, there have been growing calls from international bodies and domestic jurisdictions for the regulation of cryptocurrencies on an international scale. In comparison to traditional payment systems, such as credit and debit card transactions, cryptocurrencies are transmitted across jurisdictions with increased speed and anonymity. Many countries, according to policymakers and regulators, continue to rely on outdated monitoring frameworks that do not account for these characteristics. In response to this concern, this paper seeks to propose a common, international framework—one that is grounded in the effective regulations of FATF member countries. By establishing an international regulation to mitigate and combat the increasing rise of money laundering via cryptocurrencies, countries would not only help minimize the regulatory gap between the fast-developing virtual asset market and lagging regulatory structures, but they would also increase consumer confidence in participating in the international cryptocurrency market.

The Article consists of four parts. Part II explains the history of the cryptocurrency market, introduces the Financial Action Task Force, and explains the relationship between the two. Given that international regulation does not exist, Part III examines the domestic regulations of four countries—the United States, Mexico, Switzerland, and Singapore. These countries were selected by considering: 1) their willingness and ability to implement AML regulation of cryptocurrencies, 2) the effectiveness of the regulation, and 3) the justifications for enacting domestic AML crypto regulation. Part IV examines the characteristics drawn from the four selected countries and considers their application on an international scale. In addition, this paper will consider ways in which domestic regulations appear inadequate for direct application on the international scale; as a result, the findings suggest ways in which the applied regulations can be enhanced in order to best address international risks.

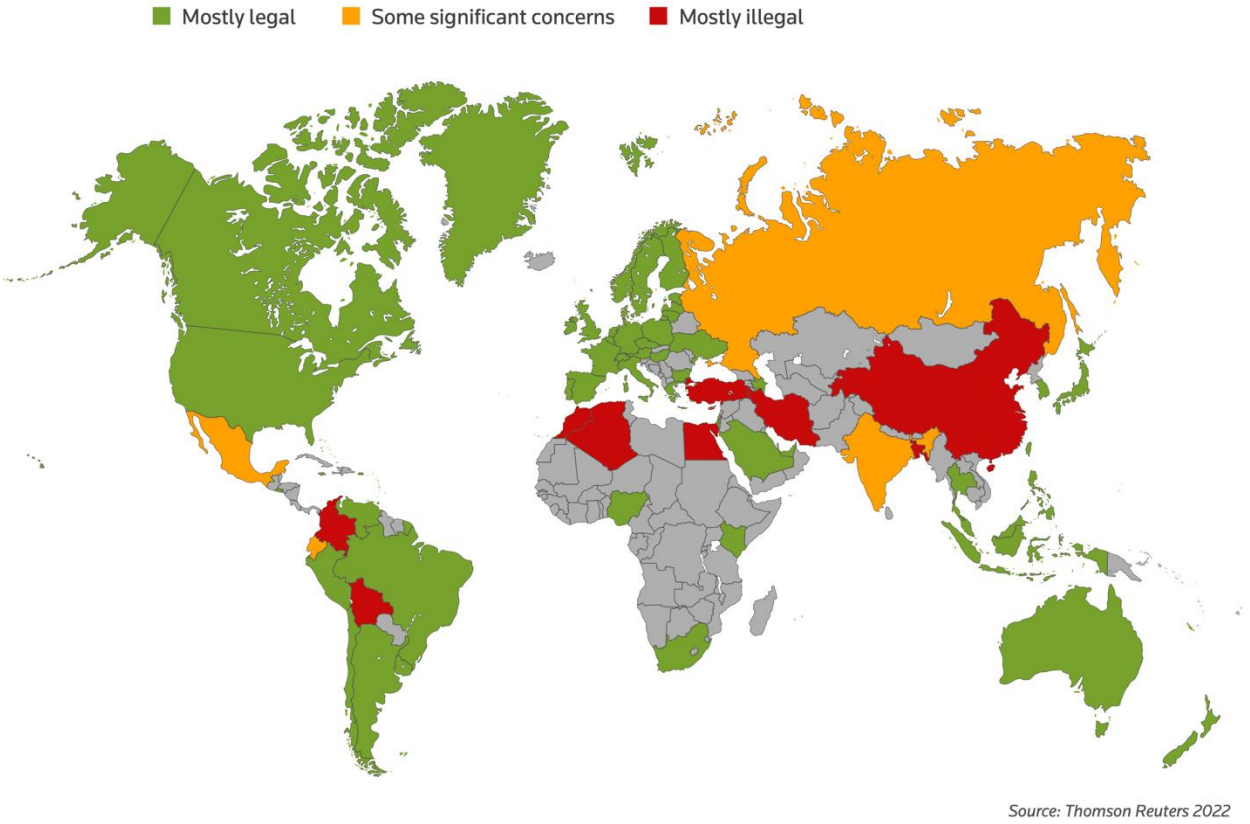
II. BACKGROUND

While the concept of encrypting messages is a relatively ancient practice, modern cryptographic theory is relatively new. In 2008, a nine-page paper was sent out under the pseudonym Satoshi Nakamoto that detailed a "new cash system that's fully peer-to-peer."[9] This email led to the emergence of Bitcoin—one of the world's most prevalent forms of cryptocurrency.[10] With the use of a pseudonym and numeric identifiers to complete transactions, criminals are attracted to holding Bitcoin and other cryptocurrencies.[11] While pseudonymity may prevent a buyer or seller from knowing an actor's true identity, it allows criminals to develop their own reputation over time while remaining virtually anonymous.[12]

[9] ORANBURG, *supra* note 5, at 133.
[10] *Id*. "Cryptocurrency," by definition, is "a digital asset created and designed to be a means of exchange utilizing advanced cryptographical procedures to verify and secure the transfer the value between users – Bitcoin, Litecoin, Ether, to name a few."
[11] *Id*. at 116-17.
[12] *Id*. at 117.

FIGURE 1. CRYPTOCURRENCY REGULATIONS BY COUNTRY[13]

With the emergence of various cryptocurrencies, countries continue to grapple with regulatory implementation for which federal agencies are primarily responsible.[14] Additionally, foreign government agencies (FGAs), national government agencies (NGAs), and nongovernmental organizations (NGOs) play a role in issuing guidance and assessments on a federal government's handling of cryptocurrency.[15] However, it is important to note that at both the domestic and international level, application of regulation to cryptocurrencies becomes



difficult—these assets were "invented and designed to avoid regulation."[16] Thus, the efforts of many countries to regulate cryptocurrencies are ineffective—leaving the virtual instruments largely unregulated.

A. MONEY LAUNDERING

Money laundering is a mechanism used by criminal actors and groups to conceal the origins of funds used in illegal activities. The money laundering process, as defined in the Vienna and

[13] *Cryptos on the rise 2022, Compendium: Cryptocurrency regulations by country*, THOMSON REUTERS 2 (2007), https://www.thomsonreuters.com/en-us/posts/wp-content/uploads/sites/20/2022/04/Cryptos-Report-Compen dium-2022.pdf.
[14] ORANBURG, *supra* note 5, at 130.
[15] *Id.*
[16] *Id.*

Palermo Conventions, is comprised of three steps—conversion, concealment, and acquisition.[17] Through conversion, the proceeds of illegal activities are transferred to a third party—oftentimes a person, a group of persons, an organization, or a business—with the understanding and knowledge that said proceeds originate from illegal activities.[18] Conversion occurs when the ill-gotten gains are first introduced into the financial system; depending upon their value, the transferred funds may be subject to reporting requirements. By undertaking concealment, individuals or groups can cloud the "true nature, source, location, disposition, movement or ownership or right" of illicit funds.[19] Also referred to as "layering," a criminal will shift money and conduct a series of transactions in an effort to distort and complicate any paper trail. For example, an individual may conduct an international wire transfer between banks accounts–with multiple account holders–at different banks. Lastly, a second buyer acquires the proceeds of illicit funds–these buyers may or may not know that these funds are ill-gotten.[20] On both domestic and international levels, money laundering can produce severe economic, social, and security concerns.[21] For example, cumulative money laundering actions can undermine the legitimacy and integrity of financial market operations from consumers and the government; in extreme cases, money launderers engage in these activities with the purpose to disrupt and overthrow a jurisdiction's government through terrorist-like monetary tactics.[22] Due to these concerns, international leaders created the Financial Action Task Force to minimize, mitigate, and manage these risks.

B. THE FINANCIAL ACTION TASK FORCE (FATF)

In 1989, leaders of the G-7 Summit in Paris, France, established the FATF, an international organizational body with the intent to establish a global standard on the prevention of money laundering.[23] Developed out of an urgency to address the increasing risk of money laundering, the G-7 leaders, the President of the European Commission, and eight other countries developed *Forty Recommendations*–a comprehensive plan to fight money laundering–in April of 1990.[24] The original *Forty Recommendations* covered a number of key elements, including: the scope of the criminal offense of money laundering, measures to be taken by financial institutions (such as

[17] *Anti-Money Laundering/Combating the Financing of Terrorism*, INT'L MONETARY FUND, https://www.imf.org/external/np/leg/amlcft/eng/aml1.htm#moneylaundering (last visited 25 Oct. 2022).
[18] *Id.*
[19] *Id.*
[20] *Id.*
[21] John McDowell & Gary Novis, *Consequences of Money Laundering and Financial Crime*, 6 ECON. PERSP. 6, 6-8 (2001), https://www.ojp.gov/ncjrs/virtual-library/abstracts/consequences-money-laundering-and-financial-crime. McDowell and Novis point to effects including: the undermining of the financial sector and the integrity of financial markers, loss of control over financial policy, "economic distortion and instability," revenue loss, and risks of reputation loss and privatization efforts.
[22] *Id.*; *see also* Press Release, Fed. Bureau of Investigation (FBI): Las Vegas Division, Member of Anti-Government Movement Pleads Guilty to Laundering Money for FBI Undercover Agents (Mar. 25, 2011), https://archives.fbi.gov/archives/lasvegas/press-releases/2011/lv032511.htm. The alleged money launderers were "heavily involved in the Sovereign Movement, an extreme anti-government organization whose members attempt to disrupt and overthrow government and other forms of authority by using 'paper terrorism' tactics, intimidation and harassment, and violence."
[23] INT'L MONETARY FUND, *supra* note 17.
[24] *History of the FATF*, FIN. ACTION TASK FORCE, https://www.fatf-gafi.org/en/the-fatf/history-of-the-fatf.html; *FATF 40 Recommendations*, FIN. ACTION TASK FORCE (2004), https://www.fatfgafi.org/en/publications/Fatfrecommendations/The40recommendationspublishedoctober2004.html#:~:text=The%2040%20Recommendations%20provide%20a,adopted%20by%20many%20international%20bodies.

customer due diligence and reporting suspicious activity), institutional measures to be taken by each country, and the need for international cooperation. Over the last thirty years, the FATF has continued to issue additional standards and guidelines to address innovations in technology, increased sophistication of the global financial network, and the expansion of money laundering threats.[25] Through the issuance of these *Recommendations*, the FAFT encourages member and non-member countries to implement "essential measures" to counterattack and mitigate money laundering risks.[26]

These "essential measures" are designed, per the FATF, to:

(i) "identify the risks, and develop policies and domestics coordination;
(ii) pursue money laundering, terrorist financing and the financing of proliferation;
(iii) apply preventative measures for the financial sector and other designated sectors;
(iv) establish powers and responsibilities for the competent authorities (e.g., investigative, law enforcement and supervisory authorities) and other institutional measures;
(v) enhance the transparency and availability of beneficial ownership information of legal persons and arrangements; and
(vi) facilitate international cooperation."[27]

In addition to encouraging countries to comply with the *Recommendations*, the FATF provided language that encourages countries to take a more tailored approach in addressing specific high-risk areas.[28] In recent years, the FATF has increased its guidance on money laundering within the international cryptocurrency industry. Importantly, there does not exist a centralized regulatory or oversight body specifically for the mitigation and investigation of cryptocurrencies.[29] Due to the lack of this type of body, the efficiency and effectiveness of prosecuting criminals is complicated.[30] This decentralized approach to monitoring cryptocurrency transactions also complicates the ability of law enforcement and regulatory agencies to access pertinent records as they are often held amongst multiple entities across multiple jurisdictions.[31]

III. REGULATION FROM AROUND THE WORLD

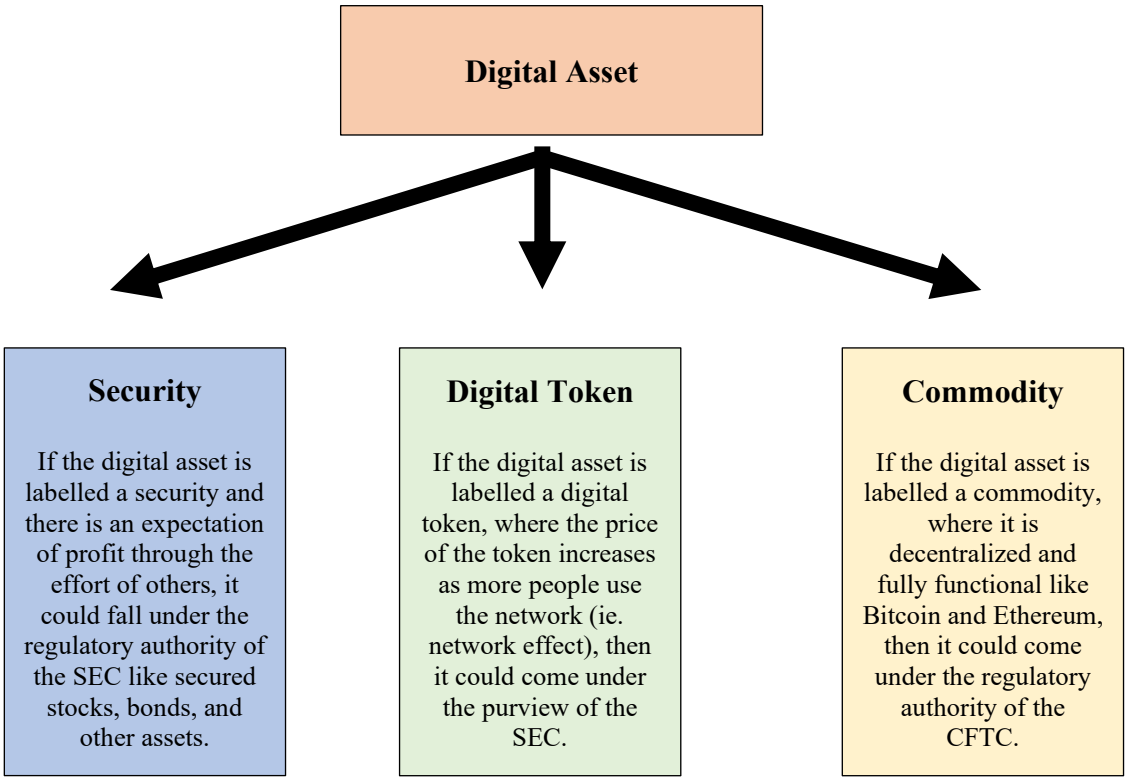
A. THE UNITED STATES

As one of the most proactive countries to regulate money laundering, the United States is frequently observed as a guide to countries developing and implementing money laundering regulation. In the United States, the regulation of cryptocurrency is largely administered by the Financial Crimes Enforcement Network (FinCEN), the Securities and Exchange Commission

[25] *Id.*; *see also International Standards on Combating Money-Laundering and the Financing of Terrorism & Proliferation*, FIN. ACTION TASK FORCE (2012), https://www.fatf-gafi.org/content/dam/recommandations/pdf/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf.
[26] International Standards, *supra* note 25, at 7.
[27] *Id.*
[28] *Id.* at 8.
[29] *Virtual Currencies–Key Definitions and Potential AML/CFT Risks*, FIN. ACTION TASK FORCE 9 (2014), https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf.
[30] *Id.*
[31] *Id.* at 9-10.

(SEC), the Federal Trade Commission (FTC), and the Commodity Futures Trading Commission (CFTC)–all of which implement guidance, policy, and rules incorporating the Bank Secrecy Act (BSA).[32] BSA was passed to address money laundering risks, to improve regulatory oversight, and to ensure financial certainty within the United States' jurisdiction.[33]Despite efforts undertaken by regulators and the federal government to implement policies and laws to combat money laundering, some digital investors and policymakers are concerned that the exponential growth of the digital assets sector will produce unanticipated consequences and an increased exposure to new and developing money laundering risks.[34]

FIGURE 1. REGULATION OF DIGITAL ASSETS[35]



1. REGULATORY BODIES

As its mission, FinCEN works to "safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial

[32] Katherine A. Lemire, *Cryptocurrency and anti-money laundering enforcement*, REUTERS (Sept. 26, 2022, 11:06 AM), https://www.reuters.com/legal/transactional/cryptocurrency-anti-money-laundering-enforcement-2022-09-26/; *see also* ORENBURG, *supra* note 5, at 130.
[33] *The Bank Secrecy Act*, FIN. CRIMES ENF'T NETWORK (1970), https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act.
[34] Press Release, U.S. Dep't of the Treasury, Remarks from Secretary of the Treasury Janet L. Yellen on Digital Assets, Univ. Kogod Sch. Bus. Ctr. Innovation (Apr. 7, 2022) https://home.treasury.gov/new s/press-releases/jy0706.
[35] ORANBURG, *supra* note 5, at 130.

intelligence."[36] In an effort to fulfill its mission, FinCEN requires that money services businesses (MSBs) "develop, implement, and maintain" measures that satisfy AML regulatory requirements."[37] Money transmitters, such as PayPal and MoneyGram, exist as a subcategory of MSBs and transmit currencies or funds from one person or business to another. Additionally, FinCEN administered guidance indicating that money laundering obligations also extend in part to the cryptocurrency industry through the BSA.[38]

The SEC is responsible for the regulation of securities and, therefore, regulates cryptocurrencies when they fall into the legal definition of a security. Cryptocurrencies are considered securities for regulatory application if they meet the "*Howey* Test," which was set out in *Securities and Exchange Commission v. W.J. Howey Co. et al*.[39] The Supreme Court outlined the four factors of the *Howey* Test: (i) an investment of money, (ii) an expectation of profit from the investment, (iii) the investment of money into a common enterprise, and (iv) profits generated from the efforts of a promoter or third party.[40] Though the *Howey* Test does provide parameters for the regulation of cryptocurrencies by the SEC, it is limited—there are "many" cryptocurrencies that fall outside of the *Howey* Test.[41] A bitcoin investment, for example, does not interact with a third party to ensure profits and does not require the collective efforts of a group. In fact, bitcoin transactions are commonly conducted by an individual investor. Cryptocurrencies that do fall under the definition of a security under the *Howey* Test are subject to securities laws and rules, as well as general oversight.[42]

Additionally, the Federal Bureau of Investigation (FBI) plays an important role in mitigating the risks of money laundering. As a body that acquires and conducts domestic and international intelligence, the FBI functions to prevent the illegal use of cryptocurrency in crimes such as domestic terrorism, drug trafficking, and organized crime.[43] While the FBI does play a role in the cryptocurrency sector, there is not yet a comprehensive strategy that addresses the increased risks of cryptocurrency—particularly anti-money laundering.[44] However, the United States Department of Justice has, as recent as 2020, encouraged the FBI to implement protocols, plans, and strategies that directly target the increasing risks associated with cryptocurrencies.[45]

2. AMERICAN REGULATORY INSTRUMENTS

The BSA, passed in 1970 by Congress, outlines guidelines and requirements that hold financial institutions and federal agencies accountable in their respective roles to prevent money

[36] *Mission*, FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/about/mission.
[37] Lemire, *supra* note 32. *See also Definition of Money Transmitter (Merchant Payment Processor*, FIN. CRIMES ENF'T NETWORK, https://www.fincen.gov/resources/statutes-regulations/administrative-rulings/definition-money-transmitter-merchant-payment.
[38] *Id*.
[39] ORANBURG, *supra* note 5, at 131. *See also* S.E.C. v. W.J. Howey Co., 328 U.S. 293 (1946).
[40] *Id*.
[41] *Id*.
[42] *Id*. at 116.
[43] *Id*. at 137.
[44] ORANBURG, *supra* note 5, at 137.
[45] *Id*. at 116.

laundering.[46] Importantly, the BSA requires financial institutions to record and report cash transactions that exceed a daily aggregate of $10,000 and to report activities—through completion of a Suspicious Act Report (SAR)—that are indicative of "money laundering, tax evasion, or other criminal activities."[47] Section 5318A of the BSA provides specific actions for "jurisdictions, financial institutions, international transactions, or types of accounts of primary money-laundering concern," which also applies to cryptocurrencies.[48] The Section outlines anti-money laundering requirements, including reporting and record-keeping, as well as additional jurisdictional and institutional factors in reaching a suspicion of money laundering activity.[49] These jurisdictional factors not only outline how domestic federal agencies are to assess jurisdictions outside of the United States, but they also serve as a general model for other countries to adopt.

These jurisdictional factors include:

(i) evidence that organized criminal groups, international terrorists, or entities involved in the proliferation of weapons of mass destruction or missiles have transacted business in that jurisdiction;

(ii) the extent to which that jurisdiction or financial institutions operating in that jurisdiction offer bank secrecy or special regulatory advantages to nonresidents or nondomiciliaries of that jurisdiction;

(iii) the substance and quality of administration of the bank supervisory and counter-money laundering laws of that jurisdiction;

(iv) the relationship between the volume of financial transactions occurring in that jurisdiction and the size of the economy of the jurisdiction;

(v) the extent to which that jurisdiction is characterized as an offshore banking or secrecy haven by credible international organizations or multilateral expert groups;

(vi) whether the United States has a mutual legal assistance treaty with that jurisdiction, and the experience of United States law enforcement officials and regulatory officials in obtaining information about transactions originating in or routed through or to such jurisdiction; and

(vii) the extent to which that jurisdiction is characterized by high levels of official or institutional corruption. [50]

In January 2021, Congress enacted the National Defense Authorization Act (NDAA)—a bill that brought significant updates and revisions to the Corporate Transparency Act (CTA) and the Anti-Money Laundering Act of 2020 (AMLA) as well as significant reforms to the BSA and

[46] The Bank Secrecy Act, *supra* note 33.
[47] *Id*.
[48] Bank Secrecy Act, 31 U.S.C. § 5318A (2020).
[49] *Id*. at 451-52.
[50] 31 U.S.C. § 5318A(c)(2)(A).

the USA PATRIOT Act of 2001.[51] Under the NDAA, the United States is obligated to streamline and update SAR by considering: (i) whether reporting threshold requirements should be adjusted, (ii) the ability to streamline the process for filing continuous SARs, and (iii) applying threshold requirements to a broader range of activities.[52] Additionally, the NDAA tasks the United States Treasury with testing its AML compliance technology in an effort to anticipate and determine the "impact of financial technology on financial crimes compliance."[53] With the passage of the NDAA, definitions within the language of BSA were expanded to apply to virtual currencies, and codified applicable FinCEN guidance associated with virtual currencies.[54] This need to update SAR reporting is partly due to the fact that the process was not originally designed with cryptocurrency in mind. Thus, while cryptocurrencies are subject to SAR reporting, financial officers often find it difficult to answer questions—causing further delay in transaction reporting. With further delays in reporting suspicious cryptocurrency transactions, criminals can conduct further criminal activity.

B. MEXICO

Virtual assets, as defined by the Mexican Government in its Anti-Money Laundering Law, is any representation of value registered electronically and used as payment for legal acts and transfers that can only be carried out electronically.[55] The Mexican AML Law points out, however, that virtual assets are prohibited from being considered legal tender or currency.[56] Thus, the Mexican government and financial regulatory authorities have taken a more conservative view of cryptocurrencies despite an international—and even domestic—increase in popularity.[57]

1. GOVERNING BODIES

According to the *Comisión Nacional Bancaria y de Valores* (CNBV), the Mexican AML regulatory system directs "one of the most comprehensive and sophisticated financial systems in the world."[58] The CNBV is responsible for regulating and supervising financial institutions on a variety of topics, including anti-money laundering and combating the financing of terrorism (AML and CFT). [59] The *Procuraduría General de la República* (PGR) is the prosecutorial arm of the Mexican government; as the Attorney General's Office of Mexico, the PGR is responsible for investigating and prosecuting individuals connected to money laundering and terrorist financing

[51] *Anti-Money Laundering Act of 2020 ICBA Summary*, INDEP. CMTY. BANKERS OF AMERICA 1 (2021), https://www.icba.org/docs/default-source/icba/advocacy-documents/summaries/icba-summary---anti-money-laundering-act-of-2020.pdf?sfvrsn=78ac0d17_0.
[52] *Id*. at 2.
[53] *Id*. at 3.
[54] *Id*. at 4.
[55] LEY FEDERAL PARA LA PREVENCION E INDENTIFICACION DE OPERACIONES CON RECURSOS DE PROCEDENCIA ILICITA (FEDERAL LAW FOR THE PREVENTION AND IDENTIFICATION OF OPERATIONS WITH RESOURCES OF ILLICIT ORIGIN) [LFPIORPI] art. 16; Diario Oficial de la Federación [DOF] 17-10-2012, últimas reformas DOF 20-05-2021 (Mex.), https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPIORPI_200521.pdf.
[56] *Id*. at art. 17.
[57] CRYPTOS ON THE RISE 2022, *supra* note 13, at 4.
[58] Comisión Nacional Bancaria y de Valores [Mexican Nat'l Banking Sys. and Sec. Comm'n] & Secretaria de Hacienda y Crédito [Ministry of Fin. and Public Credit], *Overview of the Mex. Fin. Sys. and its AML/CFT Regul. and Supervision 2*, https://www.gob.mx/cms/uploads/attachment/file/196042/SFM_230217.pdf.
[59] *Id*. at 6. Translated, the CNBV is the Mexican National Banking and Securities Commission.

(ML and TF).[60] The *Unidad de Inteligencia Financiera* (UIF) plays an important role in AML regulation and supervision.[61] Of its responsibilities, the UIF "receiv[es], analyz[es], and disseminat[es] to the competent authorities the information contained in the different types of AML and CFT reports;" requests AML and CFT-related "information, documentation, data and images… from financial institutions;" drafts regulations relating to AML and CFT; works with the PGR to initiate cases on AML and CFT violations; and informs financial entities of non-compliance in accordance with reporting requirements under AML regulation.[62] The *Secretaria de Hacienda y Crédito* (hereinafter referred to as SHCP) serves as the Ministry of Finance and Public Credit. Under its authority, the SCHP is responsible for drafting and issuing AML and CFT regulation; in addition, the SCHP also monitors financial institutions and entities to ensure that they are complying with AML and CFT laws and regulations. The *Unidad de Banca, Valores y Ahorro* (hereinafter referred to as the UBVA) serves as the Banking, Securities, and Savings Unit—responsible for the interpretation of AML and CFT regulation.[63] Through a collaborative and multi-agency approach, the Mexican financial system enhances their ability to monitor and investigate suspicious cryptocurrency transactions. By sharing information across agencies and across financial markets, this approach contributes to the knowledge base of regulators, policymakers, and investors. Together, these entities are best situated to address money laundering activities.

2. LEY FEDERAL PARA LA PREVENCION E INDENTIFICACION DE OPERACIONES CON RECURSOS DE PROCEDENCIA ILICITA (AML ACT)

Originally enacted in 2013, the Congress of Mexico enacted *Ley Federal para la Prevencion e Indentificacion de Operaciones con Recursos de Procedencia Ilicita*–the Federal Law for the prevention and Identification of Operations with Resources of Illicit Origin.[64] Commonly referred to as the AML Act, its outlined purposes are to protect the Mexican economy and financial system, to implement procedures that detect and prevent transactions involving resources from illicit origin, and to promote inter-agency collaboration to investigate and prosecute money laundering.[65]

The AML Act outlines the roles of financial institutions and what constitutes "vulnerable activities" for purposes of the Mexican financial system.[66] Financial institutions must establish measures that detect and prevent money laundering acts and implement customer identification mechanisms.[67] The AML Act lists sixteen different vulnerable activities that must be monitored by financial institutions.[68] Listed last are cryptocurrency exchnages–a transaction of virtual assets

[60] *Id*. at 10.
[61] *Id*. at 11.
[62] *Id*.
[63] OVERVIEW OF THE MEX. FIN. SYS. AND ITS AML/CFT REGUL. AND SUPERVISION, *supra* note 58, at 12-13.
[64] FED. LAW FOR THE PREVENTION AND IDENTIFICATION OF OPERATIONS WITH RES. OF ILLICIT ORIGIN (Mex.), https://www.global-regulation.com/translation/mexico/560553/regulation-of-the-federal-act-for-the-prevention-and-identification-of-operations-with-resources-of-illicit-origin.html (Aug. 16, 2013).
[65] *Id*. at art. 2.
[66] *Id*. at art. 17.
[67] *Id*. at art. 15.
[68] FED. LAW FOR THE PREVENTION AND IDENTIFICATION OF OPERATIONS WITH RES. OF ILLICIT ORIGIN, *supra* note 64, at art. 17.

occurring on electronic platforms that manage, operate, facilitate, or carry out these purchases or sales.[69] This definition applies to those who own these virtual assets and to those who guard, store, or transfer virtual assets.[70] Thus, financial institutions are required by law to monitor cryptocurrency transactions.[71] Once a customer engages in the exchange or sale of an amount equal to or greater than 605 units of a virtual asset, the financial institution is subject to a Notice from the Secretariat General's Office informing them that the consumer meets the transaction threshold.[72] Even if a customer does not engage in a sale or exchange that is equal to or greater than 605 units of a virtual asset, the financial institution may still be subject to the obligations under Article 18 if the sum is reached over a six-month period. These obligations include customer identification and document and information retention associated with the vulnerable activity (for a period of five years). [73]

Article 18 outlines the obligations of financial institutions if a customer satisfies both the definitional and activity requirements of virtual assets under Article 17. First, the financial institution must identify the customer that is engaged in vulnerable activities; to do this, financial institutions may rely upon their internal documentation and can obtain copies of needed documentation for identification purposes.[74] The Article also outlines information acquisition procedures when the transactions involve a business relationship or the existence of a beneficial owner.[75] The financial institution must also ensure that adequate safeguards are in place to securely store and protect vulnerable activity information and documents–including personal identifiable information.[76] According to Article 18, this information must be physically or electronically retained for five years–beginning from when the vulnerable activities end.[77] These obligations are nearly identical to those required for traditional transactions. By extending this language to virtual currencies, Mexican financial regulators recognize that these provisions are necessary to mitigate associated security risks.

Articles 13-33 outline the method by which the Secretariat General's Office should be notified of vulnerable activity.[78] Under Article 40, the Secretariat General's Office must report all money laundering information to the appropriate prosecutorial office regardless of whether the vulnerable activity occurred inside or outside of Mexico's jurisdiction.[79] The Act also authorizes the Secretariat to collaborate with other federal authorities and agencies to the extent necessary and within the scope of the investigation. Through this, the Secretariat may exchange information,

[69] *Id*.
[70] *Id*.
[71] *Id*.
[72] *Id*.
[73] *Id*.
[74] FED. LAW FOR THE PREVENTION AND IDENTIFICATION OF OPERATIONS WITH RES. OF ILLICIT ORIGIN, *supra* note 64, at art. 18.
[75] *Id*.
[76] *Id*.
[77] *Id*.
[78] *Id*. at art. 13-33.
[79] *Id*. at art. 40.

conclude agreements, and verify information with the appropriate agencies.[80] The Secretariat is authorized to exchange information and documentation with the Bank of Mexico.[81]

Under the Act, the Secretariat General's Office may impose sanctions if a financial institution fails to cooperate with an investigation regarding virtual assets.[82] Fines are imposed against financial institutions for failing to comply with obligations or participating in prohibited acts under the AML Act.[83] These fines increase based upon the statutory violation; for instance, failing to comply with Articles 17, 18, and 24 of the AML Act result in a fine between the equivalent of two hundred and two thousand days' wages.[84] Under Article 63, according to the Mexican Federal Criminal Code, a person associated with any of the investigatory agencies may face imprisonment of four to ten years if he or she inappropriately shares information, data, or images related to an investigation of vulnerable activities.[85] Now extended to cryptocurrencies, these articles ensure that criminal activities involving virtual assets are investigated and prosecuted thoroughly. By adhering to these regulations, Mexican officials are better equipped to quickly and effectively address illicit transactions–characteristics critical in reducing crypto money laundering. In addition, these Articles also hold financial institutions accountable for complying with cryptocurrency reporting regulations. By attaching fines and penalties to financial institutions, Mexican regulators underscore the importance of accurate, timely, and adequate reporting. Holding financial institutions to these standards ensures that investigative authorities, including the Secretariat General's Office, can swiftly act against criminals–a critical element of preventing money laundering through cryptocurrencies.

3. LEY PARA REGULAR LAS INSTITUCIONES DE TECNOLOGIA FINANCIERA (FINTECH LAW)

Enacted in March of 2018, the Financial Institutions Law ("Fintech Law") was established to regulate and provide guidance on operational practices for financial technologies.[86] The Fintech Law aimed to "promote financial inclusion," "provide legal security to technological financial services users," "trigger greater competition in the financial services market," "increase the number of participants in the financial sector," "prevent money laundering activities through electronic means," and "regulate the transactions with digital assets."[87] Digital assets, which include cryptocurrencies, are defined under Article 30 of the Fintech Law as "the representation of value recorded electronically and used by the public as a means of payment for all types of legal acts and whose transfer can only be carried out by electronic means, without the virtual asset being understood as a legal tender currency in the national territory, a foreign exchange or any other asset denomination in legal tender or foreign currency."[88] Assets are considered digital assets under the Fintech Law if they (i) represent a value, (ii) are electronically registered, (iii) are a

[80] FED. LAW FOR THE PREVENTION AND IDENTIFICATION OF OPERATIONS WITH RES. OF ILLICIT ORIGIN, *supra* note 64, at art. 40-47.
[81] *Id*. at art. 51.
[82] *Id*. at art. 52-61.
[83] *Id*. at art. 53.
[84] *Id*. at art. 54.
[85] *Id*. at art. 63.
[86] *Decree Enacting the Financial Technology Institutions Law ("Fintech Law")*, DELOITTE LEGAL (2018), https://www2.deloitte.com/content/dam/Deloitte/mx/Documents/legal/2018/Fintech-Law-Decree.pdf.
[87] *Id*. at 1-2.
[88] *Id*. at 3.

means of payment used by the public, and (iv) are only transferable via electronic means.[89] Under the Fintech Law, the Bank of Mexico plays an active role in the use, conditions, and restrictions on digital assets.[90] The Bank is given the authority to define what constitutes a "digital asset" and the types of transactions that are authorized and limited with those assets that fall within its terms.[91] Before conducting these transactions, however, the individual or entity engaged in digital asset transactions must apply for authorization by the CNBV.[92] While these conditions and restrictions may first appear as a sensible protective measure, they have largely limited the number of entities and individuals that constitute digital assets under the FinTech Law. Thus, a more careful review is necessary to determine whether the overprotective measures–possibly based on protecting the Mexican financial system–are proportional to the potential benefits, such as increased market participation, that relaxing these regulations may bring.

The Fintech Law also brought reforms to the Anti-Money Laundering Law–most notably to reporting requirements and to what constitutes "vulnerable activity." Article 17 of the Law was amended to incorporate virtual asset exchanges by those other than financial institutions "carried out through electronic, digital, or similar platforms which manage or operate, facilitating or carrying out the purchase or sale transactions of such assets owned by their clients or provide means of custody, to store or transfer virtual assets other than those recognized by the Bank of Mexico in terms of the Fintech Law."[93] Additionally, the Financial Intelligence Unit of the Ministry of Finance and Public Credit must be notified of "transactions involving digital assets" that or greater than or equal to "six hundred and forty-five UMA Measure Units."[94] With the passage of the Fintech Law, Mexican lawmakers could address several of the regulatory gaps not addressed by AML Act while making necessary updates.

While it appears that the Mexican government has implemented appropriate mechanisms to detect, prevent, and investigate money laundering involving cryptocurrencies, some aspects greatly restrict the ability to conduct transactions with cryptocurrencies. Multi-agency collaboration, robust reporting requirements, and the imposition of fines and penalties are all characteristics that should reflect international regulation; however, strict language that limits what constitutes "digital assets" would be hard to implement. Different countries have different interpretations of what constitutes a digital asset, and this diversity must be incorporated into international regulation.

C. SINGAPORE

1. REGULATORY BODIES

Singapore, an early participant in cryptocurrency, is viewed by financial markets worldwide as a frontrunner in developing and creating cryptocurrency regulation. Unique to Singapore is that all cryptocurrency regulation is handled through one agency, the Monetary

[89] *Id.*
[90] *Id.*
[91] *Id.*
[92] *Fintech Law*, *supra* note 86, at 3.
[93] *Id.* at 4.
[94] *Id.*

Authority of Singapore (MAS). Additionally, crypto service providers are tasked with going through the MAS licensing process–a system that is unlike that of the United States, Switzerland, or Mexico. When considering crypto service providers, MAS requires applicants to demonstrate robust governance structures and a good board of directors and examines the applicant's history to ensure that the provider is capable of managing the money laundering risks of cryptocurrencies. This licensing process, per the MAS, is designed to make Singapore a "responsible global crypto hub . . . with strong risk management capabilities."[95] It is Singapore's hope, per the Monetary Authority, that international regulators do more to address and monitor each risk individually–including those associated with AML–rather than viewing them as "a basket of risks."[96]

While the Parliament of Singapore is responsible for the passage of legislation, the financial market of Singapore is regulated by the MAS under the Monetary Authority of Singapore Act.[97] Not only does the MAS regulate the financial sector, but it also serves as the central bank of Singapore.[98] Part of the MAS's function is to draft and implement monetary policy as well as regulate and oversee payment systems and payment service providers. Payment service providers, by definition, are systems that are licensed under the Payment Services Act of 2019 (PS Act) to facilitate funds transfers, including cryptocurrencies, between parties. PayPal, Square, and Stripe are examples of popular payment service providers. To "encourag[e] innovation and growth of payment services and FinTech," the MAS assisted in Parliament's passage of the Payment Services Act–one that provides "a forward looking and flexible framework for the regulation of payment systems and payment service providers in Singapore."[99]

2. REGULATORY GOVERNANCE

The PS Act, which became effective January 28, 2020, was enacted as a "necessary" step to address the fast emergence of payment service risks.[100] According to the Monetary Authority of Singapore, the PS Act provides a "flexible regulatory framework that reduces the impact of a failure of a payment service provider while promoting a progressive payments sector in Singapore."[101] As discussed below, the MAS considers cryptocurrencies (also referred to as digital payment tokens) a payment service that falls under the PS Act.

In crafting the PS Act, the MAS focused on two areas of regulation–designation and licensing.[102] Under the designation framework, payment systems are given a particular designation

[95] Ravi Menon, Managing Director, Monetary Auth. Sing., MAS's Approach to the Crypto Ecosystem, Keynote Interview at the Financial Times' Crypto & Digital Assets Summit (Apr. 27, 2022) (transcript available at mas.gov.sg/news/speeches/2022/mas-approach-to-the-crypto-ecosystem).
[96] *Id*.
[97] Monetary Authority of Singapore Act, 1970 (Sing.).
[98] MONETARY AUTH. OF SING., *What We Do*, https://www.mas.gov.sg/who-we-are/what-we-do (last visited Oct. 27, 2022).
[99] Monetary Authority of Singapore Payment Services Act, 2019 (Sing.); MONETARY AUTH. OF SING., *Payments*, https://www.mas.gov.sg/regulation/payments (last visited Jan. 2, 2023).
[100] *Payment Service Act: A Guide to the Essential Aspects of the Payment Services Act*, MONETARY AUTH. OF SING. 2 (2019), https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulations-Guidance-and-Licensing/Payment-Service-Providers/Guide-to-the-Payment-Services-Act-2019.pdf?la=en&hash=B03712F4EEEE907C39BA2C12DE63A545495EE1C2.
[101] *Id*.
[102] *Id*. at 3.

to promote financial stability and "to ensure efficiency or competition" within the payment system market.[103] The MAS outlines its basis for designation, including the effect that any one payment system may have on the Singapore financial system if its operations temporarily or permanently fail.[104] Given the risks associated with money laundering and terrorist financing (ML and TF), crypto financial crimes could cause systemic problems if left unaddressed. Payment service providers, on the other hand, would argue that crypto ML and TF risks would not cause a failure of the Singapore financial system but merely isolated disruptions on a case-by-case basis. The licensing regime, in comparison, aims to manage risks by aligning "regulation of payment services to mitigate risks according to the scope and scale of payment service providers."[105] The Act outlines seven key payment services, namely: account issuance, domestic money transfer, cross-border money transfer service, merchant acquisition, e-money issuance, digital payment tokens (DPTs), and money-changing service.[106] DPTs, also known as cryptocurrencies, are defined by the MAS as "digital representations of value that do not have a physical form."[107] By capturing DPTs in the PS Act, the MAS is prescribed the regulatory power to mitigate associated risks. As briefly described by the MAS, DPT services regulate the purchasing and selling of DPTs as well as platforms that provide spaces for individuals in Singapore to purchase and sell DPTs.[108] DPTs, as recognized by the MAS in its June 2019 consultation paper, have increased risks due to their anonymous nature as well as the ease with which they facilitate rapid cross-border transactions.[109]

Absent an exception, all payments service providers under the PS Act are classified into three different licensee categories.[110] Money-changing licenses only give providers the ability to engage in "money-changing services;" thus, these businesses and entities have a smaller risk due to their narrowed scope of services.[111] Standard Payment Institution (SPI) licenses, which can provide any combination of the key payment services, are subject to lighter regulatory oversight as they encourage businesses to engage in innovation and small business enterprise.[112] Major Payment Institution (MPI) licenses, which allow providers to extend services beyond regulatory thresholds, produce higher risk exposure and require enhanced and comprehensive regulation.[113]

One of the primary objectives of the PS Act is to address and mitigate key risk areas in regard to the payment services industry.[114] These areas are enumerated in the PS Act as ML and TF risks, user protection, interoperability, and technology and cyber security risks.[115] By

[103] *Id*.
[104] *Id*.
[105] *Id*.
[106] *Payment Service Act*, *supra* note 100, at 4.
[107] *What Are Digital Payment Tokens*, MONETARY AUTH. SING. (2021), https://www.mas.gov.sg/-/media/MAS-Media-Library/who-we-are/mas-gallery/MAS-Gallery/Digital-Payment-Tokens.pdf.
[108] *Payment Service Act*, *supra* note 100, at 4-5.
[109] Consultation Paper on the Proposed Payment Service Notices on Prevention of Money Laundering and Countering the Financing of Terrorism, June 6, 2019, in *Payment Service Act*, *supra* note 100, at 5.
[110] *Payment Service Act*, *supra* note 100, at at 6.
[111] *Id*.
[112] *Id*.
[113] *Id*.
[114] *Payment Service Act*, *supra* note 100, at 15.
[115] *Id*. Per the MAS in the Guide, "user protection" refers to the ability to safeguard customer money that is invested with payment service providers. "Interoperability" is defined as the extent of "fragmentation of payment solutions" and the ability for payment solutions to access and exchange information. "ML/TF" refers to money laundering and

identifying and measuring these risks, the MAS is better equipped to address the inherent risks of cryptocurrency transactions such as their anonymous and cross-border nature. The MAS promulgates the AML and CFT risk mitigation measures that apply to all three licensee classes–the money-changing license, the SPI license, and the MPI license. However, the MAS notes that "a licensee does not need to comply with … AML/CFT requirements if it only provides payment services that meet the low-risk criteria for ML/FT."[116]

Key AML and CFT requirements under the PS Act include:

(i) taking appropriate steps to identify, assess, and understand the licensee's ML and TF risks;

(ii) developing and implementing policies, procedures, and controls–including those in relation to the conduct of CDD, transaction monitoring, screening, suspicious transaction reporting, and record keeping, in accordance with PSN01 or PSN02–to enable the licensee to effectively manage and mitigate their ML and TF risks;

(iii) monitoring the implementation of those policies, procedures and controls, and enhancing them as necessary; and

(iv) performing enhanced measures where there are higher ML and TF risks to effectively manage and mitigate those higher risks.[117]

Since the emergence of the PS Act, Singapore has recognized that innovation of crypto technologies will require "international work" on developing cryptocurrencies as well as continued vigilance in monitoring trends and developments in the payment services market.[118]

To supplement the PS Act, the Monetary Authority of Singapore issued the Notice PSN02 on the Prevention of Money Laundering and Countering the Financing of Terrorism–Digital Payment Token Service.[119] The PSN02 outlines the risk management steps that digital payment service providers should take in combatting money laundering–including risk mitigation, customer

terrorist financing in financial regulatory parlance. "Technology and cyber security" refer to risks associated with data breaches, fraud, and disruption.

[116] *Payment Service Act*, *supra* note 100, at 16-17. Criteria for what constitutes "low risk criteria for ML/FT" can be found in paragraph 3.2 of Payment Services Note 01 (PSN01).

[117] *Id*. at 17. "CDD" notates "customer due diligence," "PSN01" refers to the MAS Notice "Prevention of Money Laundering and Countering the Financing of Terrorism – Specified Payment Services," and "PSN01 refers to the MAS Notice "Prevention of Money Laundering and Countering the Financing of Terrorism – Digital payment Token Service."

[118] *Id*. at 5.

[119] The Monetary Authority of Singapore also issued Notice PSN01 (Prevention of Money Laundering and Countering the Financing of Terrorism–Specified Payment Services). This notice, per the MAS, is framed to provide anti-money laundering measures for payment service providers other than digital payment token service provider. For further information, *see* MONETARY AUTH. OF SING., NOTICE PSN02 PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCE OF TERRORISM – SPECIFIED PAYMENT SERVICE (last revised Mar. 1, 2022) (Sing.).

due diligence, record keeping, and transaction document retention and reporting.[120] The MAS based its issuance of the Notice in three main principles: the exercise of due diligence, providers acting "in conformity with high ethical standards," and "to the fullest extent possible, assist and cooperate with the relevant law enforcement authorities in Singapore to prevent money laundering and terrorism financing."[121] In accordance with these principles, PSN01 outlines guidance on how payment service providers should address the risk assessment.[122] "Risk Assessment," as defined in the Notice, requires payment service providers to take the proper steps to "identify, assess and understand" the threats associated with money laundering–this assessment must apply to the provider's customers, the customer's jurisdiction or country, countries or jurisdictions where the provider operates, and to "products, services, transactions and delivery channels" associated with the provider.[123] To ensure that risk assessment is adequate and complete, the Notice provides that payment providers must document their assessment, consider all risk factors before making a determination on risk mitigation, ensure that assessments are routinely updated as needed, and provide risk assessments to the Monetary Authority.[124]

The PSN02 Notice also outlines risk mitigation steps that providers should take–including the implementation of effective policy, the monitoring of high risks, and the routine assessment of whether policy measures are adequately covering high risks.[125] As part of its 2022 Amendment, the Monetary Authority of Singapore expressly outlined that providers "shall identify and assess" the risks associated with money laundering in relation to new products and practices—"including new delivery mechanisms" and "new or developing technologies for both new and existing products."[126] The Notice also outlines in Article 6 the circumstances that trigger CDD: (i) the establishment of a business relationship with a customer, (ii) transactions with those who have not established a business relationship, (iii) receipt of digital payment tokens when a business relationship is not established, (iv) suspicion of money laundering and terrorism financing, and (v) instances when the provider has "doubts about the veracity or adequacy of any information previously obtained."[127] By verifying the identity of their customers, payment service providers are able to ascertain their customers' behavior and can better anticipate potential money laundering risks associated with their DPT transactions. If the initial relationship or transaction in question produces "any reasonable grounds to suspect that the assets or funds of a customer are proceeds of drug dealing or criminal conduct … or are property related to the facilitation or carrying out of any terrorism financing offenses," the providers must file a Suspicious Transaction Report (STR) with the Monetary Authority.[128] PSN02 also provides language that allows for digital service providers to rely on third parties.[129] While a payment service provider cannot have the third party conduct their transaction monitoring, these third parties can assist in customer due diligence as long as they

[120] MONETARY AUTH. OF SING., NOTICE PSN02 PREVENTION OF MONEY LAUNDERING AND COUNTERING THE FINANCE OF TERRORISM – SPECIFIED PAYMENT SERVICE (last revised Mar. 1, 2022) (Sing.).
[121] *Id*. at art. 3.1.
[122] *Id*. at art. 4.1.
[123] *Id*.
[124] *Id*. at art. 4.2.
[125] *Id*. at art. 4.3.
[126] NOTICE PSN02, *supra* note 120, at art. 5.1.
[127] *Id*. at art. 6.3.
[128] *Id*. at art 6.2.
[129] *Id*. at art. 11.1.

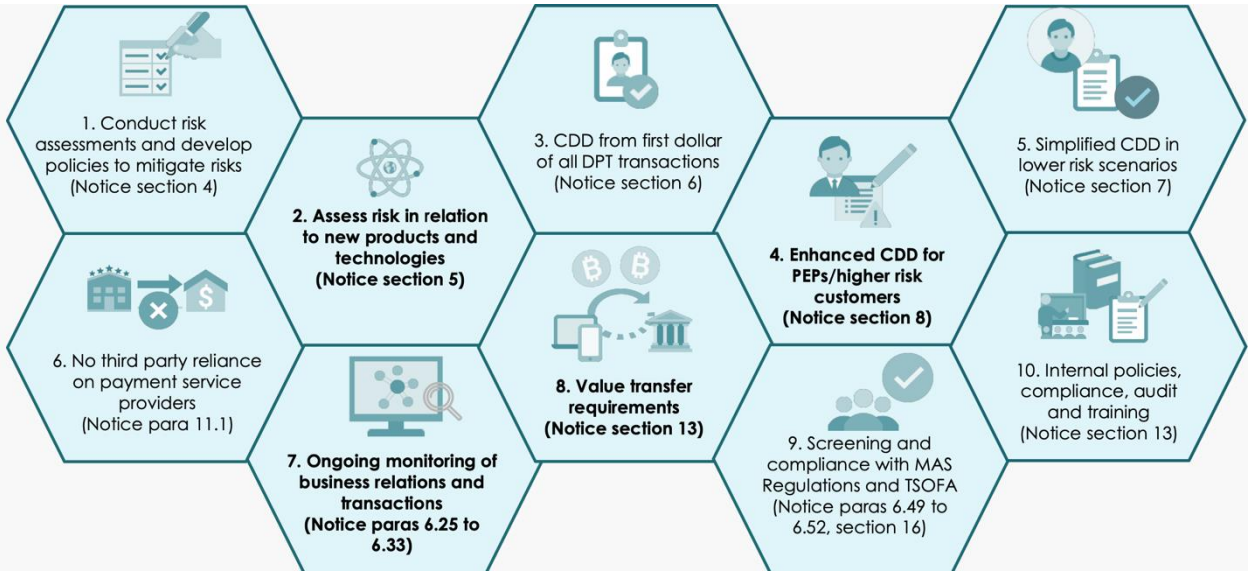
satisfy requirements, including that they "intend to rely upon" and are "subject to and supervised for compliance with AML/CFT requirements consistent with standards set by the FATF."[130]

In addition to identifying and reporting suspicious transactions, PSN02 requires continued monitoring of transactions with customers suspected of money laundering.[131] This vigilance includes continued attention to all transactions–big, small, and complex–as well as irregular patterns in a customer's transaction behavior.[132] Following careful monitoring and documentation, payment service providers should follow their international risk mitigation policies and procedures if money laundering activities are ongoing.[133] If these transactions are non-face-to-face, similar risk mitigation and monitoring steps should be taken by the provider.[134] Additionally, the provider must provide an assessment report to the Monetary Authority within a year after their first non-face-to-face contact with the customer.[135]

Under the PSN02, the Monetary Authority lists circumstances that indicate when an individual or group poses a high risk to engage in money laundering. Two of these circumstances are "where a customer or any beneficial owner of a customer is from or in a country or jurisdiction in relation to which the FATF has called for countermeasures" and "where a customer or any beneficial owner of the customer is from or in a country or jurisdiction known to have inadequate AML/CFT measures, as determined by the payment service provider for itself, or notified to payment service providers generally by the Authority or other foreign regulatory authorities."[136] Thus, these regulations take into consideration cross-jurisdictional attributes and the relative nature of other jurisdictional frameworks.

[130] *Id*. at art. 11.2; *see also* NOTICE PSN02, *supra* note 120, art. 6-8.
[131] *Id*. at art. 6.25-6.27.
[132] NOTICE PSN02, *supra* note 120, at art. 6.28-.29.
[133] *Id*. at art. 6.27.
[134] *Id*. at art. 6.34 – 6.39.
[135] *Id*. at art. 6.38.
[136] *Id*. at art. 7.4.

FIGURE 3. KEY AML/CFT CHARACTERISTICS FROM PSN02[137]



D. SWITZERLAND

Switzerland is seen by most as having one of the largest and most crypto-friendly legal regulations in the world. In fact, Switzerland is home to the "crypto valley" in Zug–an active community of entrepreneurs and businesspeople in the cryptocurrency industry that was founded in 2013.[138] Swiss crypto regulation is primarily enforced by the Swiss Financial Market Supervisory Authority (FINMA) through the Swiss Anti-Money Laundering Act and the Distributed Ledger Technology (DLT) Act. The FINMA established regulation to combat money laundering and terrorist financing, and this law applies to cryptocurrencies as well.[139] Swiss regulation is comprised of three different pieces of legislation–the Anti-Money Laundering Act, the Anti-Money Laundering Ordinance, and the FINMA Anti-Money Laundering Ordinance.[140] The Anti-Money Laundering Ordinance, issued in 2015 by the Swiss Federal Council, regulates financial intermediation, due diligence requirements, and reporting requirements promulgated under the AMLA.[141]

However, some crypto investors and regulators are concerned that Switzerland's progressive regulatory reforms chip away at some of the key characteristics of cryptocurrencies–

[137] *Strengthening AML/CFT Controls of Digital Payment Token Service Providers*, MONETARY AUTH. SING. 7 (2021), https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulations-Guidance-and-Licensing/Payment-Service-Providers/Strengthening-AMLCFT-Controls-of-Digital-Payment-Token-Service-Providers.pdf.

[138] *About the Association*, CRYPTO VALLEY ASSOCIATION (2022), https://cryptovalley.swiss/about-the-association/.

[139] *Rechtsgrundlagen für die Geldwäschereibekämpfung* [*Legal Basis for Combating Money Laundering*], EIDGENÖSSISCHE FINANZMARKTAUFSICHT [SWISS FINANCIAL MARKET SUPERVISORY AUTHORITY] (2022), finma.ch.

[140] *Id*.

[141] Verordnung über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung [Decree on the Fight Against Money Laundering and Terrorist Financing], Schweizerische Bundesrat [Swiss Federal Council] art. 1 (Switz.).

deregulation and anonymity. Thus, Swiss regulators must consider regulating cryptocurrencies in a way that not only increases consumer participation and addresses money-laundering risks, but also remains crypto-friendly and recognizes the interfering role regulations may have on entrepreneurs who are setting up business in Switzerland in order to ensure long-term success in the global markets. For the same reason, all of these should be considered when forming an international cryptocurrency regulation.

1. SWISS CRIMINAL CODE

Under Article 305 of the Swiss Criminal Code, anyone who "carries out an act that aimed at frustrating the identification of the origin, the tracing or confiscation of assets which he knows or must assume originate from a felony" may be subject to monetary penalties or a punishment of up to three years in prison.[142] In cases where a person participates in organized crime, commits a crime within a group created for the purpose or money laundering, or gains "a large turnover or substantial profit through commercial money laundering," the perpetrator faces monetary penalties or a punishment of up to five years in prison.[143] Article 305 also extends liabilities to offenses committed outside of Swiss jurisdiction "provided that such act is also an offence at the place of commission."[144] These penalties not only apply to traditional money laundering activities involving cash, but also to those involving cryptocurrencies. Given that the traditional money laundering elements of conversion, concealment, and acquisition also apply to cryptocurrencies, Swiss authorities may also prosecute these criminals under Article 305.

2. ANTI-MONEY LAUNDERING ACT

The Anti-Money Laundering Act (AMLA), first enacted in 1997 by the Federal Assembly of the Swiss Confederation, was designed to "regulate[] the combating of money laundering….,the combating of terrorist financing…, and the due diligence required in financial transactions."[145] The Act primarily pertains to financial intermediaries, defined as "persons who on a professional basis accept or hold on deposit assets belonging to others who assist in the investment or transfer of such assets."[146] In its August 2019 press release, the Swiss Financial Market Supervisory Authority (FINMA) recognized that it has "always applied the Anti-Money Laundering Act to blockchain service providers."[147] The Anti-Money Laundering Act requires that blockchain service providers–financial entities licensed by FINMA to conduct payment transactions on the blockchain–implement customer and beneficial owner identification verification, employ risk

[142] Schweizerisches Strafgesetzbuch [Swiss Criminal Code] art. 305 (Switz.), *translated by* Eidgenössiche Finanzmarktaufsicht [Swiss Financial Market Supervisory Authority (FINMA)].
[143] *Id*.
[144] *Id*.
[145] Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung [Federal Act on Combating Money Laundering and Terrorist Financing] art. 1 (Switz.), *translated by* Eidgenössiche Finanzmarktaufsicht [FINMA].
[146] *Id*. at art. 3.
[147] *FINMA Aufsichtsmitteilung 02/2019: Zahlungsverkehr auf der Blockchain* [*FINMA Guidance 02/2019: Payments on the Blockchain*], EIDGENÖSSICHE FINANZMARKTAUFSICHT [FINMA] 1 (2019), https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20190826-finma-aufsichtsmitteilung-02-2019.pdf.

mitigation strategies when engaging in business relationships, and report suspicions of money laundering activity to the Money Laundering Reporting Office of Switzerland (MROS).[148]

3. FINMA ANTI-MONEY LAUNDERING ORDINANCE

The FINMA Anti-Money Laundering Ordinance, issued in 2015 by FINMA, explains how financial intermediaries are to implement policies and practices in order to monitor and combat money laundering and terrorist financing.[149] Article 6 of the Ordinance emphasizes the role of global risk monitoring–including those that arise with money laundering.[150] Under the Ordinance, financial intermediaries with international offices or that operate with foreign entities "shall record, limit, and monitor [their] legal and reputational risks related to money laundering and terrorist financing on a global level."[151] To monitor these international risks, the Ordinance outlines that financial intermediaries should complete consolidated risk analysis periodically, complete an annual assessment that qualifies and quantifies consolidated risks, "inform [] on their own and in a timely manner… the acceptance and continuation of business relationships that are globally significant form a risk perspective," as well as perform routine visits to sites in order to best implement internal risk controls.[152] In 2020, FINMA revised the Ordinance by incorporating Article 51(a), "Transactions with virtual currencies."[153] Financial intermediaries involved in virtual currency transactions, under the Article, must identify transactions with parties that appear "interconnected," meet or exceed CHF 1,000, or are suspected to be potential money laundering or terrorist financing.[154] Article 74 of the Ordinance enumerates the documents that must be retained, which includes business relationship documents, investigation documents, and anti-money laundering report documents.[155]

4. DISTRIBUTED LEDGER TECHNOLOGY (DLT) ACT

In 2019, the Federal Assembly of the Swiss Confederation passed the Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology–often referred to as the DLT Act.[156] Generally, distributed ledger technologies, such as blockchain, use independent computers to "record, share and synchronize transactions" into an electronic ledger.[157] These recorded transactions are organized into "blocks" and "chained" together unlike that of a

[148] *Id*.
[149] *Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung* [*Anti-Money Laundering Ordinance*], KPMG (2015), *translated in* Ordinance of the Swiss Financial Market Supervisory Authority on the Prevention of Money laundering and the Financing of Terrorist Activities, https://assets.kpmg/content/dam/kpmg/ch/pdf/swiss-anti-money-laundering-ordinance-finma-en.pdf.
[150] *Id*. at art. 6.
[151] *Id*.
[152] *Id*.
[153] *Id*. at art. 51(a).
[154] *Id*.
[155] Anti-Money Laundering Ordinance, *supra* note 149, at art. 74.
[156] *Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register* [*Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology*], *translated by* SCHWEIZERISCHE BUDENSTRAT [FEDERAL COUNCIL] (2019), https://www.newsd.admin.ch/newsd/message/attachments/60601.pdf.
[157] THE WORLD BANK, *Blockchain & Distributed Ledger Technology (DLT)* (Apr. 12, 2018), https://www.worldbank.org/en/topic/financialsector/brief/blockchain-dlt.

traditional centralized ledger.[158] As the full name suggests, the DLT Act's goal was to modernize a series of federal laws into better alignment with innovation and emerging risks of the Swiss financial market system.[159] Of these, the Anti-Money Laundering Act of October 10, 1997, was revisited in order to account for innovation in crypto technologies.[160] The DLT Act revised the definition of "financial intermediaries" under Article II, Paragraph II of the AML Act.[161] This revised definition applied to central "counterparties" and "securities depositories in accordance with the Financial Market Infrastructure Act."[162] This definition revision allowed DLTs to fall under the authority of the AML Act; thus, distributed ledgers are held to the same risk mitigation, monitoring, and reporting requirements as other physical and digital assets under the Act.[163]

IV. APPLICATION ON THE INTERNATIONAL SCALE

The United States, Mexico, Singapore, and Switzerland have all enacted measured and directed regulation that attempts to address the increasing risk of money laundering via digital assets. After examining the four selected countries, one can see the diversity and complexities of domestic cryptocurrency regulation. While each country has implemented regulation to address the money laundering risks associated with cryptocurrency, some of these regulations would scale nicely on an international level whereas others would not. This part examines the aspects of the United States, Mexico, Singapore, and Switzerland's respective regulations and considers their international application. By such comparison, international regulators can begin to put together potential global regulations of money laundering.

A comparative analysis provides valuable insight for the future of the cryptocurrency regulation–countries may be encouraged to adopt anti-money laundering regulation that has operated successfully in other countries. On the other hand, jurisdictions may wish to revise or reconsider their current regulations considering another country's failures and experiences. Fortunately, the respective regulations of the United States, Mexico, Singapore, and Switzerland are worth implementing on an international scale. However, certain characteristics are unique to their own jurisdictions–specifically tailored to address cryptocurrency risks through a lens of domestic political, social, economic, and ideological factors. Additionally, each country viewed has undergone significant regulatory reform in recent years; while these changes were arguably necessary, the question remains as to the quality and adequacy of currently enacted laws. As such, these gaps on the domestic level will only be magnified as these policies and regulations are implemented on an international scale. Thus, policymakers, lawmakers, and stakeholders should be cognizant of their roles to address any regulatory gaps as cryptocurrencies continue to develop.

A. ACCOMMODATING DIFFERENCES

In addressing the regulation of cryptocurrencies, each relationship amongst a country's federal agencies and financial institutions are different. For example, while Mexico has banned

[158] *Id*.
[159] Federal Act on the Adaptation of Federal Law to Developments in Distributed Ledger Technology, *supra* note 156. For a list of other legislatives instruments amended by the DLT act, *see generally id.*
[160] *Id*. at 9.
[161] *Id*. at 10.
[162] *Id*.
[163] *Id*.

cryptocurrency transactions within its borders, several federal agencies work together to monitor, prosecute, and investigate cryptocurrency transactions.[164] On the other hand, the Monetary Authority of Singapore is the sole regulatory authority of one of the most crypto-friendly environments in the world.[165] Given that these countries have successfully monitored and mitigated crypto risks with these relationships, international regulation should encourage similar types of relations. Financial institution and federal agency collaboration, when supported on an international level, would encourage other countries to do the same. This collaboration, as seen in this paper, would improve a country's ability to efficiently monitor and investigate illicit cryptocurrency transactions.

By providing an impressive regulatory baseline on an international scale, crypto money launderers would be less inclined to forum shop and move to jurisdictions that have relaxed regulatory regimes. However, countries must be willing to address domestic effects resulting from illicit cryptocurrency transactions within their jurisdictions. While this would include transactions that are fully completed domestically, countries would also be held accountable for cryptocurrency transactions that originated them. The rationale behind this is, had the country implemented sufficient regulatory monitoring and reporting requirements, these transactions would not have occured. Doing so will not only relieve the international body from being too burdening, but will also encourage and allow countries to create a crypto regulatory structure tailored to their respective risks.

While it may be more efficient and easier for international regulation to apply a uniform approach, this may create tension with domestic policy objectives and notions of security. However, centralization would likely allow the regulation to better fluctuate with international developments in AML and the cryptocurrency market–regulations would not necessarily need to be enacted on a country-by-country basis. As risk factors grow and fade over time as a result of proper risk mitigation measures, an international body would be best able to address the trend on an international level. This would ideally eliminate some of the delays to implementation that nearly all jurisdictions have faced in reaction to cryptocurrency risks.

Additionally, an international regulation must be able to reconcile that many countries have enacted complete bans on cryptocurrencies and others do not appear to have adequate enforcement mechanisms to apply international regulation. For instance, Mexico has banned cryptocurrencies. From the global perspective, it appears that cryptocurrencies are here to stay, notwithstanding bans across the world. Thus, international regulation should be mindful of ways to encourage and incentivize countries to allow cryptocurrency transactions within their financial markets; however, international regulation should provide provisions that allow for accommodations in the short-term. Implementing regulations that preserve security and minimize risk in cross-border crypto transactions would likely reduce some of concerns held by countries that ban cryptocurrency.

[164] *See supra* notes 58-63.
[165] *See supra* note 95.

B. INFORMATION SHARING

Each country's regulation emphasized the importance of information sharing.[166] As all countries alluded to, the exchange of information is necessary in order to effectively investigate and prosecute those suspected of money laundering. This aligns with the FAFT's essential recommendation that countries should make efforts to facilitate cooperation and the availability of information.[167] By exchanging information in a multi-jurisdictional format, countries are able to better identify criminals and reduce anonymity. In the international setting, this information may be best shared in a centralized secured space. This space would likely take the form of an international information exchange body–organized and governed in similar ways to the International Monetary Fund (IMF). This would allow for a more streamlined and efficient process; specifically, it allows investigative bodies to better investigate and prosecute money launderers. In addition, the FATF as the international regulatory body should consider imposing uniform reporting requirements while acknowledging any disparity in enforcement abilities by countries.

The licensing requirement of Singapore's PS Act, on an international scale, would ensure that essential information is acquired that both verifies the identity of the customer and establishes risk requirements for each customer and service provider. The issuance of a license could be granted through an international body, composed of membership from countries from across the world. International regulation would allow for the formation of this international licensing body. By forming this body through international regulation, this would create a uniform verification system across jurisdictions and would, thus, minimize anonymity and increase clarity regarding an individual's ability to engage in cryptocurrency transactions.

C. Interpretation Versus Creation

Another consideration for policy makers to think about is whether international regulation should be interpreted from existing international policy or created from existing domestic regulation. While each country has made efforts to implement its own cryptocurrency regulations, each country has done so in slightly different ways. Switzerland and the United States based their regulation upon the risks associated with traditional payment systems and currencies.[168] Mexico, on the other hand, enacted its anti-money laundering regulation in 2013; however, Mexican lawmakers created the FinTech law five years later to more directly address financial technologies.[169] Singapore, by comparison, initiated its cryptocurrency regulation with the Payment Services Act of 2019 as a stand-alone authority.[170] Thus, regulators and policymakers will want to consider whether an international regulation should be an amalgamation of existing digital asset regulations from across the globe or an entirely new model derived upon currently faced risks. Whichever way internal regulation is designed, lawmakers must be cautioned not to conflate the money laundering practices of tangible assets to those of digital assets. While there

[166] *See supra* notes 50, 74-75, 117-18, 148, 151.
[167] *See supra* notes 26-27.

[168] *See supra* notes 54, 147, 153.
[169] See s*upra* notes 64, 86.
[170] *See supra* note 97.

are certainly many similar qualities in the associated risks, digital assets are particularly difficult to track and monitor due to accelerated transaction time and increased anonymity. International crypto regulation will need to accommodate diverse approaches and perspectives while adopting universal necessities in order to effectively combat these illicit activities. While implementing these accommodations will certainly be a challenge given that international cryptocurrency regulations is new and emerging, acknowledging these differences is a critical step in the formation process.

V. CONCLUSION

The cryptocurrency market is changing quickly, and criminals are keeping pace. Transactions occur much easier and the number of individuals that participate in the market rapidly increases daily. At the same time, the risks associated with cryptocurrency exchanges are continuing to rise. Domestic regulation become antiquated as the development of financial technologies continues at an alarming rate. The ability to regulate cryptocurrencies is at a crossroads: whether to allow the cryptocurrency market to become the "Wild West" of finance or to create an effective international solution.

The article has shown that jurisdictions have begun to recognize the risks associated with international cryptocurrency transactions while acknowledging that international success is nearly impossible without international coordination and guidance. Regulations can take on numerous characteristics of countries and acknowledge that international regulation must consider the complicated and unique contexts of each country. The creation and application of international regulation is not one that will be easy, but it is one, in this time of anonymity and transnationality, that is necessary.