



**NAVAL
POSTGRADUATE
SCHOOL**

MONTEREY, CALIFORNIA

THESIS

**REFORMING THE BANK SECRECY ACT
TO ADDRESS EMERGING TECHNOLOGY AND
PREVENT ILLICIT FINANCING**

by

Shawn M. Bradstreet

December 2019

Co-Advisors:

Richard D. Bergin IV
Shannon A. Brown

Approved for public release. Distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.				
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE December 2019	3. REPORT TYPE AND DATES COVERED Master's thesis		
4. TITLE AND SUBTITLE REFORMING THE BANK SECRECY ACT TO ADDRESS EMERGING TECHNOLOGY AND PREVENT ILLICIT FINANCING			5. FUNDING NUMBERS	
6. AUTHOR(S) Shawn M. Bradstreet				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release. Distribution is unlimited.			12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) The Bank Secrecy Act (BSA) was enacted by Congress to prevent criminals from hiding or laundering their illicit gains through the U.S. banking system. Over the years, criminals continue to exploit the financial system by moving illegal money using new technology. Lawmakers should amend the age-old BSA to address monetary thresholds of currency transaction reports and suspicious activity reports, along with addressing emerging financial technology (Fintech). In dealing with these issues, a delicate balance exists between increasing regulation to prevent crime and hindering the growth of innovation and customer convenience, along with privacy concerns. This thesis provides policy analysis and proposals for legislative and technological improvements to financial fraud detection. Furthermore, policy leaders will have a comprehensive understanding of the benefits and consequences of specific policy actions. This thesis concludes with policy recommendations of the BSA to include increasing the currency transaction report from \$10,000 to \$60,000 along with incorporating the controversial beneficial ownership provision. Last, add a minimum standard for a client opening financial accounts, increase know-your-customer requirements, and regulate peer-to-peer devices. As criminal organizations continue to move money throughout the U.S. financial services sector, legislators should amend the BSA to address these areas of concern to ensure financial stability and integrity.				
14. SUBJECT TERMS Bank Secrecy Act, financial technology, fintech, money laundering, Counter Terrorism and Illicit Finance Act, machine learning, digital currency, know-your-customer, KYC, peer-to-peer, P2P, FinCEN, currency transaction report, CTR, suspicious activity report, SAR, beneficial ownership provision, anti-money laundering, H.R. 6068, H.R. 1039, distributed ledger technology, biometrics, risk-based approach			15. NUMBER OF PAGES 109	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release. Distribution is unlimited.

**REFORMING THE BANK SECRECY ACT TO ADDRESS EMERGING
TECHNOLOGY AND PREVENT ILLICIT FINANCING**

Shawn M. Bradstreet
Resident Agent in Charge, U.S. Secret Service, Department of Homeland Security
BA, Cedarville University, 1996

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2019**

Approved by: Richard D. Bergin IV
Co-Advisor

Shannon A. Brown
Co-Advisor

Erik J. Dahl
Associate Chair for Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Bank Secrecy Act (BSA) was enacted by Congress to prevent criminals from hiding or laundering their illicit gains through the U.S. banking system. Over the years, criminals continue to exploit the financial system by moving illegal money using new technology. Lawmakers should amend the age-old BSA to address monetary thresholds of currency transaction reports and suspicious activity reports, along with addressing emerging financial technology (Fintech). In dealing with these issues, a delicate balance exists between increasing regulation to prevent crime and hindering the growth of innovation and customer convenience, along with privacy concerns. This thesis provides policy analysis and proposals for legislative and technological improvements to financial fraud detection. Furthermore, policy leaders will have a comprehensive understanding of the benefits and consequences of specific policy actions. This thesis concludes with policy recommendations of the BSA to include increasing the currency transaction report from \$10,000 to \$60,000 along with incorporating the controversial beneficial ownership provision. Last, add a minimum standard for a client opening financial accounts, increase know-your-customer requirements, and regulate peer-to-peer devices. As criminal organizations continue to move money throughout the U.S. financial services sector, legislators should amend the BSA to address these areas of concern to ensure financial stability and integrity.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	PROBLEM STATEMENT	1
B.	RESEARCH QUESTION	2
C.	BACKGROUND	2
	1. Overview of the Bank Secrecy Act	2
	2. Financial Fraud Trends Involving New Technology	5
D.	RESEARCH DESIGN	7
E.	CHAPTER OUTLINE.....	9
II.	LITERATURE REVIEW	11
A.	HISTORICAL DEBATE.....	11
B.	REGULATORY ISSUES	12
C.	COUNTER TERRORISM AND ILLICIT FINANCE ACT	14
D.	FINANCIAL TECHNOLOGY	17
	1. Machine Learning for Fraud Detection	17
	2. Digital Currency.....	20
	3. Know-Your-Customer Rule.....	22
	4. Peer-to-Peer	23
E.	CONCLUSION	25
III.	LEGISLATIVE SOLUTIONS: H.R. 6068 (COUNTER TERRORISM AND ILLICIT FINANCE ACT)	27
A.	DESCRIPTION OF COUNTER TERRORISM AND ILLICIT FINANCE ACT	27
	1. Goals.....	28
	2. Advantages.....	28
	3. Limitations.....	30
	4. Beneficial Ownership Debate.....	30
B.	POLICY ANALYSIS.....	33
	1. Policy Options Criteria.....	33
	2. Policy Options Matrix.....	35
C.	DISCUSSION	36
	1. Bank Executives	36
	2. Law Enforcement.....	37
	3. Privacy Advocates	37
D.	ANALYSIS	38

IV.	FINANCIAL TECHNOLOGY	41
A.	OVERVIEW OF FINANCIAL TECHNOLOGY	41
	1. Machine Learning	41
	2. Digital Currency	45
	3. Know Your Customer Using Technology	54
	4. Peer-to-Peer	58
B.	TECHNOLOGY ANALYSIS	60
	1. Policy Options Criteria	60
	2. Technology Criteria	61
	3. Technology Option Matrix	62
C.	DISCUSSION	63
	1. Bank Executives	63
	2. Law Enforcement	63
	3. Privacy Advocates	64
D.	ANALYSIS	64
V.	CONCLUSION	67
A.	RECOMMENDATIONS	67
	1. Currency Transaction Reports	67
	2. Suspicious Activity Reports	68
	3. Beneficial Ownership Provision	69
	4. Machine Learning	69
	5. Digital Currency	70
	6. Know Your Customer	70
	7. Peer-to-Peer	71
B.	IMPLEMENTATION CHALLENGES	72
C.	FUTURE AREA OF RESEARCH	72
D.	CONCLUSION	73
	LIST OF REFERENCES	75
	INITIAL DISTRIBUTION LIST	87

LIST OF TABLES

Table 1. Monetary Thresholds36

Table 2. Financial Technology.....62

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ABA	American Bar Association
ACH	automated clearing house
AI	artificial intelligence
AML	anti-money laundering
BSA	Bank Secrecy Act
CDD	customer due diligence
CHDS	Center for Homeland Defense and Security
CIP	customer identification program
CTR	currency transaction report
DLT	distributed ledger technology
EFF	Electronic Frontier Foundation
FACT	Financial Accountability & Corporate Transparency
FCA	Financial Conduct Authority
FCTF	Financial Crimes Task Force
FFIEC	Federal Financial Institutions Examination Council
FinCEN	Financial Crimes Enforcement Network
fintech	financial technology
FOP	Fraternal Order of Police
GDP	gross domestic product
H.R.	House of Representatives
ICCID	integrated circuit card identifier
IMEI	international mobile equipment identity
IMSI	international mobile subscriber identity
IRS	Internal Revenue Service
KYC	know your customer
LE	law enforcement
LLC	limited liability companies
MIT	Massachusetts Institute of Technology
ML	machine learning
NACHA	National Automated Clearing House Association

NAFCU	National Association of Federally-Insured Credit Unions
NCA	National Crime Agency
P2P	peer-to-peer
PCBB	Pacific Coast Bankers Bank
PII	personally identifiable information
PwC	PricewaterhouseCoopers
RBA	risk-based approach
SAR	suspicious activity report
UIDAI	Unique Identification Authority of India

EXECUTIVE SUMMARY

The Banks Secrecy Act (BSA) of 1970 was enacted by Congress to prevent criminals from hiding or laundering their illicit gains through the U.S. banking system.¹ The statute's objective forced financial institutions to maintain currency transactions reports, along with identifying individuals conducting suspicious transactions.² Preserving these records allow law enforcement the ability to pursue and arrest criminals involved in money laundering or other financial crimes. Since the inception of the BSA, legislators have provided minimal updates, and the monetary thresholds of the currency transaction reports (CTRs) and suspicious activity reports (SARs) need to be addressed.

Furthermore, with the innovations in financial technology (fintech), criminals continue to exploit these new technologies to move money and obfuscate law enforcement. Currently, the BSA does not adequately address emerging technologies like machine learning, digital currency, know your customer, and peer-to-peer technology. As criminals continue to move money throughout the financial system, lawmakers should amend the BSA to address emerging fintech while addressing the monetary thresholds of cash transactions and suspicious activity.

In dealing with these issues, a delicate balance exists between increasing regulation to prevent crime and hindering the growth of innovation and customer convenience, along with privacy concerns. This thesis provides a policy analysis and proposal for legislative and technological improvements to financial fraud detection. Furthermore, policy leaders will have a comprehensive understanding of the benefits and consequences of specific policy action.³

¹ "FinCEN's Mandate from Congress," Financial Crimes Enforcement Network, accessed February 4, 2019, <https://www.fincen.gov/resources/fincens-mandate-congress>.

² Federal Financial Institutions Examination Council, *Bank Secrecy Act/Anti-Money Laundering Examination Manual* (Washington, DC: Federal Financial Institutions Examination Council, 2014), 3, https://www.ffiec.gov/bsa_aml_infobase/documents/bsa_aml_man_2014.pdf.

³ Samantha Holquist, "How to Conduct an Effective Policy Analysis," *GovLoop* (blog), July 18, 2013, <https://www.govloop.com/community/blog/how-to-conduct-an-effective-policy-analysis/>.

This paper discusses in detail the proposed monetary changes to the BSA as introduced in the Counter Terrorism and Illicit Finance Act. The Counter Terrorism and Illicit Finance Act would have altered the BSA to address the monetary CTR and SAR thresholds.⁴ The question surrounding these monetary requirements are: Should the current thresholds remain the same? Or should the amounts be adjusted as stated in the counter-terrorism act? Or should the monetary amounts be adjusted to account for inflation? Also, the counter-terrorism act removed the highly contested beneficiary ownership provision. Addressing these various issues becomes complicated, especially when considering the stakeholders involved. These concerns are addressed using a policy options criteria and matrix ranking the threat to public safety, the cost to the banking industry, the impact on law enforcement investigations, and political acceptance or opposition. Furthermore, several viewpoints with a detailed perspective from bank executives, law enforcement, and privacy advocates are discussed to provide a complete representation of the affected parties.

Fraud detection is an ongoing and challenging problem for financial institutions. Internal currency alerts only detected 50% of money laundering or terrorist financing.⁵ The banking industry also has difficulty hiring experienced staff to detect or comply with anti-money laundering (AML) regulations.⁶ With these two significant issues, machine learning (ML) can process large amounts of data to detect fraudulent activity that thus assists financial institutions. In the financial sector, “machine learning is trained to recognize normal transactions within the data and then identify all deviations and anomalies in real-time.”⁷ Using this relatively new technology, financial institutions can detect suspicious activity instead of paying a traditional analyst. However, ML has

⁴ LegiNation, “US—HR 6068: Counter Terrorism and Illicit Finance Act,” Bill Track 50, accessed February 21, 2019, <https://www.billtrack50.com/BillDetail/986684>.

⁵ Trevor White, Mark Anderson, and Didier Lavion, *Adjusting the Lens on Economic Crime* (PwC US, 2016), 42.

⁶ White, Anderson, and Lavion, 42.

⁷ Mercator Advisory Group, Inc., *Fraud Detection 2.0: Dynamic Tools for Fighting E-Commerce Fraud* (Boise, ID: Knout, 2017), 5, <https://info.kount.com/white-paper/fraud-detection-dynamic-tools-for-fighting-ecommerce-fraud>.

disadvantages in regards to accuracy, along with costly implementation and maintenance concerns.

Digital currency has also been a growing concern among regulators. When people think of digital currency, Bitcoin comes to everyone's mind. Bitcoin has the largest market financial resources of any decentralized digital currency.⁸ Even though Bitcoin is the most widely circulated digital currency, many other digital currencies are available, such as Ethereum, Ripple, Litecoin, and Monaro, to name a few. The concept of having a decentralized payment system is very enticing to several citizens and entities. Nevertheless, criminals continue to use digital currency as a means to launder illicit funds without detection. Sophisticated criminals even use digital privacy coins, mixers, and blenders, to further exasperate law enforcement tracing abilities.

Know-your-customer (KYC) has become a common term within the banking industry. KYC is often referred to as the customer identification programs (CIP) as mentioned in the USA PATRIOT Act.⁹ The customer identification program or the term used now as KYC was purposely left vague to allow the banking industry flexibility in implementing this requirement.¹⁰ The KYC portions of the USA Patriot Act were used to verify new customers and not focus on longtime loyal customers.¹¹ With the development of new technology, individuals can open bank accounts and transfer money without appearing at a local bank. This same technology allows criminals to move illicit money throughout the financial system while providing limited identification to banks. Appropriate KYC rules governing financial institutions are crucial in maintaining financial integrity to identify the source of money.¹² The BSA must provide banks with a

⁸ William Frentzen and Kathryn Haun, *United States vs BTC-E and Alexander Vinnik* (Washington, DC: Department of Justice, 2017), 3, <https://www.justice.gov/usao-ndca/press-release/file/984661/download>.

⁹ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism, Public Law 107–56, 3162 H.R. 272 (2001), 317, <https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf>.

¹⁰ Steve Cocheo, "Flexible Patriot Rules Prove Double-Edged Blade," *ABA Banking Journal* 95, no. 12 (December 2003): 52, ProQuest.

¹¹ Cocheo, 54.

¹² Federal Financial Institutions Examination Council, *Bank Secrecy Act/Anti-Money Laundering Examination Manual*, 3.

minimum standard for a client to open an account. These rules should ensure consistency among local and national banks, while carefully considering the implications of international banking.

With the development of the fintech industry, access to mobile money and peer-to-peer (P2P) transfers continue to increase. As more consumers and merchants embrace P2P networks solutions, criminals exploit these new platforms to launder illicit funds. Many P2P services meet the definition of financial institutions or money transmitters under the BSA/AML rules, as defined by the Financial Crimes Enforcement Network (FinCEN). The BSA should clearly define P2P services. Many fintech P2P services are not maintaining an adequate KYC program, anti-money laundering program, or filing appropriate CTRs. The BSA should address P2P transactions by using not only specific payment cards but also the international mobile equipment identity (IMEI), international mobile subscriber identity (IMSI), and the integrated circuit card identifier (ICCID). Regulators must hold P2P payment services more accountable by increased monitoring and using fintech to detect the movement of illicit funds by mandating P2P services monitor not only payment cards, but also phone devices through IMEI, IMSI, and ICCID for fraud detection.

This thesis discusses the advantages and disadvantages of ML, digital currency, KYC, and P2P technologies. An analysis of the technologies will consider cost, ease of implementation, sustainability, accuracy, privacy concerns, and public and political acceptability. A matrix will be developed objectively ranking each criterion and concluding with a detailed discussion on the results. The arguments will focus on bank executives, law enforcement, civil libertarian groups followed by a comprehensive analysis.

This document concludes with several recommendations to improve and updated the BSA. First, raising the monetary threshold of CTR filing from \$10,000 to \$60,000, the rate of inflation. Furthermore, the BSA should grant the U.S. Secretary of Treasury the ability to raise the monetary CTR filing on a five-year basis to adjust for inflation. The current monetary thresholds for SARs should remain the same, and the highly contested beneficial ownership provision should be added.

Advanced technology, like ML and distributed ledger technology, should not be mandated in the BSA but encouraged as the technology develops. Currently, the complexity of the technology, the monetary cost to banking institutions, privacy concerns, and political oppositions are all reasons for not mandating this type of technology in the BSA.

On the other hand, the BSA should regulate digital currency. FinCEN has already mandated several regulations on digital currency exchangers, but these regulations should be discussed and addressed by legislators. Advanced digital privacy coins, mixers, and tumblers also should be regulated within the BSA.

This thesis also recommends a minimum standard for a client to open an account. As a KYC requirement, fintech can utilize biometrics as an additional provision. Also, using a risk-based approach regarding KYC, as suggested by the Financial Crimes Task Force.¹³ These recommendations ensure consistency not only throughout the United States but also globally. Finally, P2P payment services should increase monitoring of financial transactions as related to IMEI, IMSI, and ICCID.

Supporters and challengers of the BSA all agree on the need to update the historical mandates within the act to address emerging threats and technology. As criminal organizations continue to move money throughout the U.S. financial services sector, legislators should amend the BSA to address these areas of concern to ensure financial stability and integrity. Legislators should also be cautious in restricting innovation within the United States, as fintech encourages financial ingenuity and security to accelerate financial services globally.

¹³ Financial Action Task Force on Money Laundering, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* (Paris, France: Financial Action Task Force on Money Laundering, 2018), 62–63, www.fatf-gafi.org/recommendations.html.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I want to begin by thanking the U.S. Secret Service, specifically the executives within the Office of Investigations and the San Francisco Field Office, for allowing me the opportunity to pursue this master's program through the Naval Postgraduate School's Center for Homeland Defense and Security (CHDS). I am also grateful to the members of the San Jose Resident Office, particularly during the In-Resident sessions of this course. They were outstanding in maintaining the office duties and operations in my absence.

Professor Shannon Brown, my co-advisor, assisted with the construction and shaping of this academic paper. He provided guidance and a level of experience in this subject that significantly enriched my journey.

Professor Richard Bergin, my co-advisor, provided structure and direction during the proposal process that greatly assisted with the scoping of this project. Likewise, to Professor Lauren Wollman and the entire CHDS writing and research staff at the center for their continuous mentoring and instructions during this research excursion.

To the members of CHDS cohort 1803/1804, it has been an honor to endure this academic journey with each one of you. You continuously challenged my perspectives and biases, along with broadening my knowledge and understanding. I will always be truly grateful and look forward to our lasting friendships.

Lastly and most importantly, I would like to thank my wife for the continued support during this challenging academic endeavor. Being pregnant, subsequently taking care of a newborn, along with a loving preschooler, and working a full-time job during this process, cannot be described in words. She never wavered during this pursuit and continuously held the household and family together. I pray for many more enjoyable years together as a family.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

The Bank Secrecy Act (BSA) of 1970 mandates that financial institutions in the United States assist U.S. law enforcement (LE) agencies in detecting and preventing the movement of illicit money through the nation’s financial system.¹

Based on this law, banks are required to “file reports of cash transactions exceeding \$10,000 (daily aggregated amount), and to report suspicious activity” indicative of potential money laundering.² Providing and preserving these records allow law enforcement the ability to pursue and arrest criminals involved in money laundering or other financial crimes. Since the inception of the BSA, legislators have provided minimal updates, and the monetary thresholds of the currency transaction reports (CTRs) and suspicious activity reports (SARs) need to be addressed.

The innovations in financial technology (fintech) create another payment method for criminals to move money and obfuscate law enforcement. Currently, the BSA does not adequately address emerging technologies like machine learning (ML), digital currency, know-your-customer (KYC), and peer-to-peer (P2P) technology. In November 2018, the senior deputy comptroller Grovetta Gardineer, for Compliance and Community Affairs testified before the Senate Committee on Banking, Housing, and Urban Affairs, “It is critical that the nearly 50-year-old BSA/AML [Bank Secrecy Act/Anti-Money Laundering] regime be updated and enhanced to address today’s threats and better utilize the capabilities of modern technology in protecting the financial system from illicit

¹ “FinCEN’s Mandate from Congress,” Financial Crimes Enforcement Network, accessed February 4, 2019, <https://www.fincen.gov/resources/fincens-mandate-congress>.

² Financial Crimes Enforcement Network.

activity.”³ As criminals continue to move money throughout the financial system, lawmakers should amend the BSA to address emerging fintech.

In dealing with the current monetary thresholds and advanced technology, a delicate balance exists between increasing regulation to prevent crime and hindering the growth of innovation and customer convenience. For example, P2P technology allows for the movement of funds among the financial sector, but the reporting requirements are ambiguous as to the movement of cash.⁴ Also, with the opening of accounts online, customer identification is an increasing concern; “know your customer” is a common motto within the banking industry, but with the development of new technologies, different techniques can identify customers whether through biometrics or the use of international mobile equipment identity numbers. The BSA does not explicitly address these types of technological advances to address money-laundering detection.

B. RESEARCH QUESTION

How can the BSA be reformed to address the monetary thresholds and emerging technology to prevent money laundering and illicit financing?

C. BACKGROUND

1. Overview of the Bank Secrecy Act

Money laundering has been an ongoing problem for years and continues to pose a threat to international economies regardless of the BSA regulations. Global money laundering transaction is estimated to be around \$1–2 trillion annually.⁵ This amount is

³ *Combating Money Laundering and Other Forms of Illicit Finance: Regulator and Law Enforcement Perspectives on Reform: Hearing before the Committee on Banking, Housing, and Urban Affairs, Senate, 115th Cong., 2nd sess., November 29, 2018, 13, <https://www.banking.senate.gov/hearings/10/24/2018/combating-money-laundering-and-other-forms-of-illicit-finance-regulator-and-law-enforcement-perspectives-on-reform>.*

⁴ Benjamin Lo, “Fatal Fragments: The Effect of Money Transmission Regulation on Payments Innovation,” *Yale Journal of Law and Technology* 18, no. 1 (2017): 126, <https://digitalcommons.law.yale.edu/yjolt/vol18/iss1/4/>.

⁵ Trevor White, Mark Anderson, and Didier Lavion, *Adjusting the Lens on Economic Crime* (PwC US, 2016), 41.

equal to 2 to 5% of the global GDP (gross domestic product).⁶ According to a 2011 United Nations Office on Drugs and Crime, law enforcement authorities seize less than 1% of global illicit funds.⁷ Over the years, Congress has adjusted the BSA to combat the movement of unlawful money.

Congress enacted the Bank Secrecy Act of 1970 to prevent criminals from hiding or laundering their illicit gains through the U.S. banking system. The statute's objective forced financial institutions to maintain currency transactions reports, along with identifying individuals conducting these illegal transactions.⁸ With the preservation of these financial statements, law enforcement agencies can detect and arrest criminals involved in financial offenses against the state.

The Money Laundering Control Act augmented the BSA and made money laundering a federal crime. In 1986, Congress criminalized money laundering by passing two significant sections, Title 18 U.S.C. 1956 (Money Laundering Crime) and Title 18 U.S.C. 1957 (Monetary Transactions Crime).⁹ Money laundering crime specifies the criminal activity to disguise or conceal the movement of money used for drug trafficking, organized misconduct, or other financial crimes. Monetary transactions crime is anyone who "knowingly engages" or "attempts to engage" in an illegal monetary transaction.¹⁰ These two laws enforce U.S. efforts to pursue money launders aggressively.

The BSA received further regulation from the Money Laundering Suppression Act of 1994. This act provided guidance and also empowered banking regulators to stop money laundering in two significant ways.¹¹ First, regulators' training from law enforcement regarding recent trends used by criminals and examination procedures to

⁶ White, Anderson, and Lavion, 41.

⁷ White, Anderson, and Lavion, 41.

⁸ Federal Financial Institutions Examination Council, *Bank Secrecy Act/Anti-Money Laundering Examination Manual*, 3.

⁹ Charles Plombeck, *The International Lawyer* (Cary, NC: American Bar Association, 1988), 2–8.

¹⁰ Plombeck, 8.

¹¹ Cory Howard, "Financial Crimes Compliance Self-Governance: Applying the Faragher Defense to Bank Secrecy Act/Anti-Money Laundering Violations," *The University of Memphis Law Review* 48, no. 1 (2017): 57, https://www.memphis.edu/law/documents/howard_financialcrimescomplianceself-governance.pdf.

detect money laundering schemes was enhanced.¹² Second, the Secretary of Treasury authorized regulators the ability to impose civil money penalties on financial institutions.¹³ This act streamlined the civil penalty cases by removing the older cumbersome process.¹⁴ With this provision, depository institutions received training and were held accountable by the risk of civil money penalties.

Federal regulators released the long-awaited new SAR in 1996. The new SAR requirements replaced the criminal referral forms and restructured the reporting requirements using computer software.¹⁵ With the new requirement, financial institutions only file with Financial Crimes Enforcement Network (FinCEN) instead of multiple law enforcement agencies and the monetary reporting threshold increased.¹⁶ These new regulations reduced the administrative burdens on the banking industry.

The USA PATRIOT Act of 2001 also enhanced the BSA's customer identification program. Section 311 of the Act allows the Secretary of Treasury to enact "special measures" against any foreign county or foreign institution involved in money laundering.¹⁷ These special measures include reporting certain transactions, record keeping, collection of beneficial ownership, payable account information, and gathering correspondent accounts.¹⁸ Under section 326 of the Act, the Secretary of Treasury sets forth a standard for customers opening bank accounts at financial institutions.¹⁹ At a minimum, banking institutions must verify the identity of any account holder, maintain

¹² U.S. Government Accountability Office, *Bank Secrecy Act: Opportunities Exist for FinCEN and the Banking Regulators to Further Strengthen the Framework for Consistent BSA Oversight*, GAO-06-386 (Washington, DC: U.S. Government Accountability Office, 2006), 24, <https://www.gao.gov/assets/160/157691.pdf>.

¹³ U.S. Government Accountability Office, 24.

¹⁴ U.S. Government Accountability Office, 24.

¹⁵ Anonymous, "New Suspicious Activity Report Streamlines Reporting System," *ABA Bank Security & Fraud Prevention*; 3, no. 1 (January 1996): 1, ProQuest.

¹⁶ Anonymous, 1.

¹⁷ Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, H. Res. 3162, 107th Cong., 1st. sess., 21, <https://www.congress.gov/bill/107th-congress/house-bill/3162/text/enr>.

¹⁸ USA PATRIOT ACT, 28–32.

¹⁹ USA PATRIOT ACT, 46.

accurate records, and consult a list of suspected terrorists.²⁰ The USA PATRIOT Act strengthened the BSA by enforcing these additional provisions.

Based on these alterations to the BSA, the U.S. government is holding banks accountable for not having an effective anti-money laundering procedure in place. In 2012, HSBC Group “agreed to forfeit \$1.256 billion as part of its deferred prosecution agreement” and “pay \$665 million in civil penalties” for violating the BSA.²¹ According to the Department of Justice, \$881 million in drug proceeds were laundered through HSBC’s financial system.²² In 2017, the Deutsche Bank was also fined \$41 million by the U.S. Federal Reserve for not having an adequate anti-money laundering program.²³ They were provided with guidelines and deadlines to bring their internal systems into compliance.²⁴ Regulators continue to use the BSA to hold financial institutions accountable.

2. Financial Fraud Trends Involving New Technology

Throughout history, the American currency system continues to evolve from paper currency to payment cards to wire transfers and now to digital currency in the form of bits and bytes. Fintech describes the recent transformation taking place throughout the global financial services sectors.²⁵ The use of contactless payments, digital wallets, and apps are the norm for purchasing or transferring funds.²⁶ Users and financial institutions are adopting fintech solutions as a new way to conduct money transfers and payments.

²⁰ USA PATRIOT ACT, 46.

²¹ United States Attorney’s Office, “HSBC Holdings Plc. and HSBC Bank USA N.A. Admit to Anti-Money Laundering and Sanctions Violations, Forfeit \$1.256 Billion in Deferred Prosecution Agreement,” Department of Justice, December 11, 2012, <https://www.justice.gov/opa/pr/hsbc-holdings-plc-and-hsbc-bank-usa-na-admit-anti-money-laundering-and-sanctions-violations>.

²² United States Attorney’s Office.

²³ Ann Misback, *United States of America before the Board of Governors of the Federal Reserve System Washington, D.C.* (Washington, DC: The Federal Reserve Board, 2017), 13, <https://www.federalreserve.gov/newsevents/pressreleases/enforcement20170530a.htm>.

²⁴ Misback, 5–14.

²⁵ Michael Lamer, *The Future of Fintech ~ The New Standard* (United Kingdom: Juniper Research, 2019), 1, <https://www.juniperresearch.com/document-library/white-papers/the-future-of-fintech-the-new-standard-white-paper>.

²⁶ Lamer, 2.

Money launders continue to increase in sophistication and complexity with the use of fintech-like digital currency. This new currency has become a game changer regarding the movement of illicit money because anonymous transactions are allowed. In using this new form of currency, criminals can avoid using the U.S. financial system and transfer money without accessing a centralized government authority that draws serious scrutiny from regulators.²⁷ Digital currencies have become the money of choice to move funds anonymously and avoid law enforcement detection.

PayPal is an example of one fintech that operates a worldwide P2P online money transfer platform. Simser describes PayPal as “an online intermediary that processes payments between users over the internet.”²⁸ The Federal Deposit Insurance Corporation determined that PayPal was not a banking institution.²⁹ Later though in 2009, FinCEN considered PayPal a money transmitter from the anti-money laundering perspective.³⁰ According to Juniper Research, mobile wallet users will increase from the currently 2.3 billion users to 4 billion users by 2024. Also, fintech platform revenues are expected to reach \$638 billion by 2024.³¹ These numbers reveal an explosive growth in online payment services and fintech platforms like PayPal and other web-based apps.

As announced in June 2019, Facebook is expected to launch a new cryptocurrency called Libra in 2020.³² With this new technology, users can transfer money, pay bills, or send digital currency using a digital wallet available in messenger, or as a separate app.³³ Facebook states:

²⁷ Jeffrey Simser, “Bitcoin and Modern Alchemy: In Code We Trust,” *Journal of Financial Crime*, 22, no. 2 (2015): 157, <http://dx.doi.org/10.1108/JFC-11-2013-0067>.

²⁸ Simser, 163.

²⁹ Simser, 163.

³⁰ “FinCEN Issues Ruling (FIN-2008-R011) on Whether a Company that Engages in Microfinance Is a Money Services Business,” Financial Crimes Enforcement Network, 1, February 20, 2009, <https://www.fincen.gov/resources/statutes-regulations/administrative-rulings/fincen-issues-ruling-fin-2008-r011-whether>.

³¹ Lamer, *The Future of Fintech*, 8.

³² Facebook, “A New Digital Wallet for a New Digital Currency,” Facebook Newsroom, June 18, 2019, <https://newsroom.fb.com/news/2019/06/coming-in-2020-calibra/>.

³³ Facebook.

For many people around the world, even basic financial services are still out of reach: almost half of the adults in the world don't have an active bank account, and those numbers are worse in developing countries and even worse for women. The cost of that exclusion is high — approximately 70% of small businesses in developing countries lack access to credit and \$25 billion is lost by migrants every year through remittance fees.³⁴

This new cryptocurrency is one example of fintech changing the global financial payment systems, but it also allows another method for criminals to move money globally.

As the cost of regulatory compliance continues to increase, bankers need to update their legacy monitoring systems with innovative technology regularly. Combating the financing of terrorism and detecting money launderers continue to be an expensive and challenging endeavor even for well-established and sophisticated financial institutions.³⁵ Banking executives should embrace fintech solutions, and regulators need to monitor this new technology closely to prevent money laundering while allowing continued innovation.

D. RESEARCH DESIGN

This thesis is a policy analysis and proposal, conducted according to the eight steps recommended by Eugene Bardach, for legislative and technological improvements to financial fraud detection. Bardach's policy analysis ensures an accurate and efficient assessment of the potential outcome.³⁶ Furthermore, policy leaders will have a comprehensive understanding of the benefits and consequences of specific policy action.³⁷

First, the background of the BSA and a proposed Congressional Bill called the Counter Terrorism and Illicit Finance Act is discussed in detail. On June 12, 2018, Representative Stevan Pearce introduced the bill in the House of Representatives, but it

³⁴ Facebook.

³⁵ White, Anderson, and Lavion, *Adjusting the Lens on Economic Crime*, 44.

³⁶ Holquist, "How to Conduct an Effective Policy Analysis."

³⁷ Holquist.

never appeared for a vote.³⁸ The Counter Terrorism and Illicit Finance Act would alter the BSA to address the SAR and CTR requirements and advanced technology. It is currently unknown whether the bill will be reintroduced in 2019, but this bill and the BSA based on the criteria of risk to public safety, costs to banks, impact on law enforcement and political opposition are evaluated with recommendations made. The examination of the BSA is limited to elements that pertain to money laundering detection by financial institutions.

The second part of this proposed thesis is an evaluation of several emerging financial technologies that might help detect, prevent, or investigate money laundering, with an emphasis on CTR and SAR requirements. Specifically, the focus is on machine learning, digital currency, KYC technology, and P2P transfers.

The analysis of the technologies consider complexity, costs to banks, privacy concerns, and political opposition. Each category is given a specific criterion to distinguish a low, medium, or high rating. Each category is given a specific criterion to distinguish a low, medium, or high rating. A matrix objectively ranks each criterion and concludes with a detailed discussion on the results. For example, financial institutions favor any policy recommendation that alleviates workforce stressors and expense, and that reduces reporting requirements. On the other hand, law enforcement and FinCEN favor policy recommendations that increase reporting requirements for specific insight into the movement of illicit money. Civil libertarian groups are concerned with privacy and the sharing of personal information between banks and law enforcement.

For each criterion, data and evidence obtained from financial institutions, private sector companies, congressional briefings, and comparing often-contradictory sources of academic research are used. Based on these guidelines, this thesis makes recommendations based on current gaps within the BSA.

³⁸ Counter Terrorism and Illicit Finance Act.

E. CHAPTER OUTLINE

This thesis explores gaps within the BSA with a specific emphasis on current monetary thresholds and financial technology. Chapter I defines the problem space along with the primary research question. Also, this chapter presents a historical overview of the BSA and recent financial fraud trends involving new technology to obfuscate law enforcement.

The second chapter provides a literature review on the Counter Terrorism and Illicit Finance Act and fintech. This chapter also addresses the current arguments regarding the current monetary thresholds and fintech to monitor and regulate the movement of illicit funds.

Chapter III addresses the Counter Terrorism and Illicit Finance Act, which amends the BSA. This thesis describes the objective of this act with the advantages and limitations of making this act a law. The thesis describes various policy options and provides a detailed analysis using a policy options matrix.

In Chapter IV, the thesis provides an overview of recent financial technologies, specifically, machine learning, digital currency, KYC, and P2P. This chapter analyzes each fintech for possible impacts on the BSA and each option is rated in a matrix.

The fifth chapter provides a series of recommendation for policymakers regarding the BSA along with implementation challenges. This chapter concludes with future areas of research.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

The literature on reforming the BSA yields four broad categories: the historical debate, regulatory issues, a proposed congressional bill called the Counter Terrorism and Illicit Finance Act, and the use of advanced fintech to monitor money-laundering activities.

A. HISTORICAL DEBATE

Since the law was enacted in 1970, the BSA has been highly contested by regulators who demand that banks maintain financial records along with specific reporting requirements to prevent money laundering versus the violations of privacy as guaranteed under the Fourth Amendment by civil liberty advocates.³⁹ A three-judge federal panel even ruled parts of the BSA unconstitutional two years after the BSA became law in a 2:1 decision in *Stark v. Connally*.⁴⁰ Following the ruling, James Dobe, the current executive vice president of Wells Fargo, stated, “Our position, since the regulations were first spelled out by the Treasury Department, were [*sic*] that they were too all-inclusive and had gone beyond what was necessary to stop the illegal flow of funds overseas. We are pleased that the court agrees.”⁴¹ Judge Hamilin was the lone dissenting opinion who stated the courts should be “slow in finding a congressional enactment unconstitutional.”⁴² The court upheld portions of the BSA that deal with foreign recordkeeping and reporting requirements.⁴³ The American Civil Liberties Union and the California Bankers Association also challenged the act’s constitutionality.⁴⁴ Business owners find confidentiality and secrecy attractive in dealing with trade and

³⁹ James E. Eldridge, “The Bank Secrecy Act: Privacy, Comity, and the Politics of Contraband,” *North Carolina Journal of International Law and Commercial Regulation* 11, no. 3 (1986): 668, <https://scholarship.law.unc.edu/ncilj/vol11/iss3/12/>.

⁴⁰ “Bank Secrecy Act Found to Violate Right of Privacy: Court Rules Unconstitutional Part Requiring Reports of Activity in U.S. Accounts Other Sections Are Upheld,” *Wall Street Journal*, September 12, 1972.

⁴¹ “Bank Secrecy Act Found to Violate Right of Privacy.”

⁴² “Bank Secrecy Act Found to Violate Right of Privacy.”

⁴³ Eldridge, “The Bank Secrecy Act,” 677.

⁴⁴ “Bank Secrecy Act Found to Violate Right of Privacy.”

commerce.⁴⁵ Following the three-judge panel, the U.S. Supreme Court under Justice Rehnquist, reversed the lower court's ruling and upheld the BSA as constitutionally valid.⁴⁶

When it comes to this topic, the Treasury Department argues that the BSA is necessary for reducing the movement of illicit money and will benefit the general public.⁴⁷ The provisions of the BSA require banks to report "large currency transactions," which assists in the detection of money laundering, tax evasion, and securities fraud.⁴⁸ Historically, it has been challenging to prosecute tax and securities violations without information regarding secret offshore bank accounts.⁴⁹ Likewise, the Security and Exchange Commission has expressed concern over the integrity of the financial system given the increased safe havens for criminal activity.⁵⁰

B. REGULATORY ISSUES

The regulatory requirements within the BSA need to consider the costly burden placed on financial institutions while not allowing criminals to exploit the Federal Reserve System. On November 29, 2018, the senior deputy comptroller for compliance and community affairs, Grovetta Gardineer, testified before the Senate Committee on Banking, Housing, and Urban Affairs, about updating the age-old BSA and using fintech to protect the U.S. financial sector.⁵¹ The testimony discusses the reform and modernization needed for AML regulations without compromising law enforcement

⁴⁵ Eldridge, "The Bank Secrecy Act," 679.

⁴⁶ Eldridge, 678.

⁴⁷ "Bank Secrecy Act Found to Violate Right of Privacy."

⁴⁸ Eldridge, "The Bank Secrecy Act," 668.

⁴⁹ "The 1970 Bank Secrecy Act and the Right of Privacy," *William & Mary Law Review* 14, no. 4 (1973): 929, <https://scholarship.law.wm.edu/wmlr/vol14/iss4/7>.

⁵⁰ Eldridge, "The Bank Secrecy Act," 671.

⁵¹ S., *Combating Money Laundering*, 1.

efforts.⁵² Jodi Avergun and Colleen Kukowski, a former U.S. Attorney and FBI employee, agree with Gardineer’s concerns over AML regulations.⁵³

Furthermore, Paul Treleaven, a professor of the Financial Computer Center in London advises that effective financial regulations are crucial in the fintech industry.⁵⁴ The author writes on behalf of EY, a global company and leader in financial transaction and advisory services.⁵⁵ The author describes current regulatory pressures and the need for regulatory reform without hindering the growth of new businesses.⁵⁶ He explains that a relationship must exist between the regulators and the regulated for a cohesive solution.⁵⁷

Along the same line, Benjamin Lo published an article in the *Yale Journal of Law and Technology* describing the regulatory burden on payment startup companies.⁵⁸ The articles explains that fintech companies must deal with fragmented regulations among the various states along with federal regulation.⁵⁹ Lo contends that financial regulation should be harmonized across states to allow for more opportunities for innovation.⁶⁰ Agreeing with Lo, Paul Treleavan mentions regulators, financial institutions, and fintech companies must work together to improve financial regulations.⁶¹ Both Lo and Treleavan, along with the Counter Terrorism and Illicit Finance Act, deputy comptroller,

⁵² S., *Combating Money Laundering*, 2.

⁵³ Jodi Avergun and Colleen Kukowski, “Complying with AML Laws: Challenges for the Fintech Industry,” *Crowdfund Insider*, April 5, 2016, <https://www.crowdfundinsider.com/2016/04/83845-complying-with-aml-laws-challenges-for-the-fintech-industry/>.

⁵⁴ Philip Treleaven, “Financial Regulation of FinTech,” *Journal of Financial Perspectives: FinTech* 3, no. 3 (Winter 2015): 2–3, [https://www.ey.com/Publication/vwLUAssets/ey-financial-regulation-of-fintech/\\$FILE/ey-financial-regulation-of-fintech.pdf](https://www.ey.com/Publication/vwLUAssets/ey-financial-regulation-of-fintech/$FILE/ey-financial-regulation-of-fintech.pdf).

⁵⁵ Treleaven, 17.

⁵⁶ Treleaven, 2.

⁵⁷ Treleaven, 11.

⁵⁸ Lo, “Fatal Fragments,” 111.

⁵⁹ Lo, 111.

⁶⁰ Lo, 111.

⁶¹ Treleaven, “Financial Regulation of FinTech,” 14.

and congressmen, encourage innovation and competition without hindering growth from excessive oversight and financial regulation.⁶²

Lo also describes an interesting debate around broad money transmitter laws.⁶³ In which, regulators contend that institutions moving large amounts of money should be regulated for consumer protection and money laundering prevention.⁶⁴ On the other hand, fintech companies criticize these heavy regulatory requirements that stifle innovation and growth.⁶⁵

C. COUNTER TERRORISM AND ILLICIT FINANCE ACT

The Counter Terrorism and Illicit Finance Act, if enacted into law under the original draft, would have been “the most substantial overhaul to the Bank Secrecy Act (‘BSA’) since the PATRIOT Act.”⁶⁶ In June 2018, Representative Stevan Pearce and Blaine Luetkemeyer introduced the highly contested Counter Terrorism and Illicit Finance Act, formally known as H.R. 6068.⁶⁷ This act would increase the dollar amount for SAR and CTR requirements and allow for the sharing of suspicious activities among financial groups.⁶⁸ The bill also requests that the Secretary of Treasury along with federal law enforcement agencies review current reporting requirements under the BSA to reduce the current regulatory burdens on financial institutions.⁶⁹

⁶² Julien Courbe, *Financial Services Technology 2020 and Beyond: Embracing Disruption* (New York: PricewaterhouseCoopers, 2016), 9, <https://www.pwc.com/gx/en/financial-services/assets/pdf/technology2020-and-beyond.pdf>.

⁶³ Lo, “Fatal Fragments,” 113.

⁶⁴ Lo, 113.

⁶⁵ Lo, 113.

⁶⁶ Brad Gershel, “Beneficial Ownership Provision Stripped from Latest Draft of Counter Terrorism and Illicit Finance Act,” *National Law Review*, June 20, 2018, <https://www.natlawreview.com/article/beneficial-ownership-provision-stripped-latest-draft-counter-terrorism-and-illicit>.

⁶⁷ Counter Terrorism and Illicit Finance Act, H.R. 6068, 115th Cong., 2nd sess., June 12, 2018, 1, <https://www.congress.gov/115/bills/hr6068/BILLS-115hr6068ih.pdf>.

⁶⁸ Counter Terrorism and Illicit Finance Act, 1.

⁶⁹ Counter Terrorism and Illicit Finance Act, 3.

Before the bill was introduced, the original draft was stripped of the beneficial ownership provision.⁷⁰ This provision mandates that shell companies or front companies reveal their true beneficial owner, which has caused great debate.⁷¹

The National Association of Federally-Insured Credit Unions (NAFCU) along with 11 other financial industry trades supported the beneficial ownership provision.⁷² The associations stated in a joint letter to the finance committee:

It is our hope that this will help reduce the anticipated burden of complying with the requirements of the CDD rule. Financial institutions should be able to rely on the information reported by businesses to FinCEN, which would, in turn, reduce the reporting burden on those businesses.⁷³

Along with encouraging the provision, the association supports the use of machine learning and new technology for detecting suspicious activity.⁷⁴

Along the same line, the Delaware Secretary of State sent a letter to the Financial Services Committee Chairman and ranking members endorsing the beneficial ownership provision.⁷⁵ The letter encourages a nationwide framework of collecting beneficial ownership information for combating money laundering and financing of terrorism rather than an unsystematic partial state-based approach with loopholes.⁷⁶ The provision also provides law enforcement with tools needed to combat financial crimes successfully.⁷⁷

Law enforcement, specifically the Fraternal Order of Police (FOP), which is the world's largest sworn law enforcement organization, supports the beneficial ownership

⁷⁰ Gershel, "Beneficial Ownership Provision Stripped."

⁷¹ Gershel.

⁷² National Association of Federally-Insured Credit Unions, "NAFCU, Others Support Bill to Strengthen Anti-Money Laundering Efforts," Newsroom, NAFCU, January 5, 2018, <https://www.nafcu.org/newsroom/nafcu-others-support-bill-strengthen-anti-money-laundering-efforts>.

⁷³ National Association of Federally-Insured Credit Unions.

⁷⁴ National Association of Federally-Insured Credit Unions.

⁷⁵ Jeffrey Bullock, *Letter to Chairman Hensarling* (State of Delaware, Department of State, 2018), 1, <https://thefactcoalition.org/wp-content/uploads/2018/06/DE-June-2018-Letter-to-HFSC-on-BOT.pdf>.

⁷⁶ Bullock, 1.

⁷⁷ Bullock, 1.

provision. For years, the FOP has supported legislations to reveal the true beneficial ownership information to combat criminal activity.⁷⁸ The FOP further believes the beneficial ownership information of the Counter Terrorism and Illicit Finance Act is the most critical provision, and without this legislation, law enforcement will not have the adequate tools to pursue criminal activity.⁷⁹ Federal law enforcement agencies have discontinued criminal investigations based on the difficulty in determining true beneficial ownership.⁸⁰

On the other hand, FreedomWorks, an association that supports individual liberties and free markets, strongly opposes the Counter Terrorism and Illicit Finance Act. FreedomWorks states the Act along with the ownership provision “detonates due process and the right to privacy.”⁸¹ FreedomWorks believes the Act encourages businesses to spy on banking customers and destroys another level of individual privacy.⁸² According to Jason Pye, a vice president for FreedomWorks, “The government would gain warrantless access to even more sensitive financial records protected by the Fourth Amendment.”⁸³

Congressman Luetkemeyer and Pearce argue the Counter Terrorism and Illicit Finance Act will assist in protecting and safeguarding the U.S. financial system.⁸⁴

⁷⁸ Chuck Canterbury, *Letter to Chairman and Representative Waters* (Washington, DC: Fraternal Order of Police, 2018), 1, <https://static.politico.com/bb/07/a3e3dfbd48aab8446528bf02bcad/fop-on-beneficial-ownership.pdf>.

⁷⁹ Canterbury.

⁸⁰ J. W. Verret, “Terrorism Finance, Business Associations, and the ‘Incorporation Transparency Act,’” *Louisiana Law Review* 70, no. 3 (2010): 857, <https://digitalcommons.law.lsu.edu/lalrev/vol70/iss3/5/>.

⁸¹ Jason Pye, “Oppose the Counter Terrorism and Illicit Finance Act,” *Oppose the Counter Terrorism and Illicit Finance Act* (blog), November 28, 2017, <https://www.freedomworks.org/content/oppose-counter-terrorism-and-illicit-finance-act>.

⁸² Pye.

⁸³ Pye.

⁸⁴ Blaine Luetkemeyer and Steve Pearce, “It’s Time to Modernize the Bank Secrecy Act,” *American Banker*, June 13, 2018, <https://www.americanbanker.com/opinion/its-time-to-modernize-the-bank-secrecy-act>.

Furthermore, the bill will assist in updating anti-money laundering and counterterrorism standards throughout the financial industry.⁸⁵

D. FINANCIAL TECHNOLOGY

Several key industry leaders have mentioned the need for advanced technology in financial services. One of these leaders is PricewaterhouseCoopers (PwC), which assists businesses with digital transformation leveraging fintech so that companies can maintain efficient and agile operations.⁸⁶ Julien Courbe, the Global Financial Service Technology Leader for PwC, describes that executives must understand technology to compete in financial services.⁸⁷ Agreeing with this statement, Paul Treleavan, the author of *Financial Regulation of FinTech*, recommends financial services need to improve through automation and analytic standards, and reduce systemic risk.⁸⁸

Providing statistics and graphs describing the increase in fintech, KPMG operates globally in over 150 countries and territories that publishes a bi-annual report on recent trends in the fintech industry.⁸⁹ KPMG also derives data from a company called PitchBook.⁹⁰ PitchBook tracks datasets and features across public and private markets, venture capital, private equity, and mergers and acquisitions.⁹¹ With this combined data, the article describes the global rise of fintech and the way technology is transforming the financial services industry. Several other scholars confirm the rise of fintech.

1. Machine Learning for Fraud Detection

One obligation under the BSA is monitoring for suspicious activity. Failure to comply can be extremely costly. In February 2018, U.S. Bancorp agreed to pay a fine of

⁸⁵ Luetkemeyer and Pearce.

⁸⁶ Treleavan, “Financial Regulation of FinTech.”

⁸⁷ Courbe, *Financial Services Technology 2020 and Beyond*, 2.

⁸⁸ Treleavan, “Financial Regulation of FinTech,” 13.

⁸⁹ Ian Pollari and Anton Ruddenklau, *The Pulse of Fintech 2018: Biannual Global Analysis of Investment in Fintech* (Zurich: KPMG International, 2018), 2, <https://home.kpmg/content/dam/kpmg/us/pdf/2018/07/pof-1H-18-report.pdf>.

⁹⁰ Pollari and Ruddenklau, 56.

⁹¹ “Home Page,” Pitch Book, accessed February 8, 2019, <https://pitchbook.com/>.

\$528 million for violating the BSA.⁹² ML is a recent fintech that can assist with monitoring for illicit activity. The comptroller, Grovetta Gardiner, testified before Congress that banks should use new technology, such as artificial intelligence (AI) and ML, for increased monitoring of suspicious activity as a way to manage costs.⁹³ PwC, a leader in digital transformation, also agrees with this assessment.⁹⁴

In 2018, Massachusetts Institute of Technology (MIT) researchers attempted to reduce the number of false-positive transactions plaguing the financial sector by using transactional and historical data to increase the probability of fraud detection.⁹⁵ The researchers extracted over 200 separate features from historical payment information to obtain a profile of an individual's spending habits.⁹⁶ Using these features, the data scientists tested millions of transactions from an international bank using ML technology.⁹⁷ The results of the study revealed that using historical behavior data and transaction data achieved better results than ML solutions that rely merely on transactional features.⁹⁸ Based on the recency of the study and the transparency of the algorithm, no one has yet disputed their findings. This study does build on current private sector ML solutions that use transactional data and behavior analytics for fraud detection. The leading private sector companies operating in this space are Guardian Analytics, Stripe Radar; FICO Flacon Platform, Feedzai, and Kount Inc., to list a few. These

⁹² U.S. Attorney's Office, "Manhattan U.S. Attorney Announces Criminal Charges against U.S. Bancorp for Violations of the Bank Secrecy Act," United States Attorney's Office Southern District of New York, February 15, 2018, <https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-criminal-charges-against-us-bancorp-violations-bank>.

⁹³ S., *Combating Money Laundering*, 10.

⁹⁴ Courbe, *Financial Services Technology 2020 and Beyond*, 21.

⁹⁵ Roy Wedge et al., *Solving the False Positives Problem in Fraud Prediction Using Automated Feature Engineering* (Dublin, Ireland: European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases, 2018), 2, <http://www.ecmlpkdd2018.org/wp-content/uploads/2018/09/567.pdf>.

⁹⁶ Wedge et al., 2.

⁹⁷ Wedge et al., 1.

⁹⁸ Wedge et al., 15.

companies agree that using ML and behavioral analytics assists with money laundering detection; several hundred banks use this fintech platform.⁹⁹

Scholars and executive managers agree on the limitations of using this fintech. One of the main issues with ML is its “black box decision-making.”¹⁰⁰ Scholars define black box decision-making as an “opaque decision system,” like ML.¹⁰¹ In a real-world application, First Data Corporation states that government policies require an explanation of why a machine or algorithm made a decision.¹⁰² This information is difficult to ascertain and pass along to customers or upper-level executives without a proper explanation. In dealing with these concerns, Bank of America even created a council in 2017 with Harvard and MIT to conduct an academic study on the possible ethical consequences of using such technology.¹⁰³ Bank of America is providing the funding for a three-year academic study, which shows the concern business executives have with using algorithms to make business decisions.

Several scholars share the concerns of using ML and algorithms in the financial sector. Campbell-Verduyn, Goguen, and Porter explain these various concerns in an academic research article funded by the Social Sciences and Humanities Research Council of Canada. Their research explains the techno-dystopian perspectives of using big data and algorithmic governance.¹⁰⁴ Their work addresses the black-box issue of using algorithms and how they are layered behind mathematical equations, nondisclosure

⁹⁹ PR Newswire, “Guardian Analytics Will Feature Newest Real-Time Digital Banking Fraud Detection Solutions at Malauzai #InnovationNATION,” Markets Insider, March 22, 2018, <https://markets.businessinsider.com/news/stocks/guardian-analytics-will-feature-newest-real-time-digital-banking-fraud-detection-solutions-at-malauzai-innovationnation-1019043726>.

¹⁰⁰ First Data Corporation, *Machine Learning, Security and the Future of Fraud* (Atlanta: First Data Corporation, 2017), 8, <https://www.firstdata.com/downloads/pdf/MachineLearningSecurityandtheFutureofFraud.pdf>.

¹⁰¹ Riccardo Guidotti et al., “A Survey of Methods for Explaining Black Box Models,” *ACM Computing Surveys* 51, no. 5 (August 2018): 1, <https://doi.org/10.1145/3236009>.

¹⁰² First Data Corporation, *Machine Learning, Security and the Future of Fraud*, 8.

¹⁰³ Penny Crosman, “Bank of America, Harvard Form Group to Promote Responsible AI,” *American Banker*, April 10, 2018, <https://www.americanbanker.com/news/bank-of-america-harvard-form-group-to-promote-responsible-ai>.

¹⁰⁴ Malcolm Campbell-Verduyn, Marcel Goguen, and Tony Porter, “Big Data and Algorithmic Governance: The Case of Financial Practices,” *New Political Economy* 22, no. 2 (2017): 222, <http://dx.doi.org/10.1080/13563467.2016.1216533>.

agreements, and trade secrets. This contrast between the advantages and concerns of ML technology is ongoing throughout the financial sector. Should financial institutions be required to use this fintech for money laundering detection under the BSA?

2. Digital Currency

An ongoing debate is whether digital currency should be regulated under the BSA or remain unregulated as suggested by the Electronic Frontier Foundation (EFF).¹⁰⁵ Digital currency was designed to exchange money between users without going through a centralized banking system like the Federal Reserve System. Chief of the fraud unit, Scott Bradford from the U.S. Attorney's Office, District of Oregon, serves as the Computer Hacking and Intellectual Property Coordinator.¹⁰⁶ Bradford wrote a detailed article on recent cybercrime threats with a focus on digital currency. The author states that under the BSA, FinCEN requires that digital currency exchanges meet the same standards as other money services businesses under Title 31 U.S. Code § 5330.¹⁰⁷ The Director of FinCEN affirmed this statement in 2018 when stating that digital currency exchangers establish an anti-money laundering program and file SARs.¹⁰⁸ FinCEN even clarified that digital currency exchangers are considered money transmitters, whether located domestically or internationally.¹⁰⁹

On a more extreme level, Congressman Brad Sherman urged his fellow colleagues to pass legislation banning digital currency in the United States.¹¹⁰ He based

¹⁰⁵ Aaron MacKey, "California Lawmaker Pulls Digital Currency Bill after EFF Opposition," Electronic Frontier Foundation, August 18, 2016, <https://www.eff.org/deeplinks/2016/08/california-lawmaker-pulls-digital-currency-bill-after-eff-opposition>.

¹⁰⁶ Scott Bradford, "You've Been Served, but Does It Count: Serving a Criminal Corporate Defendant under Federal Rule of Criminal Procedure 4," *Department of Justice Journal of Federal Law and Practice* 67, no. 1 (February 2019): 270, <https://www.justice.gov/usao/page/file/1135861/download>.

¹⁰⁷ Registration of Money Transmitting Businesses, 31 U.S.C. § 5330 (2018), <https://www.uscode.house.gov>.

¹⁰⁸ Kenneth A. Blanco, "Prepared Remarks of FinCEN Director Kenneth A. Blanco, Delivered at the 2018 Chicago-Kent Block (Legal) Tech Conference," Federal Crimes Enforcement Network, August 9, 2018, <https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-2018-chicago-kent-block>.

¹⁰⁹ Bradford, "You've Been Served, but Does It Count," 240.

¹¹⁰ Litecoin Master, *Demonrat—Brad Sherman Law to Ban Bitcoin*, YouTube, video, 1:12, May 9, 2019, <https://www.youtube.com/watch?v=IkC-uXMoy4c>.

this statement on the Palestinian terrorist group, Hamas, using Bitcoin, and Iran using cryptocurrencies to circumvent financial sanctions.¹¹¹ The currency also diminishes the power of the Federal Reserve in regulating the economy.¹¹²

Anthony Pompliano strongly opposes the outlawing of digital currency. Pompliano, the founder of Morgan Creek Digital Assets and a leading advocate of bitcoin, understands Congressman Sherman’s concern about the world moving to non-sovereign currencies.¹¹³ Pompliano conveys that Sherman’s most significant donors are from the financial services companies; thus, the Congressman wants to protect his donors.¹¹⁴ Pompliano concludes by stating, “Bitcoin is better than fiat currencies.”¹¹⁵ Eventually, politicians will have to engage with not only crypto companies but financial institutions and private companies involved in the digital currency space.

The EFF, a nonprofit organization that defends civil liberties, user privacy, and innovation, agrees with Pompliano’s assessment.¹¹⁶ The EFF further explains that even though criminals may use cryptocurrencies for illicit activity, the U.S. government should not ban this new form of currency.¹¹⁷ Well-known cryptocurrency transactions, like Bitcoin and Ethereum, are recorded on public ledgers for anyone to see. Although, a growing number of digital currencies offer more privacy protection and anonymity on the public ledger.¹¹⁸ Another benefit, cryptocurrency may eventually assist many individuals with a low credit score or people without access to financial services.¹¹⁹

¹¹¹ Litecoin Master.

¹¹² Litecoin Master.

¹¹³ Anthony Pompliano, “Banning Bitcoin Will Drive More Adoption,” *Banning Bitcoin Will Drive More Adoption* (blog), May 10, 2019, <https://offthechain.substack.com/p/banning-bitcoin-will-drive-more-adoption>.

¹¹⁴ Pompliano.

¹¹⁵ Pompliano.

¹¹⁶ “About EFF,” Electronic Frontier Foundation, July 10, 2007, <https://www.eff.org/about>.

¹¹⁷ Rainey Reitman, “Why Outlawing Cryptocurrency Purchases Is a Terrible Idea,” Electronic Frontier Foundation, May 13, 2019, <https://www.eff.org/deeplinks/2019/05/why-bill-banning-cryptocurrency-purchases-americans-terrible-idea>.

¹¹⁸ Reitman.

¹¹⁹ Reitman.

3. Know-Your-Customer Rule

The KYC rule is another significant concern under the BSA, as Iza Wojciechowska explains the requirements for financial institutions. The purpose of KYC is to restrict the ability of criminals to move money throughout the financial system anonymously. Scholars explain that under the USA PATRIOT Act, financial institutions must comply with two main requirements, the “Customer Identification Program (CIP) and customer due diligence (CDD).”¹²⁰ Banks conduct their own CIP process, which varies among institutions.¹²¹ Several pieces of literature support Wojcieshowaska’s claim.

Dr. Norman Mugarura opposes the USA PATRIOT Act and KYC solutions. Working for Global Action Research and Development Initiative, he specializes in money laundering regulation and compliance.¹²² Dr. Mugarura argues that KYC solutions, along with the USA PATRIOT Act, causes confusion, controversies, and tension between bankers and customers.¹²³ Furthermore, the ill-defined regulation is counterproductive and allows banks to conduct extensive surveillance on financial transactions.¹²⁴

Alan Gelb, the author of “Balancing Financial Integrity with Financial Inclusion,” mentions another way to KYC. He agrees with Dr. Mugarura by stating KYC is becoming an inconvenience with customers, as bank requests additional information that thus creates more friction with customers.¹²⁵ Gelb considers an alternative solution is

¹²⁰ Iza Wojciechowska, “What Is KYC and Why Does It Matter?,” *Fin*, April 5, 2017, <http://fin.plaid.com/articles/kyc-basics>.

¹²¹ Wojciechowska.

¹²² Norman Mugarura, “Does the Broadly Defined Ambit of Money Laundering Offences Globally, a Recipe for Confusion than Clarity?,” *Journal of Money Laundering Control* 19, no. 4 (2016): 432, <http://doi.org/10.1108/JMLC-06-2015-0024>.

¹²³ Mugarura, 443.

¹²⁴ Mugarura, 443.

¹²⁵ Wojciechowska, “What Is KYC and Why Does It Matter?”

applying a risk-based approach (RBA) toward KYC.¹²⁶ Gelb argues that the level of due diligence and incentives for KYC should be proportional to the balance of risk.¹²⁷ Balancing financial integrity and financial inclusion should be not only a domestic priority but a global one as well.¹²⁸ Striking a balance between banking requirements and customer satisfaction is always a priority.¹²⁹

Gelb also mentions using biometric systems to identify individuals and specifically uses India's Unique Identification Program as an example and explains the advantages and disadvantages of the program.¹³⁰ Gelb recommends a tiered requirement for KYC based on the various banking needs.¹³¹

The American Bankers Association's journal published an article on using augmented intelligence to assist with KYC requirements. Using augmented intelligence connects a bank's internal monitoring system with regulatory requirements.¹³² This system scans documents for possible regulation infractions and allows compliance officers to focus on specific areas.¹³³ Augmented intelligence can assist with compliance management classifications, anti-money laundering systems, and KYC compliance.¹³⁴

4. Peer-to-Peer

P2P solutions usually exchange or lend fiat or digital currency online without going through a centralized banking system. As consumers embrace the P2P marketplace,

¹²⁶ Alan Gelb, *Balancing Financial Integrity with Financial Inclusion: The Risk-Based Approach to "Know Your Customer,"* CGD Policy Paper 074 (Washington, DC: Center for Global Development, 2016), 1, <http://www.cgdev.org/sites/default/files/CGD-Policy-Paper-Gelb-KYC-Financial-Inclusion.pdf>.

¹²⁷ Gelb, 1.

¹²⁸ Courbe, *Financial Services Technology 2020 and Beyond*, 15.

¹²⁹ Wojciechowska, "What Is KYC and Why Does It Matter?"

¹³⁰ Courbe, *Financial Services Technology 2020 and Beyond*, 10.

¹³¹ Gelb, *Balancing Financial Integrity with Financial Inclusion*, 2.

¹³² Evan Sparks, "Regulatory Compliance?," *ABA Banking Journal* 109, no. 3 (June 2017): 24, <http://www.nxtbook.com/naylor/BAKS/BAKS0317/index.php#0>.

¹³³ Financial Crimes Enforcement Network, "Customer Due Diligence Requirements for Financial Institutions," *Federal Register* 81, no. 91 (May 11, 2016): 29420, 29457, <https://www.govinfo.gov/app/details/FR-2016-05-11>.

¹³⁴ Sparks, "Regulatory Compliance?," 25.

the lack of technology to identify known buyers and sellers accurately becomes difficult. These exchange platforms create another opportunity for criminals to launder money.

FinCEN advises that some new P2P exchangers fail to register as a money services business with inadequate anti-money laundering program. In 2015, FinCEN fined Ripple Labs, a P2P decentralized exchanger, \$700,000 in civil money penalties for failing to register as a money services business and violating several requirements under the BSA.¹³⁵ Furthermore, P2P exchangers act as money mixers to conceal or anonymize financial transactions further from law enforcement investigations.¹³⁶

The Financial Conduct Authority (FCA), an independent monetary regulatory body in the United Kingdom, introduces additional regulations to P2P stakeholders designed to protect investors without hindering innovation or investment opportunities.¹³⁷ The FCA is limiting P2P investment agreements for new retail customers to 10% of investable assets.¹³⁸ Several chief executives and managing directors working in the P2P lending space support the FCA ruling.¹³⁹ This regulation ensures that investors are not overexposed to undue risk during P2P lending.

On the other hand, many retail investors thought 10% was arbitrary and would reduce investment opportunities.¹⁴⁰ Also, investors portray the revelation of financial information as intrusive and distasteful. Many investors will not release their financial data, which thus hinders innovation. Likewise, treating investors differently feels

¹³⁵ “FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action against a Virtual Currency Exchanger,” Financial Crimes Enforcement Network, May 5, 2015, <https://www.fincen.gov/news/news-releases/fincen-fines-ripple-labs-inc-first-civil-enforcement-action-against-virtual>.

¹³⁶ Financial Crimes Enforcement Network, *Advisory on Illicit Activity Involving Convertible Virtual Currency* (Vienna, VA: Financial Crimes Enforcement Network, 2019), 4, <https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf>.

¹³⁷ Financial Conduct Authority, *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms: Feedback to CP 18/20 and Final Rules* (London: Financial Conduct Authority, 2019), 5, <https://www.fca.org.uk/publication/policy/ps19-14.pdf>.

¹³⁸ Financial Conduct Authority, 16.

¹³⁹ Suzie Neuwirth, “Here’s What the Industry Thinks of the FCA Rule Changes,” Here’s What the Industry Thinks, *Peer2Peer Finance News* (blog), June 4, 2019, <http://www.p2pfinancenews.co.uk/2019/06/04/heres-what-the-industry-thinks-of-the-fca-rule-changes/>.

¹⁴⁰ Financial Conduct Authority, *Loan-Based ('Peer-to-Peer')*, 6.

unethical regarding financial exclusion, fair competition, and personal freedom.¹⁴¹ Rhydian Lewis, the CEO of RateSetter, one of UK's largest P2P investment platforms, supports the regulation.¹⁴² However, he states, "The limit on savers' first investment is unnecessary and just patronizes normal people."¹⁴³ Politicians and regulators alike should carefully assess P2P platforms as another avenue to launder illicit fund.

E. CONCLUSION

In reviewing the literature, the bankers, regulators, and politicians all agree the BSA must be updated to address fintech and the various monetary reporting requirements. Terrorist financing and money launders are using innovative techniques to transfer funds while obfuscating law enforcement and intelligence services. With these new techniques for laundering money, U.S. law, specifically the BSA, must be updated to address these relevant issues. The Treasury Department, financial executives, regulators, politicians, privacy advocates, and law enforcement all have various interests and concerns regarding new regulations. Balancing these interests' groups is a daunting but important duty for the stability of the U.S. financial sector. The remainder of this thesis explores various courses of action to increase the relevancy of the BSA, while carefully considering the perspective from those impacted most.

¹⁴¹ Rhydian Lewis, "Our View on the FCA Proposals for Peer-to-Peer Lending," RateSetter, August 6, 2018, <https://www.ratesetter.com/blog/our-view-on-the-fca-proposals-for-peer-to-peer-lending>.

¹⁴² "The UK's Most Popular Peer to Peer Investment Platform," RateSetter, June 27, 2019, <https://www.ratesetter.com/about-us>.

¹⁴³ Lewis, "Our View on the FCA Proposals."

THIS PAGE INTENTIONALLY LEFT BLANK

III. LEGISLATIVE SOLUTIONS: H.R. 6068 (COUNTER TERRORISM AND ILLICIT FINANCE ACT)

This chapter discusses possible changes to the BSA as addressed in the Counter Terrorism and Illicit Finance Act. This chapter specifically focuses on the reporting requirement of the CTRs and SARs required under current law. Should these monetary requirements remain the same or should the amounts be adjusted as stated in the counter-terrorism act or should the monetary amounts be adjusted to account for inflation? The beneficiary ownership provision is also addressed along with the various arguments supporting and opposing this provision. A policy options criteria and matrix discusses several viewpoints with a detailed perspective from bank executives, law enforcement, and privacy advocates. Finally, an objective analysis addresses the monetary thresholds of the CTRs and SARs, along with the beneficiary ownership provision.

A. DESCRIPTION OF COUNTER TERRORISM AND ILLICIT FINANCE ACT

The Counter Terrorism and Illicit Finance Act is a legislative bill that alters specific monetary reporting requirements in the BSA. In June 2018, Representative Stevan Pearce introduced the Counter Terrorism and Illicit Finance Act, formally known as H.R. 6068.¹⁴⁴ This act increases the dollar amount for CTR requirements from \$10,000 to \$30,000 and allows for the sharing of suspicious activities among financial groups.¹⁴⁵ The bill also requests that the Secretary of Treasury, along with federal LE agencies, review current reporting requirements under the BSA to reduce the current regulatory burdens on financial institutions.¹⁴⁶ In overcoming these regulatory burdens, can fintech be used to assist the banking industry?

¹⁴⁴ Counter Terrorism and Illicit Finance Act, H.R. 6068, 1.

¹⁴⁵ Counter Terrorism and Illicit Finance Act, 1.

¹⁴⁶ Counter Terrorism and Illicit Finance Act, 3.

1. Goals

The Counter Terrorism and Illicit Finance Act address several current issues within the BSA. These issues include revising section Title 31 USC § 5313 from \$10,000 to \$30,000 regarding currency transactions.¹⁴⁷ Changing section Title 31 USC § 5318 (g) concerns increasing the threshold for suspicious activity reports from \$5,000 to \$10,000 and each \$2,000 amount to \$3,000.¹⁴⁸ Revising section Title 31 Code of Federal Regulations § 1010.100 (ff), which deals with money services business, such as foreign currency exchangers, check cashers, issuers of traveler’s checks or money orders, providers of prepaid access devices and money transmitters includes updating each \$1,000 threshold to \$3,000.¹⁴⁹ Streamlining the reporting requirement for CTRs and SARs, sharing suspicious activities reports within a financial group to include foreign branches, subsidiaries, and affiliates, and encouraging the use of technological innovations is another revision.¹⁵⁰ Addressing these various issues becomes complicated, especially when accounting for the stakeholders involved.

2. Advantages

The passage of the Counter Terrorism and Illicit Finance Act provides several advantages. The current regulatory standard and compliance costs associated with these regulations are harming all financial institutions, but more specifically, community banks and local broker dealers.¹⁵¹ Banks absorbing these substantial compliance costs eventually pass these monetary burdens onto their customers.¹⁵² Data obtained from the Conference of State Bank Supervisors found compliance costs fell from 2016 to 2017,

¹⁴⁷ Counter Terrorism and Illicit Finance Act, 2.

¹⁴⁸ Counter Terrorism and Illicit Finance Act, 2–3.

¹⁴⁹ Counter Terrorism and Illicit Finance Act, 3.

¹⁵⁰ Counter Terrorism and Illicit Finance Act, 1–21.

¹⁵¹ “Heritage Action Supports the Revised Counter Terrorism and Illicit Finance Act (H.R. 6068),” *Heritage Action for America* (blog), June 14, 2018, <https://heritageaction.com/press/heritage-action-supports-the-revised-counter-terrorism-and-illicit-finance-act-h-r-6068>.

¹⁵² David Baumann, “Financial Regulators Fail to Evaluate Combined Impact of Rules: GAO,” *Credit Union Times*, 1, February 27, 2018, <https://www.cutimes.com/2018/02/27/financial-regulators-fail-to-evaluate-combined-imp/>.

but only for larger banks.¹⁵³ During this same time frame, smaller community banks' compliance costs increased.¹⁵⁴ The BSA, out of all the stand-alone laws, was the most burdensome, which accounted for 22% of all compliance expenses.¹⁵⁵ Policy Director Wesley Coopersmith stated:

Rep. Pearce's improved legislation takes important steps to modernize the BSA to foster improved compliance and reduce the burden imposed on the community banks and the small broker-dealers that serve main street America. The bill does so without creating a large compliance burden on small businesses and churches that could have resulted in as many as one million inadvertent felons.¹⁵⁶

Increasing the monetary threshold of the CTA and SAR will greatly alleviate the administrative burden placed on financial institutions that are ultimately passed onto their customers.

Many legislators agree with streamlining reporting requirements to alleviate the heavy regulatory burden placed on the banking industry. On February 7, 2019, Representative Denver Riggleman introduced H.R. 1039 titled, "To streamline requirements for currency transaction reports and suspicious activity reports, and for other purposes" to the House Committee on Financial Services.¹⁵⁷ This bill requires a thorough review of the reporting requirements mandated in the BSA by the Secretary of Treasury, along with other relevant stakeholders.¹⁵⁸ The bill addresses explicitly if the CTR and SAR remain at the current monetary threshold, or are tied to inflation and periodically adjusted.¹⁵⁹ Basically, Representative Riggleman took sections 3 (Streamlining Requirements for Currency Transaction Reports and Suspicious Activity

¹⁵³ "House to Act on Bank Bill | Wells Fargo's 401(k) Practices Probed | Hayashi's Take: States Try to Protect CFPB's Investigative Power," *Wall Street Journal*, 3, April 27, 2018, <https://www.wsj.com/articles/house-to-act-on-bank-bill-wells-fargos-401-k-practices-probed-hayashis-take-states-try-to-protect-cfpbs-investigative-power-1524825203>.

¹⁵⁴ *Wall Street Journal*, 3.

¹⁵⁵ *Wall Street Journal*, 3.

¹⁵⁶ "Heritage Action Supports the Revised Counter Terrorism and Illicit Finance Act (H.R. 6068)."

¹⁵⁷ Denver Riggleman, "H.R.1039," Public Law 1039, 4 (2019), 1, <https://www.congress.gov/bill/116th-congress/house-bill/1039>.

¹⁵⁸ Riggleman, 2.

¹⁵⁹ Riggleman, 2.

Reports) and 11 (Definitions) from H.R. 6068 and re-submitted the bill under H.R. 1039 as sections 1 and 2. This new proposal discusses the need to streamline reporting. Chapter IV of this thesis, describes how fintech can assist.

3. Limitations

Raising the threshold for CTR allows illicit activity to increase even if the action is not directly associated with money laundering. The Internal Revenue Service (IRS) uses CTR data for additional audit leads while examining individuals or organization for criminal or civil violations.¹⁶⁰ From 2007–2009, the IRS generated \$13.6 million from 493 audits derived from CTRs.¹⁶¹ The IRS can also use the CTR data as an indicator of several compliance issues or uncovering businesses evading taxes.¹⁶² With the discovery of illicit activity, the IRS can use CTR data to detect and pursue individuals who would otherwise go unnoticed. Thus, keeping the current CTR requirement appears to be beneficial to the Treasury Department.

4. Beneficial Ownership Debate

Before the Counter Terrorism and Illicit Finance Act was introduced, the financial services committee stripped the beneficial ownership provision. This provision mandates that shell companies or front companies reveal their real beneficial owner, which has caused considerable debate.¹⁶³ The Heritage Action for America supports the removal of the beneficial ownership provision because it “would have unfairly imposed large compliance burdens on small businesses, charities, and religious organizations.”¹⁶⁴ Others view stripping the beneficial ownership provision as reducing the impact of detecting money laundering effectively.

¹⁶⁰ Treasury Inspector General for Tax Administration, *Currency Report Data Can Be a Good Source for Audit Leads* (Washington, DC: Department of Treasury, 2010), 2, <https://www.treasury.gov/tigta/audit-reports/2010reports/201030104fr.html#transaction>.

¹⁶¹ Treasury Inspector General for Tax Administration, 2.

¹⁶² Treasury Inspector General for Tax Administration, 2.

¹⁶³ Gershel, “Beneficial Ownership Provision Stripped.”

¹⁶⁴ “Heritage Action Supports the Revised Counter Terrorism and Illicit Finance Act (H.R. 6068).”

On one side of the debate, the Financial Accountability & Corporate Transparency (FACT) Coalition believes the beneficial ownership provision should be re-inserted into the bill. FACT “is a non-partisan alliance of more than 100 state, national, and international organizations working toward a fair tax system that addresses the challenges of a global economy and promoting policies to combat the harmful impacts of corrupt financial practices.”¹⁶⁵ FACT sent a detailed letter in June 2018 to the congressional sub-committee on Terrorism and Illicit Finance that detailed its concerns about the removal of the ownership provision.¹⁶⁶ FACT concludes that incorporation transparency is paramount to alleviate world poverty, corruption, tax evasion, arms, and human trafficking.¹⁶⁷ Confirming FACT’s assessment, OXFAM International, a global independent charitable organization, states, “The 50 biggest U.S. companies stashed \$1.6 trillion offshore in 2015, while Europe’s 20 biggest banks are registered over a quarter of their profits in tax havens—an estimated €25 billion (\$28 billion) in 2015.”¹⁶⁸ Based on these statistics, striking the beneficial ownership provision appears irresponsible.

The Department of Treasury acknowledges the importance of obtaining beneficial ownership information. In 2016, the Department of Treasury stated, “Illicit actors may well set up complex webs of shell companies or structure their ownership so as to increase the difficulty of determining the individual who in fact owns the entity; it is because of this vulnerability that legal entities are also required to provide the name of one natural person under the control prong. And while a criminal may well lie regarding a legal entity’s beneficial ownership information, verification of the identity of the natural person(s) identified as a beneficial owner will limit her ability to do so in a meaningful way such that she could avoid scrutiny entirely. Furthermore, as the Department of Justice has noted throughout this rulemaking process, a falsified beneficial ownership identification would be valuable evidence in demonstrating criminal intent. Even the verified identity of a natural person whose status as a beneficial owner has not been verified provides law enforcement and

¹⁶⁵ “About Us,” FACT Coalition, accessed April 6, 2019, <https://thefactcoalition.org/about>.

¹⁶⁶ Financial Accountability & Corporate Transparency, *RE: Discussion Draft Counter Terrorism and Illicit Finance Act* (Washington, DC: Financial Accountability & Corporate Transparency, 2018), 1, <https://thefactcoalition.org/wp-content/uploads/2019/01/INGOs-letter-on-beneficial-ownership.pdf>.

¹⁶⁷ Financial Accountability & Corporate Transparency, 1.

¹⁶⁸ OXFAM International, “Paradise Papers: The Hidden Costs of Tax Dodging,” *The Power of People against Poverty*, accessed April 6, 2019, <https://oxf.am/2zAYO0u>.

regulatory authorities with an investigatory lead from whom they can develop an understanding of the legal entity.¹⁶⁹

The Departments of Treasury and Justice both realize the implications of not disclosing the true identity of a beneficiary.

The Financial Integrity Network also supports the disclosure of beneficial owners. On November 2017, President Chip Poncy testified before the House Financial Services Committee.¹⁷⁰ Poncy demanded transparency and a systemic reporting of beneficial ownership information, along with a clear definition of the term.¹⁷¹ His arguments concur with the Treasury Department's view in harmonizing the requirements of beneficial ownership.

On the other side of the debate, the beneficial ownership provision was removed from the original bill and replaced by a requirement by the Comptroller General of the United States. The Comptroller is "to submit a report evaluating the effectiveness of the collection of beneficial ownership information under the CDD [Customer Due Diligence] rule"¹⁷² This provision was removed to give the Comptroller time to evaluate the effectiveness in collecting ownership information properly.

The American Bar Association (ABA) also agreed with the removal of the beneficial ownership provision. The ABA claims the requirement would impose a burdensome regulation on millions of small businesses.¹⁷³ Limited liability companies (LLCs) and other small corporations or their lawyers would be required to submit

¹⁶⁹ Financial Crimes Enforcement Network, "Customer Due Diligence Requirements for Financial Institutions," 29402.

¹⁷⁰ Chip Poncy, "Legislative Proposals to Counter Terrorism and Illicit Finance," § House Financial Services Committee, Financial Institutions and Consumer Credit and Terrorism and Illicit Finance Subcommittees, 1, 2017, <https://www.fdd.org/analysis/2017/11/29/legislative-proposals-to-counter-terrorism-and-illicit-finance/>.

¹⁷¹ Poncy, 24.

¹⁷² Counter Terrorism and Illicit Finance Act, H.R. 6068, 18.

¹⁷³ Harold Bass, *Joint Subcommittee Hearing on H.R. 6068, the Counter Terrorism and Illicit Finance Act and Concerns Regarding Section 9* (Chicago, IL: American Bar Association, 2017), 2, [https://www.americanbar.org/content/dam/aba/uncategorized/GAO/gatekeeperregandtheprofessiontf\(abalettertohfscfinalversionnov272017\).authcheckdam.pdf](https://www.americanbar.org/content/dam/aba/uncategorized/GAO/gatekeeperregandtheprofessiontf(abalettertohfscfinalversionnov272017).authcheckdam.pdf).

extensive information about the real owner.¹⁷⁴ The companies would also be required to update the data continuously and be subject to civil or criminal penalties for a lack of compliance.¹⁷⁵ The ABA further states this personal information could be passed along to FinCEN, federal, or foreign governmental agencies.¹⁷⁶ FinCEN would be required to maintain a secure database that could be subject to a future cyberattack that could thus disclose sensitive information about a business.¹⁷⁷ The ABA believed the provision would even weaken the current anti-money laundering tools by suspending the new CDD rule.¹⁷⁸ Based on all these drawbacks, the ABA determined that the beneficial ownership provision would be an additional regulatory burden on small businesses with minimal or no benefits.

The ABA and the Financial Integrity Network agree that defining beneficial ownership is essential for clarification among businesses, regulators, and financial institutions. They contend the term is overly broad and vague. Company formation authorities may interpret the definition of beneficial ownership differently under the CDD rule.¹⁷⁹ Whether supporting or opposing the regulation of beneficial ownership, many agree the term should be clearly defined.

B. POLICY ANALYSIS

1. Policy Options Criteria

The policy options criteria follow Eugene Bardach's steps to a practical policy options analysis. The policy options criteria consist of measuring the current \$10,000 CTR requirement that exists in the BSA.¹⁸⁰ The CTR threshold, as mentioned in the

¹⁷⁴ Bass, 1.

¹⁷⁵ Bass, 1.

¹⁷⁶ Bass, 1.

¹⁷⁷ Bass, 2.

¹⁷⁸ Bass, 2.

¹⁷⁹ Poncy, "Legislative Proposals to Counter Terrorism and Illicit Finance," 25.

¹⁸⁰ Federal Financial Institutions Examination Council, *Bank Secrecy Act/Anti-Money Laundering Examination Manual*, 64.

Counter Terrorism and Illicit Finance Act, would increase to \$30,000.¹⁸¹ Should the current regulations be adjusted for inflation? The Bureau of Labor Statistics inflation calculator shows that \$10,000 in October 1970 is equal to \$63,866 in January 2019.¹⁸² This thesis rounds the monetary requirement to \$60,000 to account for inflation. The financial threshold for SAR is \$5,000.¹⁸³ According to the Department of Labor, adjusting the \$5,000 limit for inflation equals approximately \$30,000.¹⁸⁴ Finally, the beneficial ownership provision is assessed. The matrix addresses the risk to public safety, costs to the banking industry, impact on law enforcement, and political opposition.

a. Risk to Public Safety

Measuring the threat to public safety is difficult to assess accurately. The mitigating factors associated with the CTRs and SARs can have a dramatic effect on public safety, as these requirements allow law enforcement to pursue suspicious behavior actively. Providing a statistical analysis on the results of these requirements is not currently captured accurately and can lead to the seizure of funds or arrests derived directly from a bank filing. To rate the risk, a sliding scale must be used to classify the risk in terms of general applications. A “low” in the matrix refers to the risk of reporting the transactions to FinCEN in regards to public safety. A “high” represents an increased risk to the public for failing to report illicit activity.

b. Cost to the Banking Industry

The regulatory costs for financial intuitions are a heavy burden. This unit measures the cost of filing CTR or SARs in terms of low, medium, and high. A specific dollar amount is not utilized, as the data for filing these reports vary depending on accuracy, thoroughness, and complexity.

¹⁸¹ Counter Terrorism and Illicit Finance Act, H.R. 6068, 2.

¹⁸² “CPI Inflation Calculator,” United States Department of Labor, accessed April 23, 2019, https://www.bls.gov/data/inflation_calculator.htm.

¹⁸³ Federal Financial Institutions Examination Council, *Bank Secrecy Act/Anti-Money Laundering Examination Manual*, 60.

¹⁸⁴ United States Department of Labor, “CPI Inflation Calculator.”

c. Impact on Law Enforcement

Does the current reporting requirement affect LE's ability to pursue criminals involved in financial fraud? A sliding scale from low to high is also used to rate this impact. "Low" has minimal impact on LE detection and "high" has a more significant outcome for LE operations.

d. Political Opposition

Political opposition is classified by the likelihood that elected officials will not pass the selected reporting requirement. Elected officials consider the public base, political environment, and critical stakeholders and realize that being greatly opposed does not result in a favorable vote for the enacted change in the law. The criteria for this unit of measurement are also abstract, but this area needs to be addressed for any bill's passage. "Low" represents a politically acceptable requirement. "High" represents a regulatory requirement unlikely to pass, or major outside pressures result to negate the passage.

2. Policy Options Matrix

Table 1 displays the risks to public safety, costs to the banks, the impact on law enforcement, and the level of political opposition. A sliding scale of low, medium, and high is shown for each criterion.

Table 1. Monetary Thresholds

	Risk to Public Safety	Costs to Banks	Impact on LE	Political Opposition
CTR \$10,000	Low	High	Low	High
CTR \$30,000	Medium	Medium	Medium	Medium
CTR \$60,000	Medium	Low	Medium	Low
SAR \$5,000	Low	High	Medium	Medium
SAR \$30,000	Medium	Medium	High	Medium
Beneficial Ownership Revealed	Low	Medium	Low	Medium

C. DISCUSSION

This section discusses the various major party views impacted by the legal proposal. The bank executives or bankers, law enforcement, and privacy advocates have strong opinions regarding the changes to CTRs, SARs, and the beneficial ownership provision.

1. Bank Executives

The changes to the BSA primarily affect bankers. Currently, to remain compliant, the overhead costs of training bank employees, paying salaries, and providing benefits stretch the financial burden of the banking industry. The banking executives support any relief in regards to the regulatory burden. Thus, bankers support the \$60,000 CTR and the \$30,000 SAR threshold to alleviate costs. Clarification within the BSA reveals beneficial ownership will add to the regulatory burden on the banking industry. The Federal Financial Institutions Examination Council (FFIEC) provides guidance, standards, and uniformity regarding the due diligence of obtaining the beneficiary owner of a

company.¹⁸⁵ Even so, FinCEN and law enforcement prefer a strict definition, regulatory enforcement, and specific fines placed within the BSA for clarification.

2. Law Enforcement

Law enforcement prefers access to CTRs and SARs without going through the judicial process of obtaining subpoenas or search warrants. Law enforcement is not attempting to circumvent the legal process or abuse individual privacy, but with the rapid and increase movement of illicit funds, following the legal process becomes an administrative burden. The legal process slows the investigative process and reduces the likelihood of seizing money. The movement of money continues to accelerate with fintech, and by the time law enforcement follows the legal process, the funds have already changed financial institutions or been moved internationally. Thus, law enforcement supports the lower threshold requirements associated with CTRs and SARs. The higher thresholds allow money launderers to go undetected, which leads to the retrieval of stolen funds as highly unlikely. FinCEN and law enforcement also support the beneficial ownership provision in the BSA. This provision enables FinCEN to trace money used for terrorist financing effectively and reveal the rightful owner of the funds.

3. Privacy Advocates

Privacy advocates align more with the banking industry than law enforcement, but for different reasons. Privacy activists believe the judicial process is circumvented when law enforcement receives information directly from the financial institutions. The legal process provides a check and balance, so that law enforcement does not overstep its enforcement boundaries or abuse its authority. Thus, the advocates support a lower threshold of CTR and SARS and have admittedly opposed increasing the monetary limit since the inception of the law. Furthermore, privacy advocates also believe the beneficial ownership provision should not be added to the BSA. They supported the successful

¹⁸⁵ Federal Financial Institutions Examination Council, *Beneficial Ownership Requirements for Legal Entity Customers—Overview* (Washington, DC: Federal Financial Institutions Examination Council, 2018), 1–9, <https://www.ffiec.gov/press/pdf/Beneficial%20Ownership%20Requirements%20for%20Legal%20Entity%20CustomersOverview-FINAL.pdf>.

removal of the beneficial ownership from the Counter Terrorism and Illicit Finance Act, which caused an outcry among law enforcement.

D. ANALYSIS

All three fractions provide legitimate concerns regarding the various monetary thresholds and the beneficial ownership provision. With the significant movement of funds without accounting for inflation, the banking industry incurs an enormous financial burden that needs to be alleviated. Law enforcement also has a legitimate concern, as the increase in reporting thresholds and fintech allow criminals to move money without detection and obfuscate law enforcement authorities.

Increasing the CTR requirement benefits the banking industry, and privacy advocates support a less restrictive requirement. On the other hand, this increase provides minimal benefit to LE efforts. Of note, a majority of the CTRs is actually legitimate and law enforcement can always utilize the legal process to obtain evidence.

Changing the SAR requirement seems irresponsible in detecting the flow of illicit money, as internal bank investigators need a legal avenue and framework for reporting these activities. Bank investigators should report suspicious activity to FinCEN without concern for the monetary threshold. Financial schemes continue to increase, and the banking industry is the primary source of detecting and reporting these activities. As law enforcement continues to use the legal process, it is often hindered by the lack of insight into suspicious activity. Therefore, law enforcement cannot apply the legal process, and increasing the threshold will significantly hinder criminal investigations.

The privacy advocates make a valid argument based on law enforcement bypassing the legal process. On the other hand, the risk needs to be weighted between circumventing the legal process and allowing criminals to move funds without any deterrent of being arrested. Bank investigators realize suspicious activity is ongoing, and they need a legal mechanism to report this activity without repercussions from privacy groups, customers, or other legal action.

Regarding the beneficial ownership provisions, bank executives realize the initial upfront administrative costs are burdensome, but once the account, loan, or acquisition is set up, overhead costs are minimal. Revealing the beneficiary owner allows law enforcement more opportunities to trace and detect illicit funds and work more effectively with international LE partners. The ABA provides a legitimate but feeble argument about the regulatory burden on millions of small businesses.¹⁸⁶ The ABA offers no statistical evidence regarding the “millions” of small businesses. Once the financial accounts are established, and the beneficiary owner is revealed, the regulatory burden is minimal unless ownership is changed.

The next chapter addresses specific fintech that banks can utilize to detect money laundering, tax evasion, terrorist financing, and other financial crimes, as well as how criminals use fintech to move illicit funds.

¹⁸⁶ Bass, *Joint Subcommittee Hearing on H.R. 6068*, 2.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. FINANCIAL TECHNOLOGY

A. OVERVIEW OF FINANCIAL TECHNOLOGY

Financial technology has been used prolifically over the last decade, so much so that the term financial technology has been shortened to fintech. Fintech uses software and modern technology to provide specific solutions within the financial services sector.¹⁸⁷ Currently, the BSA does not adequately address this advanced technology. This chapter begins with a definition and description of ML technology and the ability to detect suspicious activity by financial institutions. This section includes the advantages and disadvantages of this technology and a discussion of whether it should be mandated within the BSA.

The following section focuses on digital currency and the impact the digital currency market is having throughout the financial sector. Should digital currency have stricter regulations based on criminals using this currency to transfer funds to avoid detection? The following section also addresses “KYC,” as well as can the fintech industry assist with identifying your customer.

The final section in the chapter addresses P2P payment systems and their ability to move illicit funds. The chapter concludes with a policy-option criterion and a matrix discussing the options discussed in this chapter.

1. Machine Learning

Fraud detection is an ongoing and challenging problem for financial institutions. Only 50% of money laundering or terrorist financing was detected by internal currency alerts.¹⁸⁸ The banking industry also has difficulty hiring experienced staff to detect or comply with AML regulations.¹⁸⁹ With these two significant issues, this section focuses on fintech called ML to address these concerns. The technological advances of ML can

¹⁸⁷ “FinTech Definition,” FinTech Weekly Definition, 2017, <https://www.fintechweekly.com/fintech-definition>.

¹⁸⁸ White, Anderson, and Lavion, *Adjusting the Lens on Economic Crime*, 42.

¹⁸⁹ White, Anderson, and Lavion, 42.

process large amounts of data to detect fraudulent activity that thus assists financial institutions. Like most technical words, ML is defined differently by the various sectors using the technology. It is understood to be a subset of AI that processes massive amounts of data leading to a decision in milliseconds.¹⁹⁰ In the financial sector, “machine learning is trained to recognize normal transactions within the data and then identify all deviations and anomalies in real-time.”¹⁹¹ A ML system receives a large data source and cleans the data or removes any data irrelevant to the end goal.¹⁹² Scientists then analyze the data to ensure that enough target attributes exist.¹⁹³ If so, the data scientist selects measurable characteristics in the ML model, while testing and evaluating the accuracy of the guiding algorithm.¹⁹⁴ Using this relatively new technology, financial institutions can detect suspicious activity instead of paying a traditional analyst.

A subsection of artificial intelligence, ML, is broken down further into two major categories, supervised and unsupervised models.¹⁹⁵ Supervised ML models are the most common in the financial sector.¹⁹⁶ A data scientist feeds information into the model and tags the transaction as either legitimate or fraudulent behavior.¹⁹⁷ Over time, the machine correlates the data with individual behavior.¹⁹⁸ As more training data is fed into the machine, the more accurate the model becomes.¹⁹⁹ Unsupervised ML is more

¹⁹⁰ Mercator Advisory Group, Inc., *Fraud Detection 2.0: Dynamic Tools for Fighting E-Commerce Fraud*, 4.

¹⁹¹ Mercator Advisory Group, Inc., 5.

¹⁹² Feedzai, *The Dawn of Machine Learning for Banking and Payments* (San Mateo, CA: Feedzai, 2017), 13, <https://feedzai.com/wp-content/uploads/2017/08/Dawn-of-Machine-Learning-041317a.pdf>.

¹⁹³ Feedzai, 13.

¹⁹⁴ Feedzai, 14.

¹⁹⁵ Dahee Choi and Kyungho Lee, *An Artificial Intelligence Approach to Financial Fraud Detection under IoT Environment: A Survey and Implementation* (Seoul, Republic of Korea: Kindawi, 2018), 3, <https://doi.org/10.1155/2018/5483472>.

¹⁹⁶ Jason Brownlee, “Supervised and Unsupervised Machine Learning Algorithms,” *Machine Learning Mastery* (blog), March 15, 2016, <https://machinelearningmastery.com/supervised-and-unsupervised-machine-learning-algorithms/>.

¹⁹⁷ Choi and Lee, *An Artificial Intelligence Approach to Financial Fraud Detection*, 3.

¹⁹⁸ TJ Horan, “5 Keys to Using AI and Machine Learning in Fraud Detection,” July 3, 2018, <http://www.fico.com/en/blogs/analytics-optimization/5-keys-to-using-ai-and-machine-learning-in-fraud-detection/>.

¹⁹⁹ Horan.

complicated. Unlike supervised machines, the data entered into an unsupervised model is not labeled or categorized as legitimate or fraudulent activity.²⁰⁰ The network learns normal behaviors, consistencies, and trends from the data.²⁰¹ The machine then issues alerts about any anomalies falling outside the given parameters.²⁰² The anomalies or outliers are categorized as suspicious or fraudulent activity. A troubling concern is only half of the identified suspicious activity are currently being detected by current monitoring systems.²⁰³ Financial institutions can utilize either supervised or unsupervised ML to detect suspicious activity more efficiently.

a. Advantages

As stated previously, using ML technology provides several advantages. ML can be used to detect a variety of suspicious activities and abnormal behavioral patterns.²⁰⁴ Individuals from the University of British Columbia, Amazon AI, and Yahoo Research even believe ML can effectively predict legitimate accounts that may be more susceptible to suspicious activities in the future.²⁰⁵ Various private sector solutions are also available, such as Verafin, which use technology to monitor transactions across several channels to uncover criminal activity or possible terrorist financing.²⁰⁶ ML can identify trends or abnormal behavior quicker than those typically going undetected by rule-based traditional

²⁰⁰ Jason Brownlee, “Supervised and Unsupervised Machine Learning Algorithms,” *Machine Learning Mastery* (blog), March 15, 2016, <https://machinelearningmastery.com/supervised-and-unsupervised-machine-learning-algorithms/>.

²⁰¹ Martin Renstrom and Timothy Holmsten, *Fraud Detection on Unlabeled Data with Unsupervised Machine Learning* (Stockholm, Sweden: Examensarbete Inom Datateknik, 2018), 8, <http://kth.diva-portal.org/smash/get/diva2:1217521/FULLTEXT01.pdf>.

²⁰² Remi Domingues, “Machine Learning for Unsupervised Fraud Detection” (master’s thesis, KTH, Sweden, INSA Lyon, 2015), 5, <http://www.diva-portal.org/smash/get/diva2:897808/FULLTEXT01.pdf>.

²⁰³ White, Anderson, and Lavion, *Adjusting the Lens on Economic Crime*, 50.

²⁰⁴ Hassan Halawa et al., “Forecasting Suspicious Account Activity at Large-Scale Online Service Providers,” *ArXiv:1801.08629 [Cs]*, 1, January 25, 2018, <http://arxiv.org/abs/1801.08629>.

²⁰⁵ Halawa et al., 1–10.

²⁰⁶ “Money Laundering Detection: Flow of Funds, Structuring, Funnel Accounts,” Verafin, accessed April 25, 2019, <https://verafin.com/solution/money-laundering-detection/>.

detection methods.²⁰⁷ Over time, humans become complacent, bored, or just lazy. On the other hand, machines improve with efficiency and accuracy, which leads to detecting illegal activity better, and thus saving banks and customers money.

b. Challenges

ML technology is constantly evolving and far from perfect. The technology has a steep learning curve, and the amount of time and data needed to create an effective model is beyond the investment of many banking risk teams.²⁰⁸ Though ML can detect abnormal activity, it does not always discover suspicious behaviors and can produce false-positive results. It can reduce the number of staff hours required to authenticate a transaction; however, only human intelligence can review the data to determine a legitimate or suspicious transaction. ML solutions rely on highly skilled and well-trained data scientists working together as a team.²⁰⁹ The team continuously adjusts the controlling algorithm to reduce the number of false-positives.²¹⁰ Detecting suspicious activity and reducing the number of false-positives is a constant issue with this fintech.

Unsupervised ML can lead to additional issues for bank executives. As unsupervised machines detect false-positive transactions, the controlling algorithm identifies the transaction as fraudulent.²¹¹ However, problems arise as the transaction is actually authentic and the machine continues to learn incorrectly, which creates additional false-positives.²¹² This type of learning reinforces a deficient decision matrix, and can quickly lead to multiple false-positives if the model is not resolved soon.²¹³ Bank

²⁰⁷ Zhiyuan Chen et al., “Machine Learning Techniques for Anti-Money Laundering (AML) Solutions in Suspicious Transaction Detection, A Review,” *Knowledge and Information Systems* 57, no. 2 (November 2018): 246, <https://doi.org/10.1007/s10115-017-1144-z>.

²⁰⁸ First Data Corporation, *Machine Learning, Security and the Future of Fraud*, 8.

²⁰⁹ Feedzai, *Operationalizing Machine Learning for Fraud* (San Mateo, CA: Feedzai, 2017), 5, <https://feedzai.com/wp-content/uploads/2017/09/Operationalizing-Machine-Learning-For-Fraud-v107.pdf>.

²¹⁰ Chen et al., “Machine Learning Techniques,” 247.

²¹¹ Ravelin Technology Ltd., *The Complete Guide to Machine Learning and Fraud Prevention* (London, New York: Ravelin Technology Ltd., 2017), 5, <https://cdn2.hubspot.net/hubfs/2322855/Machine%20learning/The%20Complete%20Guide%20to%20Machine%20Learning%20and%20Fraud%20Prevention.pdf>.

²¹² Ravelin Technology Ltd., 5.

²¹³ Ravelin Technology Ltd., 5.

executives need to be aware of these issues with unsupervised ML to maintain customer satisfaction if the controlling algorithm goes awry.

ML solutions require constant feedback and programming by data science teams to both maintain consistent results and improve performance. Data scientists need to master several types of programming, or a company must employ an entire data science team.²¹⁴ Using a complete data scientist team to ensure enhanced performance of the technology can be extremely costly for smaller financial institutions.

Another ML limitation is called “black box decision making.” Data is processed through an intricate machine, and the algorithm declares the transactions suspicious without any knowledge of its internal working.²¹⁵ Policy makers at financial institutions need to understand why specific transactions or accounts are reported as suspicious. Banking executives cannot see behind a sophisticated algorithm or propriety information if machines are declaring accounts suspicious.

ML can be extremely costly to purchase, and implementing a sophisticated data-analytical platform to detect suspicious activity can be complicated. Unfortunately, the cost to implement and maintain these systems is beyond the financial capability of community or smaller banks.

2. Digital Currency

Digital currency and virtual currency are usually used conjointly throughout the tech industry, even though they have minor differences. For this thesis, the definition of digital currency is defined as in H.R. bill 56. The bill defines digital currency as a “digital representation of value that is used as a medium of exchange, unit of account, or stored value; and is not an established legal tender.”²¹⁶ Virtual currency was referred to as currency that could not buy a real commodity. Thus, currency in a video game is referred

²¹⁴ First Data Corporation, *Machine Learning, Security and the Future of Fraud*, 8.

²¹⁵ Guidotti et al., “A Survey of Methods for Explaining Black Box Models.”

²¹⁶ Ted Budd, “H.R.56—Financial Technology Protection Act,” Public Law 56, 12 (2019): 11, <https://www.congress.gov/bill/116th-congress/house-bill/56/text>.

to as virtual currency. Once a virtual currency could buy and sell goods, it became known as a digital currency.

The San Francisco U.S. Attorney’s Digital Currency task force agreed with the digital currency definition and never used the word virtual currency, since it would never prosecute virtual currency crimes. The digital currency task force referred to digital currency as intangible but considered it real money even though it was not backed by fiat. Still, the U.S. Attorney’s offices and FinCEN use the terms digital and virtual currency interchangeably.

When people think of digital currency, Bitcoin comes to everyone’s mind. Bitcoin has the largest market capitalization of any decentralized digital currency.²¹⁷ Bitcoin is the first decentralized digital payment system. An individual known as Satoshi Namato invented Bitcoin.²¹⁸ Bitcoin operates using blockchain technology and records all transactions on a public distributed ledger. People who own Bitcoin have a private key, which is similar to any private financial account password or personal identification number. This unique key allows them to sell or transfer their Bitcoin to a new owner, and the transaction is then recorded on the public ledger. Since no centralized authority exists, such as the Federal Reserve Bank, the digital currency uses “miners.” These computer enthusiasts maintain the public ledger, verify each transaction, and reconcile the ledger continuously.²¹⁹ Even though Bitcoin is the most widely circulated digital currency, many other digital currencies are available, such as Ethereum, Ripple, Litecoin, and Monero, to name a few. The concept of having a decentralized payment system is very enticing to several citizens and entities.

a. Advantages

The uniqueness of Bitcoin or any digital currency is the owner does not rely on a third-party service like the federal banking system or a private company like PayPal or

²¹⁷ Frentzen and Haun, “US vs BTC-E,” 3.

²¹⁸ Jerry Brito and Andrea Castillo, *Bitcoin: A Primer for Policymakers*, vol. 29 (Arlington, VA: Mercatus Center, 2013), 3, https://www.mercatus.org/system/files/Brito_BitcoinPrimer.pdf.

²¹⁹ NACHA, *Faster Payments Tracker* (Boston, MA: PYMNTS.COM, 2016), 2, <https://web.nacha.org/system/files/resource/2017-08/NACHA-Faster-Payments-Tracker-FEB.pdf>.

Visa to move the funds. Digital currency can quickly move from P2P without oversight or regulation by a financial institution or the U.S. government. Digital currency is also not backed by gold, government fiat, or the U.S. government. People on the open market determine the value of digital currency, much like with stock prices.²²⁰ This movement of funds becomes enticing for citizens with the ideology that favors less or no government intervention or oversight.

Since no centralized banking authority authorizes the movement of digital currency, the transactions are significantly cheaper. U.S. traditional payment systems require customers or merchants to pay a transaction fee to complete the transactions. Processing several thousand transactions daily can become expensive for businesses, and the corporation must account for this additional overhead cost.

The movement of digital currency is quicker compared to the automated clearing house (ACH) of financial institutions. The ACH is an electronic funds clearing and settlement system that facilitates payments between consumers, businesses, and governments that clears \$2 trillion daily.²²¹ The “miners” of digital currency and the ACH perform similar functions.²²² The National Automated Clearing House Association (NACHA) operates the ACH, with future plans for same-day ACH processing in 2021.²²³ The NACHA is attempting to enhance its speed of processing transactions to compete with digital currency and increase customer satisfaction. Digital currency exchangers are usually slowed down when transferring funds from a fiat source to a digital currency based on the delay with ACH processing.²²⁴ One of the benefits of digital currency is the processing speed of transactions.

²²⁰ Brito and Castillo, *Bitcoin: A Primer for Policymakers*, 29:4.

²²¹ “ACH,” The Clearing House, accessed April 29, 2019, <https://www.theclearinghouse.org/payment-systems/ach>.

²²² NACHA, *Faster Payments Tracker*, 1–13.

²²³ “Expanding Same Day ACH,” NACHA, accessed April 29, 2019, <https://www.nacha.org/rules/expanding-same-day-ach>.

²²⁴ “Why Does a Buy Take so Long?,” Coinbase, accessed April 29, 2019, <https://support.coinbase.com/customer/portal/articles/1392022-why-does-a-buy-take-so-long->.

Digital currency also protects citizens and ensures financial privacy from repressive governments. Oppressed individuals benefit significantly from the ability to make private transactions to avoid scrutiny or oppression from a tyrannical government.²²⁵ Many Argentina citizens are moving toward digital currency to circumvent the high foreign exchange rate imposed by the government.²²⁶ Another reason Argentines are using digital currency is to remain anonymous and the privacy for holding U.S. dollars overseas without the knowledge of Argentinian regulators.²²⁷ Globally, Argentina is not considered an oppressive government, but its citizens now have the option to ensure financial privacy from what they deem to be an oppressive oversight.

b. Law Enforcement Concerns

Despite the numerous benefits of digital currency, some significant drawbacks remain. Digital currency has become an increasing concern for law enforcement and policymakers over the past decade. Criminals use digital currency to launder money and accept payment for illicit goods to remain anonymous and avoid LE detection. A few examples of illegal online marketplaces using digital currency in nefarious ways follow.

- Silk Road, which operated on the Tor network from 2011–2013, “emerged as the most sophisticated and extensive criminal marketplace on the Internet, at the time.”²²⁸ It served, “as a sprawling black-market bazaar where unlawful goods and services... were bought and sold regularly” using the digital currency Bitcoin.²²⁹ “Silk Road was used by thousands of drug dealers and other unlawful vendors to distribute hundreds of

²²⁵ Brito and Castillo, *Bitcoin: A Primer for Policymakers*, 29:15.

²²⁶ Zoe Thomas, “Bitcoin Becoming Argentina’s Fx Alternative,” *International Financial Law Review*, 1, August 13, 2015, <https://www.iflr.com/Article/3479503/Bitcoin-becoming-Argentinas-FX-alternative.html?ArticleId=3479503>.

²²⁷ Thomas, 1.

²²⁸ “Manhattan U.S. Attorney Announces Extradition of Senior Adviser to the Operator of the ‘Silk Road’ Website,” United States Attorney’s Office, June 15, 2018, <https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-extradition-senior-adviser-operator-silk-road-website>.

²²⁹ “Ross Ulbricht, The Creator and Owner of the ‘Silk Road’ Website, Found Guilty in Manhattan Federal Court on All Counts,” United States Attorney’s Office, May 13, 2015, <https://www.justice.gov/usao-sdny/pr/ross-ulbricht-creator-and-owner-silk-road-website-found-guilty-manhattan-federal-court>.

kilograms of illegal drug dealers and other unlawful services to well over 100,000 buyers, and launder hundreds of millions of dollars” using Bitcoin to remain anonymous.²³⁰ The owner of Silk Road earned a commission valued over \$13 million from illegal online sales.²³¹ Eventually, LE authorities seized millions of dollars in Bitcoin.²³² The proceeds obtained from selling illegal goods online are so lucrative that one month after Silk Road was shut down by law enforcement, its predecessor, Silk Road 2.0, was operating.²³³

- In July 2017, LE authorities seized the “largest criminal marketplace on the Internet, AlphaBay, which operated for over two years on the dark web.”²³⁴ The bazaar sold malware, hacking tools, counterfeit goods, fentanyl, heroin, other toxic chemicals, and firearms.²³⁵ During the final days of operation, it had over 350,000 unlawful listings with 40,000 vendors.²³⁶ Digital currency was the method of exchange for goods and services, and millions of dollars in digital currency were seized.²³⁷ Chief Don Forst of the IRS stated, “AlphaBay was the world’s largest underground marketplace of the dark net, providing an avenue for criminals to conduct business anonymously and without repercussions.”²³⁸
- According to Jeffrey Simser, the legal director at Ministry of the Attorney General for Canada, “Liberty Reserve allowed anonymous transfers

²³⁰ United States Attorney’s Office, “Manhattan U.S. Attorney Announces Extradition.”

²³¹ United States Attorney’s Office, “Ross Ulbricht, The Creator and Owner.”

²³² United States Attorney’s Office.

²³³ “Operator of ‘Silk Road 2.0’ Website Charged in Manhattan Federal Court,” United States Attorney’s Office, May 13, 2015, <https://www.justice.gov/usao-sdny/pr/operator-silk-road-20-website-charged-manhattan-federal-court>.

²³⁴ “AlphaBay, the Largest Online ‘Dark Market,’ Shut Down,” United States Attorney’s Office, July 20, 2017, <https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down>.

²³⁵ United States Attorney’s Office.

²³⁶ United States Attorney’s Office.

²³⁷ United States Attorney’s Office.

²³⁸ United States Attorney’s Office.

around the world, operating like a virtual currency; when disrupted, there were 1 million users worldwide (200,000 in the USA) conducting 12 million transactions annually.”²³⁹ The founder Arthur Budovsky developed “the largest payment processor and money transfer system” according to the defunct website.²⁴⁰ The purpose was to allow anonymous and untraceable illegal transactions to launder money globally using digital currency. Assistant Attorney General Caldwell stated the following after a guilty plea, “After a Prior conviction for operating an unlicensed money transmitting business, Budovsky developed Liberty Reserve, which quickly became a premier service used by criminals around the world to launder their criminal proceeds.”²⁴¹ All together prosecutors alleged the company laundering approximately \$6 billion even though he pleaded to \$250 million.²⁴²

- BTC-e, another enormous digital currency exchanger operated globally from 2011 to 2017.²⁴³ The internet-based money transmitter exchanges fiat currency with several digital currencies.²⁴⁴ The operator defendant, Alexander Vinnik, is charged in the Northern District of California for operating an international money-laundering scheme using digital currency.²⁴⁵ BTC-e conducted approximately \$296 million in Bitcoin

²³⁹ Simser, “Bitcoin and Modern Alchemy,” 162.

²⁴⁰ “Founder of Liberty Reserve Pleads Guilty to Laundering more than \$250 Million through His Digital Currency Business,” United States Attorney’s Office, January 29, 2016, <https://www.justice.gov/opa/pr/founder-liberty-reserve-pleads-guilty-laundering-more-250-million-through-his-digital>.

²⁴¹ United States Attorney’s Office.

²⁴² Frentzen and Haun, “US vs BTC-E,” 6.

²⁴³ Frentzen and Haun, 5.

²⁴⁴ “FinCEN Fines BTC-e Virtual Currency Exchange \$110 Million for Facilitating Ransomware, Dark Net Drug Sales,” Financial Crimes Enforcement Network, July 27, 2017, <https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware>.

²⁴⁵ United States Attorney’s Office, “Russian National and Bitcoin Exchange Charged in 21-Count Indictment for Operating Alleged International Money Laundering Scheme and Allegedly Laundering Funds from Hack of Mt. Gox,” Department of Justice, July 26, 2017, <https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged>.

transactions, and over 300,000 were traceable to theft.²⁴⁶ During the operation, BTC-e had no “KYC” processes or internal policy in place and failed to collect customer data.²⁴⁷

As stated by these examples, criminals or money launderers utilize digital currency to conceal the origin of illegally obtained funds and avoid LE detection. Tracing the funding streaming from criminal organizations has always been an avenue for law enforcement to investigate. This tracking has now become more difficult and resource intensive with digital currency. Criminals have taken a step further with digital currency to conceal their nefarious activities. Perpetrators are now using mixers or tumblers to hide activity further. A tumbler is a service that mixes several transactions, which thus makes tracing impossible once the currency is intertwined with other funds.²⁴⁸ Bitcoin Blender touts a function to blend or mix digital currency to make the transaction 100% anonymous.²⁴⁹ This technology allows criminals to use another avenue to conceal their activities.

During a digital currency conference hosted by the Department of Justice in November 2015, FinCEN Director Jennifer Shasky Calvery stated:

FinCEN was the first regulator to address virtual currency. But we only opened the door for the hundreds of other questions beyond our anti-money laundering perspectives. It is vitally important that government regulators and law enforcement agencies engage with leaders of the virtual [digital] currency sector to make sure we understand each other.²⁵⁰

²⁴⁶ Financial Crimes Enforcement Network, “FinCEN Fines BTC-e,” 2.

²⁴⁷ Frentzen and Haun, “US vs BTC-E,” 9.

²⁴⁸ Corinne Ramey, “The Crypto Crime Wave Is Here; from Stickups and Drug Deals to White-Collar Scams, Cryptocurrency-Related Crime Is Soaring—and Law Enforcement Is Scrambling to Keep Up,” *Wall Street Journal*, 4, April 26, 2018, <https://www.wsj.com/articles/the-crypto-crime-wave-is-here-1524753366>.

²⁴⁹ Anonymous, “Bitcoin Blender,” Bitcoin Blender, accessed May 1, 2019, <https://bitblender.io/index.html>.

²⁵⁰ “Justice Department Convenes Summit on Digital Currency and the Blockchain,” United States Attorney’s Office, November 16, 2015, <https://www.justice.gov/usao-ndca/pr/justice-department-convenes-summit-digital-currency-and-blockchain>.

Acting U.S. Attorney Brian Stretch echoed Calvery’s response during a keynote address stating, “As emerging technologies such as digital currency and block chains expand into new and legitimate applications, it becomes all the more critical for industry leaders and government agencies to share insights and perspectives in order to combat the illicit use of these technologies.”²⁵¹ Thus, the BSA needs to address the regulation of digital currency.

Based on the expanding use of digital currency, the U.S. Attorney’s Office in San Francisco created the first Digital Currency Task Force consisting of the U.S. Secret Service, Homeland Security Investigations, the Internal Revenue Service, the Federal Bureau of Investigations, the Drug Enforcement Agency, and local law enforcement partners to combat the illicit use of digital currency.²⁵² This task force focuses on criminals using digital currency to launder funds and addresses this growing threat landscape.

Much confusion has occurred over the years, and clarification has been needed to address digital currency. On March 18, 2013, FinCEN issued this interpretive guide:

to clarify the applicability of the regulations implementing the Bank Secrecy Act (“BSA”) to persons creating, obtaining, distributing, exchanging, accepting, or transmitting virtual currencies. Such persons are referred to in this guidance as “users,” “administrators,” and “exchangers,” all as defined below. A user of virtual currency is not an MSB under FinCEN’s regulations and therefore is not subject to MSB registration, reporting, and recordkeeping regulations. However, an administrator or exchanger is an MSB under FinCEN’s regulations, specifically, a money transmitter, unless a limitation to or exemption from the definition applies to the person. An administrator or exchanger is not a provider or seller of prepaid access, or a dealer in foreign exchange, under FinCEN’s regulations.²⁵³

²⁵¹ United States Attorney’s Office.

²⁵² United States Attorney’s Office.

²⁵³ “Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies,” Financial Crimes Enforcement Network, March 2013, <https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering>.

FinCEN provided further regulations from users engaged in “mining” bitcoin. According to FinCEN, miners are not subject to AML oversight.²⁵⁴ On the other hand, “those who mine Bitcoins and sell them to someone else are subjected to AML oversight as money transmitters.”²⁵⁵ The lines between a user, administrator, and exchanger can become blurred depending on an individual’s point of view. Digital currency needs to be updated in the BSA to provide clear guidance for miners, administrators, exchanger, regulators, policymakers, and law enforcement.

Foreign law enforcement is also having difficulty with digital currency. The National Crime Agency (NCA) from the United Kingdom claims the money is being used to launder smaller amounts, but at high volumes.²⁵⁶ The NCA has made three observations.²⁵⁷ First, digital currency is used in extortion-type crimes like ransomware in which victims pay cybercriminals.²⁵⁸ Second, it aids the growth of cybercrime-related services.²⁵⁹ Criminals use digital currency to exchange illicit tools or goods among different crime families.²⁶⁰ Lastly, digital currency is used to launder money throughout cybercriminal networks.²⁶¹ The NCA is expecting the use of digital currency to grow as the need to cash-out or change digital currency to a fiat currency increases.²⁶² The growing concern of using digital currency is a continual issue throughout international law enforcement.

²⁵⁴ Brito and Castillo, *Bitcoin: A Primer for Policymakers*, 29:162.

²⁵⁵ Simser, “Bitcoin and Modern Alchemy,” 162.

²⁵⁶ Stephen Barclay and Ben Wallace, *National Risk Assessment of Money Laundering and Terrorist Financing 2017* (New York: Crown, 2017), 40, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf.

²⁵⁷ Barclay and Wallace, 40.

²⁵⁸ Barclay and Wallace, 40.

²⁵⁹ Barclay and Wallace, 40.

²⁶⁰ Barclay and Wallace, 40.

²⁶¹ Barclay and Wallace, 40.

²⁶² Barclay and Wallace, 40.

3. Know Your Customer Using Technology

KYC has become a common term within the banking industry. KYC is often referred to as CIP, as mentioned in the USA PATRIOT Act under Section 326.²⁶³ This section allowed the Secretary of the Treasury to set forth regulations on bankers regarding the identification of customers opening new accounts.²⁶⁴ The customer identification program or the term used now as KYC was purposely left vague to allow the banking industry flexibility in implementing this requirement.²⁶⁵ The KYC portions of the USA Patriot Act were used to verify new customers and not focus on longtime loyal customers.²⁶⁶ With the development of fintech, now KYC can be explored in a new realm that balances customer satisfaction with compliance.

With the development of new technology, individuals can open bank accounts and transfer money without appearing at a local bank. This same technology allows criminals to move illicit money throughout the financial system while providing limited identification to banks. Appropriate KYC rules governing financial institutions are crucial in maintaining financial integrity to identify the source of money.²⁶⁷ The BSA needs to provide banks with a minimum standard for a client to open an account. These rules should ensure consistency among local and national banks, while carefully considering the implications of international banking. Within those standards, the KYC rules should not hinder innovation or cause undue friction in setting up an account. In this day and age, customers request a proper balance between convenience and usability.

Three primary steps are followed to identify customers when dealing with KYC rules. First, the information must be collected. Second, the institutions need to verify the data, and lastly, the information should be authenticated through a government database or a trusted third party. KYC must be dynamic and continuously authenticating

²⁶³ USA PATRIOT ACT, 317.

²⁶⁴ USA PATRIOT ACT, 317.

²⁶⁵ Cocheo, "Flexible Patriot Rules," 52.

²⁶⁶ Cocheo, 54.

²⁶⁷ Federal Financial Institutions Examination Council, *Bank Secrecy Act/Anti-Money Laundering Examination Manual*, 3.

transactions and detecting suspicious activity.²⁶⁸ Particular focus should be on businesses conducting transactions with insufficient AML regulations.²⁶⁹ Being able to analyze transfers between two accounts should be a requirement under the KYC rule.²⁷⁰ All these steps need to be implemented appropriately for strict KYC rules to be effective. In addition, various methods are available for collecting, verifying, and authenticating information.

The financial cost for increasing regulations as mentioned previously should also be addressed when dealing with KYC regulations. According to a Thomson Reuters survey, “the costs and complexity of KYC are rising.”²⁷¹ Financial firms are spending millions of dollars in KYC compliance, and some larger financial institutions are spending \$500 million on compliance costs.²⁷² Financial institutions may increase KYC compliance and reduce overhead costs by using fintech.

a. Biometrics

KYC can also use biometrics to include fingerprint, retina, facial, finger vein recognition. Two major issues have been identified with using biometrics. The “false acceptance of an invalid identity claim (possibly fraud)” and the “false rejection of a valid identity claim (unwarranted denial of service).”²⁷³ Another issue is the failure to capture a biometric because of a software or hardware failure.²⁷⁴ Costs, system performance, reliability, and convenience are concerns in using this technology. However, biometrics could be a beneficial avenue as a KYC initiative as technology continues to develop and accessibility increases.

²⁶⁸ White, Anderson, and Lavion, *Adjusting the Lens on Economic Crime*, 49.

²⁶⁹ White, Anderson, and Lavion, 49.

²⁷⁰ Gelb, *Balancing Financial Integrity with Financial Inclusion*, 5.

²⁷¹ “Thomson Reuters 2016 Know Your Customer Surveys Reveal Escalating Costs and Complexity,” Thomson Reuters, May 9, 2016, <https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html>.

²⁷² Thomson Reuters.

²⁷³ Gelb, *Balancing Financial Integrity with Financial Inclusion*, 3.

²⁷⁴ Gelb, 3.

b. *Distributed Ledger Technology*

In 2017, two researchers wrote a paper on distributed ledger technology (DLT) to assist with KYC due diligence and reduce the cost of compliance within the banking industry. The researchers explained that customers or businesses would only go through the verification process with one financial institution.²⁷⁵ The verification data would then be added to a decentralized interbank ledger to allow any financial institution to obtain the data and reduce the duplication process of KYC.²⁷⁶ The ledger would act as a single point of verification and authentication for other banks, much like blockchain technology with digital currency.²⁷⁷ DLT technology has future potential, but financial institutions need to conduct further testing.

c. *Tiered KYC Requirement—Risk Based Approach*

In dealing with the KYC requirement, the level of due diligence by the banks should be proportional to the amount of risk. With the advancement of technology, banks can use fintech to assist with a tiered or risk-based approach. The Financial Crimes Task Force (FCTF) is an “inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.”²⁷⁸ The FCTF recommends a risk-based approach to mitigate money laundering with high-risk countries.²⁷⁹ Whereas, countries with a lower-risk score would be allowed to simplify their KYC requirements to allow for financial inclusion.²⁸⁰ Using a risk-based approach should focus on the prevention or mitigation of money laundering.

²⁷⁵ José Parra Moyano and Omri Ross, “KYC Optimization Using Distributed Ledger Technology,” *Business & Information Systems Engineering* 59, no. 6 (December 2017): 411, <http://dx.doi.org/10.1007/s12599-017-0504-2>.

²⁷⁶ Moyano and Ross, 412.

²⁷⁷ Michael Rennock, Alan Cohn, and Jared Butcher, *Blockchain Technology and Regulatory Investigations* (Washington, DC: Steptoe & Johnson LLP, 2018), 413, <https://www.steptoel.com/images/content/1/7/v2/171967/LIT-FebMar18-Feature-Blockchain.pdf>.

²⁷⁸ Financial Action Task Force on Money Laundering, *International Standards on Combating Money Laundering*, 1.

²⁷⁹ Financial Action Task Force on Money Laundering, 29.

²⁸⁰ Gelb, *Balancing Financial Integrity with Financial Inclusion*, 4.

A few customer risk factors mentioned by the FCTF of banks to consider are as follows:

- Business relationship involves unusual circumstances
- Customers are located outside the United States
- Legal persons are used as personal asset-holding vehicles
- Companies are cash-intensive
- Business ownership structure is unusual or complex
- Countries with an inadequate AML system
- Countries subject to embargos or sanctions
- Countries known for being corrupt or significant criminal activity
- Anonymous transactions
- Payments received from unknown third parties²⁸¹

Having a risk-based approach allows financial institutions to deal differently with small or large customers without hindering the development of start-ups or smaller businesses. Compliance expenses for KYC can be relatively high for startup companies with a minimal profit margin.

In dealing with a risk-based approach, India has a diverse population that deals with a wide range of social classes from extreme poverty to very wealthy. India also has a unique technology component within its county. The country developed the Unique Identification Authority of India (UIDAI) to “allocate an exclusive identification number to over 1.2 billion people.”²⁸² This 12-digit identification number satisfies the verification

²⁸¹ Financial Action Task Force on Money Laundering, *International Standards on Combating Money Laundering*, 62–63.

²⁸² Amiya Bhatia and Jacqueline Bhabha, “India’s Aadhaar Scheme and the Promise of Inclusive Social Protection,” *Oxford Development Studies* 45, no. 1 (2017): 64, <https://doi.org/10.1080/13600818.2016.1263726>.

process for social and financial inclusion.²⁸³ To obtain this unique number, Indian citizens must provide their “name, address, date of birth, gender, photograph and biometric data (iris scans and fingerprints.)”²⁸⁴ The authentication process uses this 12-digit number or Aadhaar card along with the biometrics of the citizen. This new identification system enhances security and financial inclusion from the old paper, forged documents, and slow, inefficient system for verification and authentication.²⁸⁵ India also demanded citizens opening a bank account must acquire an Aadhaar card within a year.²⁸⁶ The new system allowed citizens’ social and financial inclusion, even in impoverished areas or with socially excluded populations.²⁸⁷ Before this system, the depressed areas never had access to legal documents like birth certificates; thus, they were unable to access India’s financial system. The use of biometrics technology addressed gaps within their current system and allowed for reliable cash transfers, reduced the proliferation of fraud, and mitigated identity theft.²⁸⁸ Of course, an extensive biometric system controlled by the government may exceed the scope comfortable by most privacy advocates or other citizens attempting to keep their biometrics from a government-run network.

4. Peer-to-Peer

With the development of the fintech industry, access to mobile money and P2P transfers continue to increase; “87 percentage of merchants support either mobile site or mobile application for online shopping or both.”²⁸⁹ As more consumers and merchants embrace P2P networks solutions, such as Zelle, ApplePay, Venmo, PayPal, Google Wallet, Square Cash, Facebook Messenger, and other fintech companies, criminals are

²⁸³ Bhatia and Bhabha, 64.

²⁸⁴ Bhatia and Bhabha, 64.

²⁸⁵ Bhatia and Bhabha, 65.

²⁸⁶ Gelb, *Balancing Financial Integrity with Financial Inclusion*, 8.

²⁸⁷ Saibal Ghosh, “Financial Inclusion, Biometric Identification and Mobile: Unlocking the JAM Trinity,” *International Journal of Development Issues* 16, no. 2 (2017): 191, <http://doi.org/10.1108/IJDI-02-2017-0012>.

²⁸⁸ Bhatia and Bhabha, “India’s Aadhaar Scheme,” 65, 68.

²⁸⁹ Choi and Lee, *An Artificial Intelligence Approach to Financial Fraud Detection*, 1.

allowed another platform to exploit or launder illicit funds. With these new developments, FinCEN has just started imposing civil penalties against P2P exchangers involved in the movement of digital currency.

Based on these new platforms, FinCEN is beginning to penalize individuals acting as a money service business. In April 2019, FinCEN levied a punitive fine against a California citizen, Eric Powers.²⁹⁰ Powers operated as a P2P exchanger for digital currency and failed to register as a money services business under the BSA.²⁹¹ According to FinCEN, “‘money transmitters,’ peer-to-peer exchangers are required to comply with the BSA obligations that apply to MSBs [money service business], including registering with FinCEN; developing, implementing, and maintaining an effective AML program; filing Suspicious Activity Reports (SARs) and Currency Transaction (CTRs); and maintaining certain records.”²⁹² Powers conducted over 200 financial transactions of over \$10,000 and failed to file CTRs.²⁹³ FinCEN fined Powers \$35,000 who agreed no longer to operate as a money service business.²⁹⁴ This case is significant, as it is the first law enforcement action against a P2P digital currency exchanger.

Many P2P services meet the definition of financial institutions or money transmitters under the BSA/AML rules, as defined by FinCEN. The BSA should clearly define P2P services. Many fintech P2P services are not maintaining an adequate KYC program, anti-money laundering program, or filing appropriate CTRs. With P2P services, criminal organizations can store multiple payment cards from various banks on the same device and transfer funds through these different cards while staying under the CTR requirement. P2P services should report the transferring of funds from one device to another when the amount accumulates to \$10,000. P2P services can simply transfer money among separate banks to avoid reporting requirements. The BSA should address

²⁹⁰ “FinCEN Penalizes Peer-to-Peer Virtual Currency Exchanger for Violations of Anti-Money Laundering Laws,” Financial Crimes Enforcement Network, April 18, 2019, <https://www.fincen.gov/news/news-releases/fincen-penalizes-peer-peer-virtual-currency-exchanger-violations-anti-money>.

²⁹¹ Financial Crimes Enforcement Network.

²⁹² Financial Crimes Enforcement Network.

²⁹³ Financial Crimes Enforcement Network.

²⁹⁴ Financial Crimes Enforcement Network.

P2P transactions by using not only specific payment cards but also the international mobile equipment identity (IMEI). The IMEI number is a 15-digit serial number stored in the mobile phone memory.²⁹⁵ Every mobile phone is assigned this globally unique number that is recorded by the manufacturer.²⁹⁶ Mobile devices also have a unique 15-digit international mobile subscriber identity (IMSI) account number stored in the SIM card.²⁹⁷ This global number allows for roaming on service provider networks.²⁹⁸ The third identifier within mobile devices is the integrated circuit card identifier (ICCID). The ICCID is a unique serial number assigned to the SIM card and usually consists of 19 or 20 characters.²⁹⁹ Regulators must hold P2P payment services more accountable by increased monitoring and using fintech to detect the movement of illicit funds by mandating P2P services monitor not only payment cards, but also phone devices through IMEI, IMSI, and ICCID for fraud detection.

B. TECHNOLOGY ANALYSIS

1. Policy Options Criteria

The policy options criteria on technology also follow Eugene Bardach's steps to a practical policy options analysis. The policy options criteria consist of measuring the various types of fintech to be addressed in the BSA. The first is ML technology, and whether financial institutions should mandate this type of technology to increase their fraud detection capabilities. Second, digital currency is the new money exchange of choice among many criminals and money launders. FinCEN has issued several alerts and policies regarding digital currency, but should this new form of currency also be addressed in the BSA to provide digital currency users, miners, and exchangers clarification? Third, the matrix discusses three KYC approaches, with a focus on

²⁹⁵ Yi Yu et al., "A New Method for Identity Authentication Using Mobile Terminals," *Procedia Computer Science* 131 (2018): 774, <https://doi.org/10.1016/j.procs.2018.04.323>.

²⁹⁶ Yu et al., 774.

²⁹⁷ IMSI Oversight Council, "IMSI Home," International Mobile Subscriber Identity, 2019, <http://imsiadmin.com/>.

²⁹⁸ IMSI Oversight Council.

²⁹⁹ "IMEI Homepage," IMEI, accessed May 15, 2019, <https://www.imei.info/faq-what-is-ICCID/>.

biometrics, (DLT, and a RBA. Finally, P2P technology regarding the monitoring of IMEI, IMSI, and ICCID is presented.

2. Technology Criteria

The matrix addresses the complexity of the technology, costs to banks, privacy concerns, and political opposition.

a. Complexity

Using new technology can be extremely easy to implement and requires minimal maintenance. Other technology can be extremely complex and challenging to evaluate statically, implement, and maintain. Complexity is rated on a broad scale of “low” being non-complex, and “high” being extremely complex to implement and maintain.

b. Cost to Banks

Anytime increased regulatory costs for financial intuitions are a possibility, this criterion should be considered. This unit of measurement is assessed in terms of low, medium, and high in relation to the costs of implementing and maintaining the technology. It is not designated with a specific monetary amount, as the costs of the implementation and maintenance of technology continually adjusts.

c. Privacy

Privacy in this matrix not only deals with personally identifiable information (PII), but also general information obtained from big data, and more specifically, behavioral analytics. In dealing with new technology, biometrics, or other personal data, a constant struggle or balance occurs between security and risk. This section rates the concerns of privacy from an advocates’ perspective and their tolerance for accepting security over confidentiality. The unit of measurement is low, medium, and high, whereas low refers to little opposition from the privacy advocates and high refers to absolute objection and concern. Even though this scale can be subjective depending on the individual or group, the rating is objective, and based on the general view of the activists.

d. Political Opposition

As stated in the previous chapter, since the BSA requires congressional approval, political acceptance, or opposition, needs to be addressed. Political acceptance is classified by the likelihood that elected officials will pass the selected fintech. Thus, political opposition is the likelihood that officials will not support the technology. Elected officials consider their public base, political environment, and critical stakeholders and realize that being greatly opposed will not provide an affirmative vote. The criteria for this unit of measurement are also abstract, but this area needs to be addressed for any bill passage. The rating is based on the likelihood of passage. “Low” represents a politically acceptable requirement. “High” represents a regulatory requirement unlikely to pass, or high outside pressures result to negate the passage.

3. Technology Option Matrix

Table 2 measures the various types of fintech to be addressed in the BSA.

Table 2. Financial Technology

	Complexity	Costs to Banks	Privacy	Political Opposition
Machine Learning	High	High	High	High
Digital Currency	Low	Medium	Medium	Low
KYC Biometrics	Low	Low	Medium	Medium
KYC DLT	High	High	High	High
KYC RBA	Low	Medium	Medium	Low
P2P	Low	Low	Medium	Low

C. DISCUSSION

This section discusses the various viewpoints from the major parties involved by the legal proposal of fintech in the BSA. The bank executives, law enforcement, and privacy advocates have the strongest opinions regarding the implementation requirement of fintech in the BSA.

1. Bank Executives

In dealing with changes to the BSA, bank executives are primarily concerned about the costs associated with compliance. The financial burden placed on the banking industry is enormous, and the bankers pass those compliance burdens onto their customers to maintain a profitable business model. Requiring the implementation of advanced technology like ML and distributed ledger technology is very concerning to bankers, as seen in the matrix. Community banks or smaller banks will be extremely troubled by the implementation and maintenance costs, as well as the risk of using technology to maintain customer satisfaction. The smaller financial institutions may understand the benefits, but the costs of training skilled data scientists and maintaining their skillset is more than most can afford.

To use these advanced technologies, community banks need to outsource the technology to a private third party or join other financial institutions or an association like the Pacific Coast Bankers Bank (PCBB) to share the costly burden. The PCBB was created to assist smaller community-based banks with competitively priced banking solutions and services.³⁰⁰ The PCBB and other similar organizations may assist with advanced technology solutions like ML or distributed ledger technology in the future to distribute the costly service.

2. Law Enforcement

Law enforcement is indifferent to the various types of fintech used to detect or thwart money launderers; it needs the ability for banks to detect, retain the evidence, and report the suspicious activity promptly. Law enforcement is highly concerned with digital

³⁰⁰ “About PCBB,” PCBB, May 21, 2019, <https://www.pcbb.com/company/>.

currency, as the various cryptocurrencies have become the currency of choice among criminals. Due to this new way of transferring illicit funds, law enforcement prefers regulation that allows easier detection and monitoring of these transactions. As law enforcement improves its tracing techniques for digital currency like Bitcoin, criminals are migrating to digital currencies, like Monero, which provide a higher degree of anonymity and privacy to obfuscate law enforcement.

3. Privacy Advocates

Privacy advocates are continuously concerned with government security establishments and any regulations that threaten information privacy. As seen in the matrix, the activists are concerned with any technology involving personal information. Thus, no “low” ratings result, and the evaluation of medium and high are based strictly on the amount of privacy data retrieved or stored by the technology. The amount of personal data and behavior analytics obtained from ML technology and distributed ledger technology are of significant concern. The data stored using this advanced technology could jeopardize an individual’s privacy if stolen or used illicitly. The other technologies examined were rated as medium, as the data obtained is not less important, but the amount of data stored is less in comparison to the other fintech solutions.

D. ANALYSIS

The three separate groups affected by the implementation all have legitimate concerns that should carefully be considered when enacting a legislative law or change. Incorporating or mandating the use of fintech can have a profound effect on banking institutions. Prescribing any change should be carefully considered, as the monetary burden will eventually be placed on the consumer.

ML is extremely innovative with great potential for detecting suspicious activity. Financial institutions could benefit greatly from ML platforms if appropriately implemented. The technology is tremendously sophisticated, and monitoring costs are high, not only for the platform but to maintain data scientists with the proper training and expertise. ML solutions can provide accurate results if the data is harvested correctly and used appropriately. Based on the data needed to operate these platforms effectively,

privacy advocates have a legitimate concern about machines collecting transactional data without permission from their customers. Using this data to make a determination if a transaction is valid or illegal, poses yet another issue. With all the complications, the likelihood of Congress mandating the use of this technology is extremely low.

Law enforcement also has a legitimate concern regarding the unlawful use of digital currency. This new form of money allows criminals to circumvent financial institutions and avoid scrutiny. Thus, enacting regulations on digital currency exchangers and miners have little effect on bank executives, but can significantly reduce illicit financing if appropriately implemented. The political opposition to regulating digital currency is relatively low, and FinCEN has already provided guidance for digital currency exchangers, even though the regulations should be addressed in the BSA.

Using fintech to address the KYC regulations are wide-ranging with various implications depending on the type of technology. In using the distributed ledger technology, the same issue as ML arises. The technology is extremely sophisticated and requires constant monitoring from experienced data scientists. Also, the likelihood of Congress mandating this advanced technology is highly unlikely based on the costs and possible privacy implications.

In dealing with biometrics and a risk-based approach in KYC, privacy is a concern, but not as high as capturing or maintaining several aspects of personal data. The primary concern with biometrics is the possibility of network intrusions and a transnational cybercriminal organization obtaining the database. Once in the hands of criminals, they will conduct social engineering or other cyber schemes to exploit individuals and businesses. Using a risk-based approach appears to be a realistic and acceptable form of practice with less implementation and administrative costs. The tiered approach would also address the various classes of citizens and receive political acceptance.

Finally, regulations on P2P platforms have minimal costs to banks, and the ability to monitor IMEI, IMSI, or ICCID requires minimal software programming. Congress should receive little opposition to these regulations. Even though privacy advocates

would be opposed to this regulation, it would be minimal compared to the other fintech products mentioned.

The next chapter provides specific recommendation regarding the various fintech products and also addresses the SARs, CTRs, and beneficial ownership provision from Chapter III.

V. CONCLUSION

Proponents and opponents of increased regulations all agree the BSA must be updated to address the monetary thresholds for CTRs and SARs, along with tackling the beneficial ownership provision and fintech. Addressing these complex issues to account for all the affected members or organizations involved is daunting. Before enacting legislation with devastating effects, lawmakers must carefully consider the proper balance of increased regulations to hinder money launderers versus the violations of citizens' 4th Amendment protected privacy rights.

A. RECOMMENDATIONS

The BSA can be reformed to address emerging technology to prevent money laundering and illicit financing in several key ways: revise the monetary thresholds, add a beneficial ownership provision, and use fintech to uncover illicit finance.

1. Currency Transaction Reports

This thesis recommends raising the CTR monetary filing from \$10,000 to \$60,000, the rate of inflation. Furthermore, the BSA should grant the U.S. Secretary of Treasury the ability to raise the CTR monetary filing on a five-year basis to adjust for inflation.

The monetary requirement of the CTRs under the BSA has been debated for years by the various interest groups. One area of concern in the U.S. government, specifically the IRS and law enforcement, is the human resources to review and pursue possible violators of the BSA. According to the Treasury Inspector General for Tax Administration, "the IRS is still not systemically using the CTRs to identify and pursue potentially noncompliant individuals." Even though this statement is directed toward IRS management, it does not address the staffing levels and burden placed on the IRS. The National Treasury employees Union reported the IRS lost "\$715 million in funding and

22,000 full-time employees since 2010.”³⁰¹ If the IRS is unable to comb through CTR filing effectively, why is legislation mandating financial institutions file the CTRs at the \$10,000 monetary threshold? In 2017, financial institutions filed 15.8 million CTRs.³⁰² The larger financial institutions are spending approximately \$1 billion annually in BSA compliance.³⁰³ These high compliance costs and the lack of U.S. government staffing levels to review and investigate CTR filings actively, supports raising the current monetary threshold.

2. Suspicious Activity Reports

The current monetary thresholds for SARs in the BSA as \$1,000, \$2,000, and \$5,000 for specific categories should remain the same. The primary goal of SARs is to report suspected or known violators to law enforcement for further investigations. This reporting process is instrumental in maintaining the integrity of the financial systems and deterring criminals from using the Federal Reserve System to launder funds. With the number of financial transactions taking place on a daily bases, bank investigators have no intent on conducting surveillance of citizens bank accounts. Investigators search for unordinary or questionable activity. In 2017, financial institutions filed 1.5 million SARs; these numbers are an extraordinary human resource burden task.³⁰⁴ Daily, FinCEN takes the SARs running them through automated and internal business rule sets to identify activity requiring additional review for analysis.³⁰⁵ This internal process generates around 50 matches daily that are distributed to law enforcement around the county to identify and disrupt illegal activity.³⁰⁶ Based on this internal process, not only are the financial

³⁰¹ “Now Is the Time to Reverse the Decline of the IRS Budget,” The National Treasury Employees Union, May 22, 2108, <https://www.nteu.org/media-center/news-releases/2018/05/22/irs-budget-release>.

³⁰² Luetkemeyer and Pearce, “It’s Time to Modernize.”

³⁰³ Daniel P. Stipano, “Time to Bring BSA into This Century,” American Banker, February 21, 2017, <https://www.americanbanker.com/opinion/time-to-bring-bsa-into-this-century>.

³⁰⁴ Luetkemeyer and Pearce, “It’s Time to Modernize.”

³⁰⁵ Kenneth A. Blanco, “Prepared Remarks of FinCEN Director Blanco at the NYU Law Program on Corporate Compliance and Enforcement,” Financial Crimes Enforcement Network, June 12, 2019, <https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-blanco-nyu-law-program-corporate-compliance-and>.

³⁰⁶ Blanco.

institutions declaring the activity suspicious but further analysis is needed by FinCEN to give law enforcement the ability to review and pursue only suspicious activity.

3. Beneficial Ownership Provision

This paper recommends adding the beneficial ownership provision to the BSA. For years, the beneficial ownership provision has been highly contentious. Weighting the delicate balance between corporate privacy and the ability to pursue criminals hiding behind protective lines must be addressed. Concurring with the argument is the recent introduction of bill, H.R. 2513, the “Corporate Transparency Act,” on May 11, 2019, by Representative Carolyn Maloney.³⁰⁷ The Corporate Transparency Act states:

To ensure person who form corporations or limited liability companies in the United States disclose the beneficial owners of those corporations or limited liability companies, in order to prevent wrongdoers from exploiting United States corporations and limited liability companies for criminal gain, to assist law enforcement in detecting, preventing, and punishing terrorism, money laundering, and other misconduct involving United States corporations and limited liability companies, and for other purposes.

This bill addresses the contentious issue removed from the Counter Terrorism and Illicit Finance Act. The finance sub-committee supports the recommendation with a bipartisan 43–16 passage, thus moving the bill to the full chamber for further consideration.³⁰⁸ The beneficial ownership provision assists law enforcement and the U.S. international law enforcement partners to pursue money launders hiding behind layers of corporate bureaucracies aggressively.

4. Machine Learning

ML technology should not be mandated in the BSA, but encouraged as the technology develops. According to the matrix, the complexity of the technology, the monetary cost to banking institutions, privacy concerns, and political oppositions are all

³⁰⁷ Carolyn B. Maloney, “H.R.2513—116th Congress (2019–2020): Corporate Transparency Act of 2019,” Public Law 2513, H.R. 2513 (2019), <https://www.congress.gov/bill/116th-congress/house-bill/2513>.

³⁰⁸ Chuck Canterbury, *FOP Applauds Financial Services Committee on Passage of Crucial Anti-Money Laundering Bill* (Washington, DC: Fraternal Order of Police, 2019), 1, <https://fop.net/CmsDocument/Doc/PR%20-%20H.R.%202513%20Comm%20Pass.pdf>.

reasons for not mandating this type of technology in the BSA. Also, this thesis addresses numerous concerns regarding this advanced technology.

The technology should only be encouraged as fintech continues to develop and increase. ML removes the human element of surveilling and increases efficiency in processing or reviewing enormous amounts of financial data. Larger financial institutions should be encouraged to explore ML technology to assist with SAR detection and submitting those documents through the BSA E-Filing System.³⁰⁹ However, based on the numerous concerns mentioned previously in the paper, ML should only be encouraged and not required.

5. Digital Currency

The BSA should regulate digital currency. FinCEN has already mandated several regulations on digital currency exchangers, but these regulations should be discussed and addressed by legislators. The BSA should specifically address advanced privacy digital coins like Monera, Zcash, and Dash. These privacy coins are designed for increased privacy, yet are untraceable by LE investigators. The BSA should also regulate mixer and tumblers, such as Bitmixer or Helix, that are primarily used by criminals to launder illicit funds. The mixers and tumblers should be required to keep financial records as a money services business.

6. Know Your Customer

The BSA should provide banks with a minimum standard for a client to open an account. Using fintech, the BSA should consider recommending biometrics as a component of KYC requirement. According to the Pew Research Center, over 95% of adults from the ages of 18–34 in the United States have a smartphone device.³¹⁰ A

³⁰⁹ “Important Reminders to FinCEN SAR & CTR E-Fileers: User Test System Now Available for SAR XML Batch and Discrete Testing FinCEN to Release the SAR, as Well as the Updated CTR XML Schema on July 27th, 2018,” Financial Crimes Enforcement Network, 1, July 10, 2018, https://bsaeifiling.fincen.treas.gov/docs/FinCENSAR_XML_ReminderNotice.pdf.

³¹⁰ Kyle Taylor and Laura Silver, “Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally,” Pew Research Center, February 5, 2019, <https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/>.

majority of cellphones work with biometrics, whether using fingerprints or facial recognition to unlock the device. For those without a smartphone device, they can access a bank within their area to provide biometrics information.

The BSA should also require a risk-based approach regarding KYC, as suggested by the Financial Crimes Task Force.³¹¹ These recommendations ensure consistency not only throughout the United States but also globally. Using a risk-based approach ensures additional KYC requirement for high-risk countries enhancing customer identification and customer due diligence.

DLT should not be mandated within the BSA, but should be encouraged as technology advances. Like ML, DLT is extremely complex, costly to implement and maintain, with privacy concerns and political oppositions. For these reasons, mandating this type of technology should only be encouraged.

7. Peer-to-Peer

The BSA must hold P2P payment services more accountable by increased monitoring, especially through the recording of financial transactions as related to IMEI, IMSI, and ICCID. With the development of the fintech, specifically mobile device platforms, access to mobile money continues to shape the ability to buy, sell, and transfer money at higher speeds with minimal human interaction. As more consumers and merchants embrace these solutions, criminals use these same platforms to exploit or launder illicit funds.

The legislators should be cautious in restricting innovation within the United States, as fintech encourages financial ingenuity and security to accelerate financial services globally. Likewise, the BSA should support fintech throughout the financial sector, but only mandating the use of fintech if beneficial.

³¹¹ Financial Action Task Force on Money Laundering, *International Standards on Combating Money Laundering*, 62–63.

B. IMPLEMENTATION CHALLENGES

Implementing these recommendations in the BSA is a challenging obstacle to overcome. Before the changes can occur, the Treasury Department, members of the House Financial Services Committee, Congressmen, Senators, or even a lobbyist involved in the financial services sector must construct a preliminary bill. Designing a bill that accounts for these various interest groups is a difficult task. Thus, striking a proper balance is instrumental in obtaining bi-partisan support. The recommendations of this thesis consider the various interest groups and attempt to find the proper balance between privacy advocates, the regulated, law enforcement, and the regulators. Moving forward, the Treasury Department should write a bill adding the aforementioned recommendations, as well as understanding the objections from the various interest groups. Discussions and modifications to the proposed bill occurs once introduced to the House Financial Service Committee.

C. FUTURE AREA OF RESEARCH

In dealing with regulation to prevent money laundering, continued research can pursue various options. One option, should an international body be created to monitor and regulate this new form of exchange? A primary issue is the specific regulation of digital currency. As mentioned in this paper, digital currency is not backed by any government or national body. Another option of continued research, should regulation limit the use of privacy coins, like Monero, that is specifically designed to avoid tracing? Alternatively, do the privacy advocates have a valid position that regulation should not restrict individual privacy regarding new forms of cryptocurrency? In creating a new international body, who should be part of this committee and how much authority? Cryptocurrency is unlikely to be an issue for just one nation, but a global concern for future generations.

Narrowing the focus of digital currency as a nation state-sponsored concern leads to another area of research. Should the U.S. Federal Reserve or the U.S. Department of Treasury create their own digital currency with oversight? What are the advantages, limitations, and possible unintended consequences of the U.S. government operating its

cryptocurrency? One of the main benefits of digital currency is the fact that it operates as a decentralized authority. If the U.S. government owned and operated a form of digital currency, is another layer of bureaucracy and regulations added that so many are attempting to avoid.

As mentioned in this thesis, blockchain technology has several benefits in the financial services sector. Knowing a majority of financial institutions are exploring this new avenue of technology, how can blockchain technology protect anyone's financial privacy? If banking institutions use blockchain technology, how much control do these institutions have in the verification and authentication process?

A final area of research is the use of mobile devices and their impact on the financial services sector. With the development of smartphones and increased applications, mobile devices will significantly impact the future of U.S. society with financial banking, investments, and loans. Should mobile banking be regulated using an international working group? As the world becomes more connected through Wi-Fi and cellular, mobile banking will continue to grow and impact improvised areas globally.

D. CONCLUSION

Supporters and challengers of the BSA all agree on the need to update the historical mandates within the act to address emerging threats and technology. The BSA needs to address outdated monetary thresholds for CTRs and confront the beneficial ownership provision. Likewise, the BSA needs to regulate innovative financial technologies like digital currency, KYC, and P2P, to deter the movement of criminal funds. With the innovations of financial technology, criminals are finding new ways to launder money, while obfuscating detection from law enforcement authorities.

The BSA should address not only the present but future concerns involving technology and potential risks to the financial sector, while maintaining a balance between increased regulation to hinder criminal activity without stifling the growth of innovation. As criminal organizations continue to move money throughout the U.S. financial services sector, legislators should amend the BSA to address these areas of concern to ensure financial stability and integrity.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- “The 1970 Bank Secrecy Act and the Right of Privacy.” *William & Mary Law Review* 14, no. 4 (1973): 929–52. <https://scholarship.law.wm.edu/wmlr/vol14/iss4/7>.
- Aaron MacKey. “California Lawmaker Pulls Digital Currency Bill after EFF Opposition.” Electronic Frontier Foundation, August 18, 2016. <https://www.eff.org/deeplinks/2016/08/california-lawmaker-pulls-digital-currency-bill-after-eff-opposition>.
- Anonymous. “Bitcoin Blender.” Bitcoin Blender. Accessed May 1, 2019. <https://bitblender.io/index.html>.
- . “New Suspicious Activity Report Streamlines Reporting System.” *ABA Bank Security & Fraud Prevention* 3, no. 1 (January 1996): 1–2. ProQuest.
- Avergun, Jodi, and Colleen Kukowski. “Complying with AML Laws: Challenges for the Fintech Industry.” Crowdfund Insider, April 5, 2016. <https://www.crowdfundinsider.com/2016/04/83845-complying-with-aml-laws-challenges-for-the-fintech-industry/>.
- Barclay, Stephen, and Ben Wallace. *National Risk Assessment of Money Laundering and Terrorist Financing 2017*. New York: Crown, 2017. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/655198/National_risk_assessment_of_money_laundering_and_terrorist_financing_2017_pdf_web.pdf.
- Bass, Harold. *Joint Subcommittee Hearing on H.R. 6068, the Counter Terrorism and Illicit Finance Act" and Concerns Regarding Section 9*. Chicago, IL: American Bar Association, 2017. [https://www.americanbar.org/content/dam/aba/un categorized/GAO/gatekeeperregandtheprofessiontf\(abalettertohfscfinalversionnov272017\).authcheckdam.pdf](https://www.americanbar.org/content/dam/aba/un categorized/GAO/gatekeeperregandtheprofessiontf(abalettertohfscfinalversionnov272017).authcheckdam.pdf).
- Baumann, David “Financial Regulators Fail to Evaluate Combined Impact of Rules: GAO.” *Credit Union Times*, February 27, 2018. <https://www.cutimes.com/2018/02/27/financial-regulators-fail-to-evaluate-combined-imp/>.
- Bhatia, Amiya, and Jacqueline Bhabha. “India’s Aadhaar Scheme and the Promise of Inclusive Social Protection.” *Oxford Development Studies* 45, no. 1 (2017): 64–79. <https://doi.org/10.1080/13600818.2016.1263726>.
- Blanco, Kenneth A. “Prepared Remarks of FinCEN Director Blanco at the NYU Law Program on Corporate Compliance and Enforcement.” Financial Crimes Enforcement Network, June 12, 2019. <https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-blanco-nyu-law-program-corporate-compliance-and>.

- . “Prepared Remarks of FinCEN Director Kenneth A. Blanco, Delivered at the 2018 Chicago-Kent Block (Legal) Tech Conference.” Federal Crimes Enforcement Network, August 9, 2018. <https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-2018-chicago-kent-block>.
- Bradford, Scott. “You’ve Been Served, but Does It Count: Serving a Criminal Corporate Defendant under Federal Rule of Criminal Procedure 4.” *Department of Justice Journal of Federal Law and Practice* 67, no. 1 (February 2019): 263–70. <https://www.justice.gov/usao/page/file/1135861/download>.
- Brito, Jerry, and Andrea Castillo. *Bitcoin: A Primer for Policymakers*. Vol. 29. Arlington, VA: Mercatus Center, 2013. https://www.mercatus.org/system/files/Brito_BitcoinPrimer.pdf.
- Brownlee, Jason. “Supervised and Unsupervised Machine Learning Algorithms.” *Machine Learning Mastery* (blog). March 15, 2016. <https://machinelearningmastery.com/supervised-and-unsupervised-machine-learning-algorithms/>.
- Budd, Ted. “H.R.56—Financial Technology Protection Act.” Public Law 56, 12 (2019). <https://www.congress.gov/bill/116th-congress/house-bill/56/text>.
- Bullock, Jeffrey. *Letter to Chairman Hensarling*. State of Delaware, Department of State, 2018. <https://thefactcoalition.org/wp-content/uploads/2018/06/DE-June-2018-Letter-to-HFSC-on-BOT.pdf>.
- Campbell-Verduyn, Malcolm, Marcel Goguen, and Tony Porter. “Big Data and Algorithmic Governance: The Case of Financial Practices.” *New Political Economy* 22, no. 2 (2017): 219–36. <http://dx.doi.org/10.1080/13563467.2016.1216533>.
- Canterbury, Chuck. *FOP Applauds Financial Services Committee on Passage of Crucial Anti-Money Laundering Bill*. Washington, DC: Fraternal Order of Police, 2019. <https://fop.net/CmsDocument/Doc/PR%20-%20H.R.%202513%20Comm%20Pass.pdf>.
- . *Letter to Chairman and Representative Waters*. Washington, DC: Fraternal Order of Police, 2018. <https://static.politico.com/bb/07/a3e3dfbd48aab8446528bf02bcad/fop-on-beneficial-ownership.pdf>.
- Chen, Zhiyuan, Le Dinh Van Khoa, Ee Na Teoh, Amril Nazir, Ettikan Kandasamy Karuppiah, and Kim Sim Lam. “Machine Learning Techniques for Anti-Money Laundering (AML) Solutions in Suspicious Transaction Detection, A Review.” *Knowledge and Information Systems* 57, no. 2 (November 2018): 245–285. <https://doi.org/10.1007/s10115-017-1144-z>.

- Choi, Dahee, and Kyungho Lee. *An Artificial Intelligence Approach to Financial Fraud Detection under IoT Environment: A Survey and Implementation*. Seoul, Republic of Korea: Kindawi, 2018. <https://doi.org/10.1155/2018/5483472>.
- Clearing House, The. “ACH.” Accessed April 29, 2019. <https://www.theclearinghouse.org/payment-systems/ach>.
- Cocheo, Steve. “Flexible Patriot Rules Prove Double-Edged Blade.” *ABA Banking Journal* 95, no. 12 (December 2003): 52–55. ProQuest.
- Coinbase. “Why Does a Buy Take so Long?.” Accessed April 29, 2019. <https://support.coinbase.com/customer/portal/articles/1392022-why-does-a-buy-take-so-long->.
- Courbe, Julien. *Financial Services Technology 2020 and Beyond: Embracing Disruption*. New York: PricewaterhouseCoopers, 2016. <https://www.pwc.com/gx/en/financial-services/assets/pdf/technology2020-and-beyond.pdf>.
- Crosman, Penny. “Bank of America, Harvard Form Group to Promote Responsible AI.” *American Banker*, April 10, 2018. <https://www.americanbanker.com/news/bank-of-america-harvard-form-group-to-promote-responsible-ai>.
- Domingues, Remi. “Machine Learning for Unsupervised Fraud Detection.” Master’s thesis, KTH, Sweden, INSA Lyon, 2015. <http://www.diva-portal.org/smash/get/diva2:897808/FULLTEXT01.pdf>.
- Eldridge, James E. “The Bank Secrecy Act: Privacy, Comity, and the Politics of Contraband.” *North Carolina Journal of International Law and Commercial Regulation* 11, no. 3 (1986): 667–97. <https://scholarship.law.unc.edu/ncilj/vol11/iss3/12/>.
- Electronic Frontier Foundation. “About EFF.” July 10, 2007. <https://www.eff.org/about>.
- Facebook. “A New Digital Wallet for a New Digital Currency.” Facebook Newsroom, June 18, 2019. <https://newsroom.fb.com/news/2019/06/coming-in-2020-calibra/>.
- FACT Coalition. “About Us.” Accessed April 6, 2019. <https://thefactcoalition.org/about>.
- Federal Financial Institutions Examination Council. *Bank Secrecy Act/Anti-Money Laundering Examination Manual*. Washington, DC: Federal Financial Institutions Examination Council, 2014. https://www.ffiec.gov/bsa_aml_infobase/documents/bsa_aml_man_2014.pdf.
- . *Beneficial Ownership Requirements for Legal Entity Customers—Overview*. Washington, DC: Federal Financial Institutions Examination Council, 2018. <https://www.ffiec.gov/press/pdf/Beneficial%20Ownership%20Requirements%20for%20Legal%20Entity%20CustomersOverview-FINAL.pdf>.

- Feedzai. *Operationalizing Machine Learning for Fraud*. San Mateo, CA: Feedzai, 2017. <https://feedzai.com/wp-content/uploads/2017/09/Operationalizing-Machine-Learning-For-Fraud-v107.pdf>.
- . *The Dawn of Machine Learning for Banking and Payments*. San Mateo, CA: Feedzai, 2017. <https://feedzai.com/wp-content/uploads/2017/08/Dawn-of-Machine-Learning-041317a.pdf>.
- Financial Accountability & Corporate Transparency. *RE: Discussion Draft Counter Terrorism and Illicit Finance Act*. Washington, DC: Financial Accountability & Corporate Transparency, 2018. <https://thefactcoalition.org/wp-content/uploads/2019/01/INGOs-letter-on-beneficial-ownership.pdf>.
- Financial Action Task Force on Money Laundering. *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*. Paris, France: Financial Action Task Force on Money Laundering, 2018. www.fatf-gafi.org/recommendations.html.
- Financial Conduct Authority. *Loan-Based ('Peer-to-Peer') and Investment-Based Crowdfunding Platforms: Feedback to CP 18/20 and Final Rules*. London: Financial Conduct Authority, 2019. <https://www.fca.org.uk/publication/policy/ps19-14.pdf>.
- Financial Crimes Enforcement Network. *Advisory on Illicit Activity Involving Convertible Virtual Currency*. Vienna, VA: Financial Crimes Enforcement Network, 2019. <https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf>.
- . “Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies.” March 2013. <https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering>.
- . “Customer Due Diligence Requirements for Financial Institutions.” *Federal Register* 81, no. 91 (May 11, 2016): 29398–29458. <https://www.govinfo.gov/app/details/FR-2016-05-11>.
- . “FinCEN Fines BTC-e Virtual Currency Exchange \$110 Million for Facilitating Ransomware, Dark Net Drug Sales.” July 27, 2017. <https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware>.
- . “FinCEN Fines Ripple Labs Inc. in First Civil Enforcement Action against a Virtual Currency Exchanger.” May 5, 2015. <https://www.fincen.gov/news/news-releases/fincen-fines-ripple-labs-inc-first-civil-enforcement-action-against-virtual>.

- . “FinCEN Issues Ruling (FIN-2008-R011) on Whether a Company that Engages in Microfinance Is a Money Services Business.” February 20, 2009. <https://www.fincen.gov/resources/statutes-regulations/administrative-rulings/fincen-issues-ruling-fin-2008-r011-whether>.
- . “FinCEN Penalizes Peer-to-Peer Virtual Currency Exchanger for Violations of Anti-Money Laundering Laws.” April 18, 2019. <https://www.fincen.gov/news/news-releases/fincen-penalizes-peer-peer-virtual-currency-exchanger-violations-anti-money>.
- . “FinCEN’s Mandate from Congress.” Accessed February 4, 2019. <https://www.fincen.gov/resources/fincens-mandate-congress>.
- . “Important Reminders to FinCEN SAR & CTR E-Filers: User Test System Now Available for SAR XML Batch and Discrete Testing FinCEN to Release the SAR, as Well as the Updated CTR XML Schema on July 27th, 2018.” July 10, 2018. https://bsaefiling.fincen.treas.gov/docs/FinCENSAR_XML_Reminder_Notice.pdf.
- FinTech Weekly Definition. “FinTech Definition.” 2017. <https://www.fintechweekly.com/fintech-definition>.
- First Data Corporation. *Machine Learning, Security and the Future of Fraud*. Atlanta: First Data Corporation, 2017. <https://www.firstdata.com/downloads/pdf/MachineLearningSecurityandtheFutureofFraud.pdf>.
- Frentzen, William, and Kathryn Haun. *United States vs BTC-E and Alexander Vinnik*. Washington, DC: Department of Justice, 2017. <https://www.justice.gov/usao-ndca/press-release/file/984661/download>.
- Gelb, Alan. *Balancing Financial Integrity with Financial Inclusion: The Risk-Based Approach to “Know Your Customer.”* CGD Policy Paper 074. Washington, DC: Center for Global Development, 2016. <http://www.cgdev.org/sites/default/files/CGD-Policy-Paper-Gelb-KYC-Financial-Inclusion.pdf>.
- Gershel, Brad. “Beneficial Ownership Provision Stripped from Latest Draft of Counter Terrorism and Illicit Finance Act.” *National Law Review*, June 20, 2018. <https://www.natlawreview.com/article/beneficial-ownership-provision-stripped-latest-draft-counter-terrorism-and-illicit>.
- Ghosh, Saibal. “Financial Inclusion, Biometric Identification and Mobile: Unlocking the JAM Trinity.” *International Journal of Development Issues* 16, no. 2 (2017): 190–213. <http://doi.org/10.1108/IJDI-02-2017-0012>.

- Guidotti, Riccardo, Anna Monreale, Salvatore Ruggieri, Franco Turini, Fosca Giannotti, and Dino Pedreschi. “A Survey of Methods for Explaining Black Box Models.” *ACM Computing Surveys* 51, no. 5 (August 2018): 1–42. <https://doi.org/10.1145/3236009>.
- Halawa, Hassan, Matei Ripeanu, Konstantin Beznosov, Baris Coskun, and Meizhu Liu. “Forecasting Suspicious Account Activity at Large-Scale Online Service Providers.” *ArXiv:1801.08629 [Cs]*, January 25, 2018. <http://arxiv.org/abs/1801.08629>.
- “Heritage Action Supports the Revised Counter Terrorism and Illicit Finance Act (H.R. 6068).” *Heritage Action for America* (blog), June 14, 2018. <https://heritageaction.com/press/heritage-action-supports-the-revised-counter-terrorism-and-illicit-finance-act-h-r-6068>.
- Holquist, Samantha. “How to Conduct an Effective Policy Analysis.” *GovLoop* (blog). July 18, 2013. <https://www.govloop.com/community/blog/how-to-conduct-an-effective-policy-analysis/>.
- Horan, TJ. “5 Keys to Using AI and Machine Learning in Fraud Detection.” July 3, 2018. <http://www.fico.com/en/blogs/analytics-optimization/5-keys-to-using-ai-and-machine-learning-in-fraud-detection/>.
- Howard, Cory. “Financial Crimes Compliance Self-Governance: Applying the Faragher Defense to Bank Secrecy Act/Anti-Money Laundering Violations.” *The University of Memphis Law Review* 48, no. 1 (2017): 46–82. https://www.memphis.edu/law/documents/howard_financialcrimescomplianceself-governance.pdf.
- IMEI. “IMEI Homepage.” Accessed May 15, 2019. <https://www.imei.info/faq-what-is-ICCID/>.
- IMSI Oversight Council. “IMSI Home.” International Mobile Subscriber Identity, 2019. <http://imsiadmin.com/>.
- Lamer, Michael. *The Future of Fintech ~ The New Standard*. United Kingdom: Juniper Research, 2019. <https://www.juniperresearch.com/document-library/white-papers/the-future-of-fintech-the-new-standard-white-paper>.
- LegiNation. “US—HR 6068: Counter Terrorism and Illicit Finance Act.” Bill Track 50. Accessed February 21, 2019. <https://www.billtrack50.com/BillDetail/986684>.
- Lewis, Rhydian. “Our View on the FCA Proposals for Peer-to-Peer Lending.” *RateSetter*, August 6, 2018. <https://www.ratesetter.com/blog/our-view-on-the-fca-proposals-for-peer-to-peer-lending>.
- Litecoin Master. *Demonrat—Brad Sherman Law to Ban Bitcoin*. YouTube. Video, 1:12. May 9, 2019. <https://www.youtube.com/watch?v=IkC-uXMoy4c>.

- Lo, Benjamin. “Fatal Fragments: The Effect of Money Transmission Regulation on Payments Innovation.” *Yale Journal of Law and Technology* 18, no. 1 (2017): 111–47. <https://digitalcommons.law.yale.edu/yjolt/vol18/iss1/4>.
- Luetkemeyer, Blaine, and Steve Pearce. “It’s Time to Modernize the Bank Secrecy Act.” *American Banker*, June 13, 2018. <https://www.americanbanker.com/opinion/its-time-to-modernize-the-bank-secrecy-act>.
- Maloney, Carolyn B. “H.R.2513—116th Congress (2019–2020): Corporate Transparency Act of 2019.” Public Law 2513, H.R. 2513 (2019). <https://www.congress.gov/bill/116th-congress/house-bill/2513>.
- Mercator Advisory Group, Inc. *Fraud Detection 2.0: Dynamic Tools for Fighting E-Commerce Fraud*. Boise, ID: Knout, 2017. <https://info.kount.com/white-paper/fraud-detection-dynamic-tools-for-fighting-ecommerce-fraud>.
- Misback, Ann. *United States of America before the Board of Governors of the Federal Reserve System Washington, D.C.* Washington, DC: The Federal Reserve Board, 2017. <https://www.federalreserve.gov/newsevents/pressreleases/enforcement20170530a.htm>.
- Moyano, José Parra, and Omri Ross. “KYC Optimization Using Distributed Ledger Technology.” *Business & Information Systems Engineering* 59, no. 6 (December 2017): 411–423. <http://dx.doi.org/10.1007/s12599-017-0504-2>.
- Mugarura, Norman. “Does the Broadly Defined Ambit of Money Laundering Offences Globally, a Recipe for Confusion than Clarity?.” *Journal of Money Laundering Control* 19, no. 4 (2016): 432–46. <http://doi.org/10.1108/JMLC-06-2015-0024>.
- NACHA “Expanding Same Day ACH.” Accessed April 29, 2019. <https://www.nacha.org/rules/expanding-same-day-ach>.
- . *Faster Payments Tracker*. Boston, MA: PYMNTS.COM, 2016. <https://web.nacha.org/system/files/resource/2017-08/NACHA-Faster-Payments-Tracker-FEB.pdf>.
- National Association of Federally-Insured Credit Unions. “NAFCU, Others Support Bill to Strengthen Anti-Money Laundering Efforts.” Newsroom, NAFCU, January 5, 2018. <https://www.nafcu.org/newsroom/nafcu-others-support-bill-strengthen-anti-money-laundering-efforts>.
- National Treasury Employees Union, The. “Now Is the Time to Reverse the Decline of the IRS Budget.” May 22, 2108. <https://www.nteu.org/media-center/news-releases/2018/05/22/irs-budget-release>.

- Neuwirth, Suzie. “Here’s What the Industry Thinks of the FCA Rule Changes.” Here’s What the Industry Thinks, *Peer2Peer Finance News* (blog). June 4, 2019. <http://www.p2pfinancenews.co.uk/2019/06/04/heres-what-the-industry-thinks-of-the-fca-rule-changes/>.
- OXFAM International. “Paradise Papers: The Hidden Costs of Tax Dodging.” *The Power of People against Poverty*. Accessed April 6, 2019. <https://oxf.am/2zAYO0u>.
- PCBB. “About PCBB.” May 21, 2019. <https://www.p PBB.com/company/>.
- Pitch Book. “Home Page.” Accessed February 8, 2019. <https://pitchbook.com/>.
- Plombeck, Charles. *The International Lawyer*. Cary, NC: American Bar Association, 1988.
- Pollari, Ian, and Anton Ruddenklau. *The Pulse of Fintech 2018: Biannual Global Analysis of Investment in Fintech*. Zurich: KPMG International, 2018. <https://home.kpmg/content/dam/kpmg/us/pdf/2018/07/pof-1H-18-report.pdf>.
- Pompliano, Anthony. “Banning Bitcoin Will Drive More Adoption.” *Banning Bitcoin Will Drive More Adoption* (blog). May 10, 2019. <https://offthechain.substack.com/p/banning-bitcoin-will-drive-more-adoption>.
- Poncy, Chip. “Legislative Proposals to Counter Terrorism and Illicit Finance.” § House Financial Services Committee, Financial Institutions and Consumer Credit and Terrorism and Illicit Finance Subcommittees, 1, 2017. <https://www.fdd.org/analysis/2017/11/29/legislative-proposals-to-counter-terrorism-and-illicit-finance/>.
- PR Newswire. “Guardian Analytics Will Feature Newest Real-Time Digital Banking Fraud Detection Solutions at Malauzai #InnovationNATION.” *Markets Insider*, March 22, 2018. <https://markets.businessinsider.com/news/stocks/guardian-analytics-will-feature-newest-real-time-digital-banking-fraud-detection-solutions-at-malauzai-innovationnation-1019043726>.
- Pye, Jason. “Oppose the Counter Terrorism and Illicit Finance Act.” *Oppose the Counter Terrorism and Illicit Finance Act* (blog). November 28, 2017. <https://www.freedomworks.org/content/oppose-counter-terrorism-and-illicit-finance-act>.
- Ramey, Corinne. “The Crypto Crime Wave Is Here; from Stickups and Drug Deals to White-Collar Scams, Cryptocurrency-Related Crime Is Soaring—and Law Enforcement Is Scrambling to Keep Up.” *Wall Street Journal*. April 26, 2018. <https://www.wsj.com/articles/the-crypto-crime-wave-is-here-1524753366>.
- RateSetter. “The UK’s Most Popular Peer to Peer Investment Platform.” June 27, 2019. <https://www.ratesetter.com/about-us>.

- Ravelin Technology Ltd. *The Complete Guide to Machine Learning and Fraud Prevention*. London, New York: Ravelin Technology Ltd., 2017. <https://cdn2.hubspot.net/hubfs/2322855/Machine%20learning/The%20Complete%20Guide%20to%20Machine%20Learning%20and%20Fraud%20Prevention.pdf>.
- Reitman, Rainey. “Why Outlawing Cryptocurrency Purchases Is a Terrible Idea.” Electronic Frontier Foundation, May 13, 2019. <https://www.eff.org/deeplinks/2019/05/why-bill-banning-cryptocurrency-purchases-americans-terrible-idea>.
- Rennock, Michael, Alan Cohn, and Jared Butcher. *Blockchain Technology and Regulatory Investigations*. Washington, DC: Steptoe & Johnson LLP, 2018. <https://www.steptoelaw.com/images/content/1/7/v2/171967/LIT-FebMar18-Feature-Blockchain.pdf>.
- Renstrom, Martin, and Timothy Holmsten. *Fraud Detection on Unlabeled Data with Unsupervised Machine Learning*. Stockholm, Sweden: Examensarbete Inom Datateknik, 2018. <http://kth.diva-portal.org/smash/get/diva2:1217521/FULLTEXT01.pdf>.
- Riggleman, Denver. “H.R.1039.” Public Law 1039, 4 (2019). <https://www.congress.gov/bills/116/congress-house-bill/1039>.
- Simser, Jeffrey. “Bitcoin and Modern Alchemy: In Code We Trust.” *Journal of Financial Crime* 22, no. 2 (2015): 156–69. <http://dx.doi.org/10.1108/JFC-11-2013-0067>.
- Sparks, Evan. “Regulatory Compliance?.” *ABA Banking Journal* 109, no. 3 (June 2017): 24–25. <http://www.nxtbook.com/naylor/BAKS/BAKS0317/index.php#/0>.
- Stipano, Daniel P. “Time to Bring BSA into This Century.” *American Banker*, February 21, 2017. <https://www.americanbanker.com/opinion/time-to-bring-bsa-into-this-century>.
- Taylor, Kyle, and Laura Silver. “Smartphone Ownership Is Growing Rapidly Around the World, but Not Always Equally.” Pew Research Center, February 5, 2019. <https://www.pewresearch.org/global/2019/02/05/smartphone-ownership-is-growing-rapidly-around-the-world-but-not-always-equally/>.
- Thomas, Zoe. “Bitcoin Becoming Argentina’s Fx Alternative.” *International Financial Law Review*, August 13, 2015. <https://www.iflr.com/Article/3479503/Bitcoin-becoming-Argentinas-FX-alternative.html?ArticleId=3479503>.
- Thomson Reuters. “Thomson Reuters 2016 Know Your Customer Surveys Reveal Escalating Costs and Complexity.” May 9, 2016. <https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html>.

- Treasury Inspector General for Tax Administration. *Currency Report Data Can Be a Good Source for Audit Leads*. Washington, DC: Department of Treasury, 2010. <https://www.treasury.gov/tigta/auditreports/2010reports/201030104fr.html#transac tion>.
- Treleaven, Philip. “Financial Regulation of FinTech.” *Journal of Financial Perspectives: FinTech* 3, no. 3 (Winter 2015): 1–14. [https://www.ey.com/Publication/vwLU Assets/ey-financial-regulation-of-fintech/\\$FILE/ey-financial-regulation-of-fin tech.pdf](https://www.ey.com/Publication/vwLU Assets/ey-financial-regulation-of-fintech/$FILE/ey-financial-regulation-of-fin tech.pdf).
- U.S. Attorney’s Office. “Manhattan U.S. Attorney Announces Criminal Charges against U.S. Bancorp for Violations of the Bank Secrecy Act.” United States Attorney’s Office Southern District of New York, February 15, 2018. <https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-criminal-charges-against-us-bancorp-violations-bank>.
- U.S. Congress, House of Representatives. Counter Terrorism and Illicit Finance Act, H.R. 6068, 115th Cong., 2nd sess., June 12, 2018. <https://www.congress.gov/115/bills/hr6068/BILLS-115hr6068ih.pdf>.
- . Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, H. Res. 3162, 107th Cong., 1st. sess. <https://www.congress.gov/bill/107th-congress/house-bill/3162/text/enr>.
- U.S. Congress. Senate. *Combating Money Laundering and Other Forms of Illicit Finance: Regulator and Law Enforcement Perspectives on Reform: Hearing before the Committee on Banking, Housing, and Urban Affairs*. 115th Cong., 2nd sess., November 29, 2018. <https://www.banking.senate.gov/hearings/10/24/2018/combating-money-laundering-and-other-forms-of-illicit-finance-regulator-and-law-enforcement-perspectives-on-reform>.
- U.S. Government Accountability Office. *Bank Secrecy Act: Opportunities Exist for FinCEN and the Banking Regulators to Further Strengthen the Framework for Consistent BSA Oversight*. GAO-06-386. Washington, DC: U.S. Government Accountability Office, 2006. <https://www.gao.gov/assets/160/157691.pdf>.
- United States Attorney’s Office. “AlphaBay, the Largest Online ‘Dark Market,’ Shut Down.” July 20, 2017. <https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down>.
- . “Founder of Liberty Reserve Pleads Guilty to Laundering more than \$250 Million through His Digital Currency Business.” January 29, 2016. <https://www.justice.gov/opa/pr/founder-liberty-reserve-pleads-guilty-laundering-more-250-million-through-his-digital>.

- . “HSBC Holdings Plc. and HSBC Bank USA N.A. Admit to Anti-Money Laundering and Sanctions Violations, Forfeit \$1.256 Billion in Deferred Prosecution Agreement.” Department of Justice, December 11, 2012. <https://www.justice.gov/opa/pr/hsbc-holdings-plc-and-hsbc-bank-usa-na-admit-anti-money-laundering-and-sanctions-violations>.
- . “Justice Department Convenes Summit on Digital Currency and the Blockchain.” November 16, 2015. <https://www.justice.gov/usao-ndca/pr/justice-department-convenes-summit-digital-currency-and-blockchain>.
- . “Manhattan U.S. Attorney Announces Extradition of Senior Adviser to the Operator of the ‘Silk Road’ Website.” June 15, 2018. <https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-extradition-senior-adviser-operator-silk-road-website>.
- . “Operator of ‘Silk Road 2.0’ Website Charged in Manhattan Federal Court.” May 13, 2015. <https://www.justice.gov/usao-sdny/pr/operator-silk-road-20-website-charged-manhattan-federal-court>.
- . “Ross Ulbricht, The Creator and Owner of the ‘Silk Road’ Website, Found Guilty in Manhattan Federal Court on All Counts.” May 13, 2015. <https://www.justice.gov/usao-sdny/pr/ross-ulbricht-creator-and-owner-silk-road-website-found-guilty-manhattan-federal-court>.
- . “Russian National and Bitcoin Exchange Charged in 21-Count Indictment for Operating Alleged International Money Laundering Scheme and Allegedly Laundering Funds from Hack of Mt. Gox.” Department of Justice, July 26, 2017. <https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged>.
- United States Department of Labor. “CPI Inflation Calculator.” Accessed April 23, 2019. https://www.bls.gov/data/inflation_calculator.htm.
- Verafin. “Money Laundering Detection: Flow of Funds, Structuring, Funnel Accounts.” Accessed April 25, 2019. <https://verafin.com/solution/money-laundering-detection/>.
- Verret, J. W. “Terrorism Finance, Business Associations, and the ‘Incorporation Transparency Act.’” *Louisiana Law Review* 70, no. 3 (2010): 857–910. <https://digitalcommons.law.lsu.edu/lalrev/vol70/iss3/5/>.
- Wall Street Journal*. “Bank Secrecy Act Found to Violate Right of Privacy: Court Rules Unconstitutional Part Requiring Reports of Activity in U.S. Accounts Other Sections Are Upheld.” September 12, 1972.

——— “House to Act on Bank Bill | Wells Fargo’s 401(k) Practices Probed | Hayashi’s Take: States Try to Protect CFPB’s Investigative Power.” April 27, 2018. <https://www.wsj.com/articles/house-to-act-on-bank-bill-wells-fargos-401-k-practices-probed-hayashis-take-states-try-to-protect-cfpbs-investigative-power-1524825203>.

Wedge, Roy, James Max Kanter, Veeramachaneni Kalyan, Santiago Moral Rubio, and Sergio Iglesias Perez. *Solving the False Positives Problem in Fraud Prediction Using Automated Feature Engineering*. Dublin, Ireland: European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases, 2018. <http://www.ecmlpkdd2018.org/wp-content/uploads/2018/09/567.pdf>.

White, Trevor, Mark Anderson, and Didier Lavion. *Adjusting the Lens on Economic Crime*. PwC US, 2016.

Wojciechowska, Iza. “What Is KYC and Why Does It Matter?.” *Fin*, April 5, 2017. <http://fin.plaid.com/articles/kyc-basics>.

Yu, Yi, Jingsha He, Nafei Zhu, Fangbo Cai, and Muhammad Salman Pathan. “A New Method for Identity Authentication Using Mobile Terminals.” *Procedia Computer Science* 131 (2018): 771–78. <https://doi.org/10.1016/j.procs.2018.04.323>.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California