Article

FinTech Innovation and Anti-Money Laundering Compliance

Yen-Te Wu*

ABSTRACT

The rapid emergence and growth of the financial innovations industry--or FinTech as it is commonly referred to in the financial services sector--has caught many players in the global financial services industry unaware. This article analyzed the compliance of FinTech firms with anti-money laundering (AML) laws in the US. The results of the study suggest that two main laws govern issues related to the laundering of monetary instruments. These laws are the Bank Secrecy Act of 1970 (BSA) and the Organized Crime Control Act. The BSA is the primary legislation on issues related to the laundering of money. The legislation outlines the rules that banks and other financial services institutions must follow to ensure that their services are compliant with AML laws. The Organized Crime Control Act merely defines the crime of laundering in financial instruments. Furthermore, the results of the analysis state that FinTech corporations are not complying with AML laws. The results indicate that most FinTech firms do not consider themselves as financial services organizations. In fact, their business models are inconsistent with existing AML provisions. This reluctance to comply with AML laws has exposed them to suits, with the available data indicating that some founders have been received 20-year jail terms because of their failure to comply with AML provisions.

DOI：10.3966/181263242017091202002

* Associate Professor, Chinese Culture University College of Law; J.D., Washington University School of Law, U.S.A. The author wishes to express his deepest gratitude for the comments by two anonymous reviewers. All errors naturally remain the authors' own. E-mail: wyd2@ulive.pccu.edu.tw.

In the end, the concept of regulatory requirements will be explained as the conclusion.

Keywords: *FinTech, Anti-Money Laundering Laws, Bank Secrecy Act, Organized Crime Control Act, AML Compliance*

CONTENTS

I. INTRODUCTION

In the past century, leading companies in the global financial services sector maintained a tight grip on their respective market shares through their swift adoption of new technologies and the quick adaptation of their services to new technologies. In 1967, Barclays Bank Plc underlined its competitiveness by becoming the first company in the world to roll out the automated teller machine (ATMs) in its UK branches.[1] In 1965, Bank of America became the first company in the financial services industry to implement the credit card system when it purchased IBM's magnetic-stripe plastic cards and issued them to its customers, thereby marking the bank's entry into electronic banking.[2] In 1987, the UK-based Co-operative Bank Group spearheaded the move towards online banking when it collaborated with LINK Group and IBM to set up an online banking platform for its customers.[3] This swift adoption of financial technology innovations not only spurred the growth of the financial services sector, but it also proved pivotal in enabling the leading companies to expand their share of the global financial services market in the past century.

However, the recent emergence of the crop of financial technology start-ups is threatening to curtail these companies' share of the global financial services market. The new crop of financial technology startups--known widely as FinTech or financial innovations technology—is causing disruption in the industry in the speed with which they are adapting their services to new technologies and creating new technologies for the delivery of financial services.[4] The FinTech startups have used the new technologies they have adapted to and developed, for delivering a wide variety of services that target the traditional customer bases of leading banks as well as customer bases that were out of the reach of traditional banks.[5] The startups have caused ripples in the global financial services sector by a wide category of services that range from services offered by traditional banks like online banking, deposit taking, and funds transfer to a new category of services like peer-to-peer lending, big data, mobile banking,

1. *See* Bernardo Batiz-Lazo & Douglas Wood, *Diffusion of Information Technology Innovations within Retail Banking: An Historical Review*, *in* IT-BASED MANAGEMENT: CHALLENGES AND SOLUTIONS 235 (Luiz Antonio Joia ed., 2002).

2. *Id*.

3. *See* Xianzhong Mark Xu, Yanqing Duan & Yu Li, *IT-Enabled Strategic Marketing Management, in IT-Based Management: Challenges and Solutions*, *in* IT-BASED MANAGEMENT: CHALLENGES AND SOLUTIONS, *supra* note 1, at 217.

4. *See* Paolo Sironi, *My Robo Advisor Was an iPod-Applying the Lessons from Other Sectors to FinTech Disruption*, *in* THE FINTECH BOOK: THE FINANCIAL TECHNOLOGY HANDBOOK FOR INVESTORS, ENTREPRENEURS AND VISIONARIES 152, 152-54 (Susanne Chishti & Janos Barberis eds., 2016).

5. *Id*.

mobile payments, and distributed ledger technology.

The online lending market place is one of the areas where FinTech startups are exhibiting success in their quest to wrestle control over a market that consists largely of young adults and individuals who cannot secure loans in traditional banks. In the online lending market sphere, the FinTech have caused disruption by providing credit to borrowers at a faster rate than the face-to-face process utilized in traditional banks. The FinTech startups' automation of the credit risk analysis concept and their extensive use of electronic data have proved effective in enabling them to simplify the loan approval process for small loans from 72 hours to less than three minutes.[6] This innovation has created instability among leading companies in the financial services industry, as leading banks begin to grapple with the possibility that FinTech startups might take their share of the global financial services sector.

Indeed, findings from recently published studies indicate that the disruption in the financial services sector is widespread. Many organizations and scholars have conducted studies on the impact of FinTech on the market share of traditional banks and their consensus is that FinTech are becoming a force to reckon with in the countries where they have a strong presence. In fact, data from recent studies indicate that the disruption is so significant that a large percentage of financial services investments are now going to FinTech startups. Figures indicate that investment funds dedicated to the financing of firms global FinTech industry increased from $1 billion in 2008 to $3 billion in 2013.[7] The statistics suggest that North American FinTech companies took up the lion's share of the investor funds.[8] In 2008, FinTech firms in the US took up more than $900 million of the more than $1 billion that investors spent in financing firms in the global FinTech industry.[9] In 2013, US FinTech firms took up more than $2.3 billion of the $3.2 billion that venture capital companies expended in financing firms in the FinTech subsector.[10] Statistics from a study published in 2014 indicate that the global investments in the FinTech subsector spiked from $3 billion in 2013 to $12 billion in 2014, representing a more than 200% rise in investments into the subsector.[11] The statistics suggest that conventional banks were at the heart of the investments, with the conventional banking sector contributing $2

6. *See* U.S. DEPARTMENT OF THE TREASURY, OPPORTUNITIES AND CHALLENGES IN ONLINE MARKETPLACE LENDING 5-6 (2016).

7. *See* INFORMATION VENTURES PARTNERS, DISRUPTIONS DRIVING FINTECH INVESTING 1-5 (2014).

8. *Id.*

9. *Id.*

10. *Id.*

11. *See* John L. Douglas, *New Wine into Old Bottles: Fintech Meets the Bank Regulatory World*, 20 N.C. BANKING INST. 17, 17-65 (2016), http://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1391&context=ncbi.

billion of the $12 billion that investors expended in financing FinTech startups.[12] These statistics suggest that there is widespread disruption in the global FinTech subsector. They indicate that the disruptions are fueling venture capitalists' investment into FinTech firms.

Studies in regions like the EU and individual countries like Canada and the UK have confirmed that FinTech firms have witnessed significant growth because of innovations and massive injection of funds by venture capitalists. In Canada, FinTech firms have witnessed significant growth in the past decade, with statistics indicating their technology expenditure now accounts for a significant chunk of the money expended on financial innovation technologies in the country's financial services sector. McMillan LLC argues that FinTech startups spent a significant percentage of the Cdn $14.8 billion that companies in the country's financial services sector invested on new technologies.[13] In the UK and the EU, FinTech firms have recorded massive spikes in their revenue against the backdrop of regulatory support from the EU legislature and individual governments in the UK and other countries in the EU. Statistics from the UK suggests that FinTech subsector is now generating more than £20 billion in annual revenues.[14] This growth in revenue is coming against the backdrop of regulatory support from the UK government, the UK legislature, and the EU. The UK government, the EU legislature, and the UK legislature have supported the growth of FinTech firms by enacting laws and implementing policies that enhance their ability to compete with banks. Prior to the Brexit vote, the EU legislature demonstrated its support for FinTech firms in the EU by enacting the Revised Payment Services Directive.[15] The objective of this directive was to spur growth in the FinTech subsector by compelling leading financial services institutions and incumbent FinTech firms to share data with FinTech startups.[16] Drafters of the legislation believed that this move would enhance competitiveness in the financial innovations technology subsector, thereby paving way for improvements in the quality of services that FinTech firms are delivering to their customers.[17] In the same vein, the UK government implemented the Open Banking Working Group program to encourage players in the financial services industry to develop avenues for the

12. *Id*.

13. *See* MCMILLAN LLP, FINTECH AT THE CROSSROADS: REGULATING THE REVOLUTION 1-2 (2016), http://www.mcmillan.ca/Files/191422_Fintech%20at%20the%20Crossroads%20-%20Regulating%20the%20Revolution.pdf.

14. *See* FINEXTRA RESEARCH LTD., A ROADMAP FOR FINTECH STANDARDS: EXECUTIVE REPORT 3-4 (2016), https://www.bsigroup.com/LocalFiles/en-GB/PAS/Homepage/FIN_BSI_short_final.pdf.

15. *Id*.

16. *Id*.

17. *Id*.

exchange of data.[18] Policymakers in the UK government believed that this would be an effective approach to spur growth in the FinTech subsector.

While the reviewed data suggests that banks are shouldering a disproportionate burden of the speedy growth of FinTech firms, the reality is that they are not the only stakeholders in the financial services industry who are experiencing difficulties in coping with this rapid FinTech growth. An analysis of recent publications on the growth of FinTech firms and the controversies surrounding their growth suggests that regulatory agencies are among the stakeholders who struggle to make sense of FinTech firms growth. At the heart of the struggles are concerns about whether FinTech firms are subject to the same anti-money laundering laws (AMLs) that govern banks and other traditional players in the financial services sector.[19] On the one hand, one group of scholars argues that FinTech firms are outside the purview of existing AMLs because they are not subject to the same financial reporting rules as conventional banks and other players in the financial services sector.[20] On the other hand, the second group of scholars asserts that FinTech firms are outside the scope of the rules established to regulate the conduct of conventional banks.[21] They contend that subjecting FinTech firms to those stringent rules will lead to the collapse of most of those companies.

This is not the first time that regulatory agencies in the financial services grapple with the problem in identifying the legal provisions that regulate nonbank competitors. The regulators faced the same challenge when Western Union launched its telegraph-based money transfer business in 1861. More recently, the regulators faced questions on the regulations applicable to CheckFreePay and PayPal when the two companies ventured into the business of online money transfer and online bill payment. Further, regulatory agencies in the financial services industry faced the same questions on the legal rules applicable to NetSpend, InComm, and GreenDot when the three companies launched prepaid card services that customers with limited access to conventional banks used as convenient substitutes for debit cards and bank deposits.[22] The entry of these companies posed serious problems to regulatory agencies, but they weathered the storm by developing policies and rules that offered the nonbank competitors acceptable

18. *Id*.

19. *See* Jodi Avergun & Colleen Kukowski, C*omplying with AML Laws: Challenges for the Fintech Industry*, CROWDFUND INSIDER (Apr. 5, 2016), http://www.crowdfundinsider.com/2016/04/83845-complying-with-aml-laws-challenges-for-the-fintech-industry/.

20. Sironi, *supra* note 4, at 153-54.

21. *See* JIM SIVON, FINTECH AND THE EXISTING LEGAL FRAMEWORK FOR ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING 1-4 (2015), http://www.bsnlawfirm.com/newsletter/OP1506_Sivon.pdf.

22. FINEXTRA RESEARCH LTD., *supra* note 14, at 12.

accommodations within the traditional regulatory frameworks developed for banks.[23] For instance, PayPal managed to fit its services within the regulatory framework by entering into agreements with regulatory agencies - meaning providing the permission of PayPal to obtain money transfer licenses on a state-by-state basis.[24] GreenDot followed suit and entered into an agreement that permitted it to operate as a member bank of the Federal Reserve.[25] These accommodations permitted regulatory agencies to bring the nonbank competitors into the ambit of the regulations developed for conventional banks, which avoided their own regulatory questions.

Despite the regulators' extensive experience in developing acceptable regulation for nonbank competitors, an analysis of the interaction between FinTech firms and regulatory agencies suggests that these firms are posing a unique challenge to regulators. The development of FinTech firms is coming at a time when financial services sector is still reeling from the adverse effects of the global financial crisis from 2008's housing collapse. This has led policymakers and industry players to argue that there is need for regulators to implement laws that encourage, rather than hinder, the growth of the FinTech sector.[26] The policymakers argue that subjecting FinTech startups and FinTech incumbents to regulatory provisions developed for conventional banks will only serve to undermine the long-term growth prospects of the industry.[27] In addition to concerns about the impact of the laws on the growth of the industry, the clash between FinTech firms' use of new technology on delivering services that have been in the purview of conventional banks and the laws developed to regulate conventional laws has created a unique challenge to regulators. It has led many regulators to wonder whether the FinTech firms are banks within the strict meaning of the term. It has also led the regulatory agencies to wonder whether the peer-to-peer loans or securities as FinTech firms' call them fall within the ambit of statutes developed to regulate the services of conventional banks.

In this article, the author will evaluate FinTech firms' compliance with anti-money laundering laws. In conducting this evaluation, the author will carry out four critical analyses. Firstly, the author will analyze the services that FinTech firms are offering to their target customers. In particular, the author will evaluate how the services of FinTech firms touches on the business of deposit taking, which happens when the firms hold their customers' funds as they await their transfer from one location to another. Secondly, the author will take the analysis a step further by analyzing the

23. *Id.*
24. *Id.*
25. *Id.*
26. *See* U.S. DEPARTMENT OF THE TREASURY, *supra* note 6, at 26-27.
27. *Id.*

thicket of legislations that FinTech firms will run into in their quest to deliver services that were traditionally within the ambit of conventional banks. Thirdly, the author will go into an intensive and extensive analysis of how the money transmission services comply with AML regulations, the Bank Secrecy Act, and other laws developed to prevent financial services institutions from engaging in money laundering. Finally, the author will evaluate some of the regulatory problems FinTech firms might face when they decide to deliver money transmission services for their customers without a thorough consideration of the compliance rules enshrined under existing AMLs.

II. THE TECH REVOLUTION FOR FINANCIAL SERVICES

A. *Financial Services*

The division between the services offered by FinTech firms and the services offered by traditional banks is not clear-cut. Therefore, there is a risk that FinTech firms may inadvertently infringe upon the AMLs developed to regulate the service of conventional banks as they are delivering services to their customers. This risk implies that there is need to evaluate the services that FinTech firms are offering their customers, and identify way in which such services may infringe on existing banking laws.

An analysis of the services that FinTech firms offer suggests that they are offering a diverse range of services. These services include robo-advice services, crowdfunding services, big data services, online banking services, peer-to-peer lending services, mobile payment services, digital wallet services, and distributed ledger services. Unsworth and Antoniades categorize these services into four.[28] These four categories include core financial applications, financial data applications, financial security applications, payment applications, and capital markets applications.[29] The core financial applications denote the services that were within the traditional ambit of banking services. In addition, 21% of these services are offered by FinTech firms that include deposit taking, peer-to-peer lending, money transfer, and online banking.[30] FinTech firms have developed technologies that can expand these core financial services and enhance the degree of efficiency in the delivery of the services.

The financial scope that FinTech covered has principally transformed the industry, the companies have developed applications that created massive shifts that not only affect the operation of already established monetary

28. *See* INFORMATION VENTURES PARTNERS, *supra* note 7, at 11-12.
29. *Id.*
30. *Id.*

business, but also in the ways customers handle their finances. These four core financial applications could very well shape the future of the banking industry in ways none could understand now due to the emergence of these FinTech startups and their overall influence on other financial realities. The scope and overall impact of how these developing companies operate has not yet been truly discovered; however, it is possible, as displayed by this article that according to many trends in the industry the breadth of their power will only increase in time.

Other categories of services are the financial security applications, the financial data applications, the capital markets applications, and the payment applications. The financial security services encompasses the services related to the analysis of people's credit risk as well as the services related to the protection of financial services companies against fraud and other forms of criminal attacks.[31] Financial data applications consist of the FinTech firms that specialize in the development of analytics platforms that assist financial services companies in analyzing big data and making appropriate strategic decisions.[32] Capital markets services denote the category of FinTech firms that have developed technologies that permit consumers to invest in stock markets and money markets. The payments category consists of the FinTech firms that have developed technologies, and allow their customers to use their smartphones as the conduit for paying bills and purchasing goods.[33] FinTech firms whose services fall into the payment services category have experienced the greatest growth as more and more consumers seek their services.[34] In fact, data indicates that payment services account for 44% of the services offered by FinTech companies.[35] This is where the money laundering implications are most obvious.

These categorizations also support the view that FinTech services are diverse, but most of them have a strong connection to the services rendered by traditional banks. Indeed, services under the payment applications category, the core financial services category, and the capital markets category are services that one can categorize as the services that conventional banks have been rendering to their customers. Banks have been offering capital markets services, payment services, and core banking services prior to the entry of FinTech firms into the financial services sector. However, the issue that differentiates these services from the services offered in conventional banks is the fact that technology trends (rather than financial services trends) are the primary factors that spurred the FinTech firms to

31. *Id.* at 11.
32. *Id.* at 12.
33. *Id.* at 13.
34. *Id.*
35. *Id.*

develop those services.[36] FinTech firms used advancements in smartphone technology, block chains, artificial intelligence, distributed ledger technology, natural voice innovation technology, big data, and other ICT technologies to fuel their entry into the global financial services industry.[37] In contrast, the financial motives are the primary factor behind the entry of conventional banks into the financial services sector.

Despite the stated services, there are services that FinTech firms provide by default. One of these services is deposit taking. FinTech firms engage in deposit taking during the periods when they retain their customers' money for purposes of onward transfer. Similarly, FinTech firms that offer prepaid card services engage in the business of deposit taking when their customers decide to retain money in their respective cards. In all these situations, the FinTech companies are engaging in the business of deposit taking by default.[38] Generally speaking this is outside the normal flow of banking operations and thus open to various negative consequences. For example, this outcome places regulatory agencies in a difficult situation because FinTech companies regard themselves as nonbank competitors and, as such, they believe they are outside the scope of laws developed to regulate traditional banks.[39] Section 24 of the National Bank Act states that banks are the only institutions authorized to engage in the business of deposit taking. By permitting their customers to use their services as a convenient substitute for conventional banks, the FinTech companies are violating the laws.

Nonetheless, FinTech firms can argue that the decision to use their services as a convenient substitution for conventional banks is their customers' decision. Therefore, it is unfair for regulatory agencies to punish them for their customers' decision. This legal difficulty highlights some of the challenges that regulatory agencies and FinTech firms face whenever they run into the statutes that regulate the services of conventional banks. In the next section of the article, the author will evaluate the laws regulating the financial services sector. In the course of the analysis, the author will evaluate the controversies arising from the application of those laws to FinTech firms. These are important for a variety of reasons, not the least of which is that with all newly established or emerging industries there is a need for creating regulatory enterprises for legal purposes. Many of the current laws are not sufficient for the creation of these legally mandated necessities, due to the fact that many FinTech related applications are simply

---

36. *See* Ann S. Barefoot, *Letter of Comment: White Paper on Responsible Innovation*, JO ANN BAREFOOT GROUP LLC 2-3 (2016), https://www.occ.gov/topics/responsible-innovation/comments/comment-circle-financial.pdf.

37. *Id*. at 5.

38. *Id*.

39. *Id*.

too new and without precedence. They are, in fact, creating new modes of money transfer, with various industry specific hazards as a result.

B. *Regulation Technology*

The Financial Conduct Authority (FCA), a regulatory body in the United Kingdom, describes RegTech as the adoption of new technologies to facilitate the delivery of regulatory requirements.[40] Regulation technology, or RegTech, is defined as any technological innovation that helps improve efficiency, transparency and adherence to regulation. RegTech has emerged as a result of the growing need for more effective and efficient methods for businesses, both traditional and startup, to stay compliant in industries facing increased regulatory protocols and complex regulatory transitions.[41] RegTech to date has been focused on the digitization of manual reporting and compliance processes, for example in the context of know-your-customer requirements. This offers tremendous cost savings to the financial services industry and regulators. However, the potential of RegTech is far greater--it has the potential to enable a close-to-real-time proportionate regulatory regime that identifies and addresses risk while also facilitating far more efficient regulatory compliance.[42]

The emergence of RegTech is attributable to: (1) post-crisis regulation changes requiring massive additional data disclosure from supervised entities;[43] (2) developments in data science (for instance artificial intelligence ('AI') and deep learning), which allow the structuring of unstructured data;[44] (3) economic incentives for participants to minimize rapidly rising compliance costs; and (4) regulators' efforts to enhance the efficiency of supervisory tools to foster competition and uphold their mandates of financial stability (both macro and micro) and market integrity.[45]

---

40. FINANCIAL CONDUCT AUTHORITY, CALL FOR INPUT ON SUPPORTING THE DEVELOPMENT AND ADOPTERS OF REGTECH 11-14 (2016), https://www.fca.org.uk/publication/feedback/fs-16-04.pdf.

41. BURGES SALMON LLP, SUPPORTING THE DEVELOPMENT AND ADOPTION OF REGTECH: NO BETTER TIME FOR A CALL FOR INPUT 1-2 (2016), https://www.burges-salmon.com/-/media/files/publications/open-access/supporting_the_development_and_adoption_of_regtech_no_better_time_for_a_call_for_input.pdf.

42. Daniel Gutierrez, *Big Data for Finance-Security and Regulatory Compliance Considerations*, INSIDEBIGDATA (Oct. 20, 2014), http://insidebigdata.com/2014/10/20/big-data-finance-security-regulatory-compliance-considerations/.

43. *See* INSTITUTE OF INTERNATIONAL FINANCE, REGTECH IN FINANCIAL SERVICES: TECHNOLOGY SOLUTIONS FOR COMPLIANCE AND REPORTING 5-8 (2016).

44. *See id*. at 12-14. The IIF identified a number of new technologies that could improve data management and analysis which include new cryptographic technology, data mining algorithms, machine learning, blockchain, robotics and visual analytics.

45. *See* BASEL COMMITTEE ON BANKING SUPERVISION, CORE PRINCIPLES FOR EFFECTIVE BANKING SUPERVISION 30-31 (2012). For example, Principle 9 of the BCBS "Core Principles for Effective Banking Supervision" requires financial supervisors to use an appropriate range of techniques and tools to effectively implement the supervisory approach and deploy supervisory

The emergence of RegTech can be largely attributed to the complex, fragmented and ever-evolving post-GFC global financial regulatory regime. Over-reliance on complex, prescriptive and lengthy post-GFC regulations led to massive compliance and supervision costs for the regulated and the regulators. Carrying out financial supervision, in response to the growing level of regulatory complexity, inevitably required greater granularity, precision and frequency in data reporting, aggregation, and analysis.[46] Compliance costs rose significantly as a result of the increasing regulatory burden, which made the use of innovative technologies as natural and promising solution to compliance requirements.[47]

C. *New Payment Intermediary*

As surging number of online businesses turn to the new kind of transaction like online auctions, inevitably, it provides a new environment for payment systems on the internet in order to serve with the nature of this online auction transaction. From this point, there are three distinctive elements of the online auction that encourages development of a new payment intermediary. The first element is the need of a consumer to conclude the contract immediately. In other words, the nature of the online auction is fast product purchasing. Sellers need the payment immediately and buyers also want the goods to arrive at their premise as soon as possible. Another element is the participant of the online auction. As we can perceive, the online auction always consists of small businesses or individuals that are selling or purchasing. This makes transactions vulnerable to traditional.

The payment method like credit cards because the individual seller or small companies are not able to accept credit cards.[48] The last element is that the online auction usually does not require buyers and sellers to have any sort of prior relationship between each other.[49] With this element, other traditional methods of payment like money or cheque seems impossible because they cannot determine the reliability or even identify one another.[50] Even with credit card payments the seller, of course, is unlikely to accept the

---

resources. This includes a criteria that "[t]he supervisor uses a variety of tools to regularly review and assess the safety and soundness of banks and the banking system."

46. *See* INSTITUTE OF INTERNATIONAL FINANCE, *supra* note 43, at 16-19.

47. James Eyers, *Welcome to the New World of 'RegTech'*, FINANCIAL REVIEW (June 20, 2016), http://www.afr.com/technology/welcome-to-the-new-world-of-regtech-20160619-gpmj6k.

48. Carl Kaminski, *Online Peer-to-Peer Payments: PayPal Primes the Pump, Will Banks Follow?*, 7 N.C. BANKING INST. 375, 378-85 (2003).

49. Jeffrey P. Taft, *Internet-Based Payment Systems: An Overview of the Regulatory and Compliance Issues*, 56 CONSUMER FIN. L. Q. REP. 42, 42-47 (2002).

50. Andrés G. González, *PayPal: the Legal Status of C2C Payment Systems*, 20 COMPUTER L. & SEC. REV. 293 (2004).

credit card from the one whose financial status is unknown.[51]

In response to the distinctive nature of online auctions, there is great number of effort in creating new internet-based payment mechanisms to deal with it. The first attempt can be seen in the non-bank service providers such as DigiCash BC (DigiCash) and First Virtual holding Inc. (First Virtual), these non-bank services introduce the new payment option to the internet user by offering a new micro payment system.[52] An example is DigiCash. This system is motivated mostly by providing anonymity based on cryptography, in particular blind signatures. The result is a very complex system that has deficiencies in scaling and, possibly, performance. A special software called 'Cyberwallet' is required on the buyers machine to handle payments. After withdrawing digital coins from the digital token issuing currency server, the user can buy goods by visiting virtual web stores accepting DigiCash. A good is represented by an URL, by clicking on it the user gives his intention to buy. The http-server at the payee starts via the Common Gateway Interface (CGI) the program "Merchant". It receives the location of the request and sends a payment request to the Cyberwallet program of the buyer, which replies with sending the digital coins. To protect from double spending the merchant needs to contact the currency server. At the currency server the serial number of the forwarded coins is compared to a large database of all spent coins. When the coins are valid, the Merchant software sends a receipt for the successful payment to the buyer. Now the goods can be transmitted to the buyer.[53] However, those efforts have disappeared after failing to gain sufficient acceptance. For instance DigiCash was filed lawsuit for bankruptcy under Chapter 11.[54] The successful attempt was clearly seen in the introduction of the company in 1998 called PayPal. PayPal is often called "e-mail money" or peer-to-peer payment (P2P).[55]

First Virtual is using the telephone to transmit credit card information for the registration of buyers. When registered, the payment transactions are authenticated by an identification number. At First Virtual they are called Virtual PIN.[56] In a business transaction the buyer clicks on a web-page

51. *Id.*

52. *See* Sarah J. Hughes, *A Call for International Legal Standards for Emerging Retail Electronic Payment Systems*, 15 ANN. REV. BANKING L. 197, 206 (1996). First Virtual offer to prospect purchaser from the Internet vendors a trusted third-party, escrow-like security for their credit card number. The customer uses the First virtual account number instead of their credit card number in the online-transaction and First Virtual Charge the Customer's credit cards account for Authorization, DigiCash offer the potential Internet purchaser buy their electronic coins and pay for then by downloading value from their electronic wallet.

53. MICHAEL PEIRCE & DONAL O'MAHONY, SCALABLE, SECURE CASH PAYMENT FOR WWW RESOURCES WITH THE PAYME PROTOCOL SET 2-4 (2007).

54. *DigiCash Files Chapter 11*, CNET NEWS.COM, https://www.cnet.com/news/digicash-files-chapter-11/ (last visited Jan. 3, 2017).

55. *See* González, *supra* note 50.

56. RAVI KALAKOTA & ANDREW B. WHINSTON, FRONTIERS OF ELECTRONIC COMMERCE (1999).

accepting payments using the First Virtual payment method. The merchant sends the Virtual PIN of the buyer and his own to the payment server of First Virtual.[57] On receipt of the sellers' transaction request, First Virtual sends an e-mail to the buyer to let him confirm the order. After confirmation the credit card transaction will be processed on secure conventional financial networks. Note that different from other payment systems, the transaction will only be conducted if the customer explicitly confirms by an e-mail to First Virtual. Some anonymity is provided to the buyer by allowing nicknames.[58] The seller will not get the identity of the buyer. The bank, however, has to know the identity for the confirmation and thus can observe buying habits. Peer-to-peer payments are possible with this kind of third-party processor. The current implementation of First Virtual is not supporting peer-to-peer payments.

III. LAWS REGULATING THE FINANCIAL SERVICES SECTOR

A. *Laws Regulating Deposit Taking*

The National Bank Act[59] is one of the laws regulating deposit taking in the financial services sector in the US. Section 24 of the legislation states that banks are the only institutions in the country authorized to engage in the business of deposit taking. State laws affirm the exclusive responsibility of banks in deposit taking by stating that chartered commercial banks are the only institutions that can accept customer deposits. The state laws expressly exclude other institutions or businesses from taking deposits from customers. The New York Banking Law offers an illustration of the legal position on issues of deposit taking under state law. Section 96 of the New York Banking Law states that chartered banks are the only institutions that can receive deposits. Similarly, section 31 of the Texas Finance Code offers a definition of banks that underlines their exclusive role in receiving deposits from customers.[60] The Texan law states that banking entails the activities of activing deposits from customers. This definition suggests that the state's regulatory agencies will categorize all institutions that are taking deposits from customers as banks. This categorization will permit the regulatory agencies to assess the activities of the companies to determine whether they have met the qualifications to operate as banks. Further, the Federal Deposit Insurance Corporation (FDIC) rules confirm that deposit taking is the

57. *Id.*
58. *Id.*
59. The usury provisions of the National Bank Act are 12 U.S.C. §§ 85-86 (1964).
60. *See* Texas Financial Code § 393.222 (2005).

exclusive domain of banks.[61] The regulations define deposit as money held in money market deposit accounts, savings account, checking account, and negotiable order of withdrawal (NOW) account. Again, this definition suggests that banks are the only institutions in the US authorized to engage in the business of deposit taking either by default or by design.

However, an analysis on the services from FinTech firms suggests that there are periods when they are engaging in the business of deposit taking, which itself alone would indicate greater regulation is needed to oversee these occurrences. This is the case in incidents where customers decide to use the prepaid cards as convenient substitutes for conventional banks. It also transpires in instances where the FinTech firms retain customer funds in the process of transferring it.[62] In all these situations, the FinTech banks are engaging in the business of taking deposits.[63] Given that the existing laws indicate that bank are the only firms authorized to engage in the business of deposit taking, one can argue the FinTech firm's practice of retaining money violates the laws regulating the financial services sector. As noted earlier, FinTech firms can claim that they are not aware of their customers' decision use prepaid cards as a substitute for the deposit taking services offered in conventional banks. This is an example of a company taking a specific stance on an issue that would normally involve legalities such as banking laws; and also demonstrates the need for further investigation on whether or not these newly established institutions require a deeper overview in order to determine their specific legal framework within current principles.

A deeper investigation of state laws offer further confirmation that banks are the only institutions authorized to engage in the business of deposit taking. Title 7 of the Georgia Code states that banks are the only entities authorized to engage in the business of deposit taking, withdrawal of deposits on demand, and withdrawal of deposits within a predetermined timeframe.[64] The Georgia statute provides conclusive proof by baring individuals and corporations from engaging in the business of receiving money for transfer or deposit. The section states that the only institutions allowed to perform these banking practices are credit unions, building and loan associations, international banking agency, or savings and loan associations.[65] This provision suggests that FinTech firms that offer services like deposit taking will violate Georgia law if they do not have the requisite license.

---

61. *See* FDIC: FEDERAL DEPOSIT INSURANCE CORPORATION, https://www.fdic.gov/ (last visited Jan. 4, 2017).

62. *See* Douglas, *supra* note 11, at 25-26.

63. *Id.*

64. Amend Title 7 of the Official Code of Georgia Annotated, Relating to Banking and Finance, so as to Provide for Licensing of Persons Who Provide Deferred Presentment Services.

65. *Id.*

The reviewed laws suggest that FinTech firms that offer services related to payment, money transfer, and core financial services will encounter these legislations. The legislations indicate that these services are under the exclusive domain of banks and, as such, the only way that nonbank competitors can comply with the legislations is by seeking licenses that will allow them to operate as banks. In fact, the Georgia law has stringent provisions that make it unlawful for FinTech firms and other nonbank competitors to engage in the business of taking customers' money for deposit or transmission. This factor explains why companies like PayPal and GreenDot entered into agreements with state governments that allowed them to operate in those states as banks. Operating as banks allowed them to continue deliver services offered by conventional banks without the fear of offending against laws established to the conduct of conventional banks. Obviously all FinTech or similar types of banking services should also do the same in order to comply with the law.

However, PayPal's decision to apply for a banking license does not protect FinTech firms from the legal controversies that arise from their decision to perform functions traditionally performed by banks and other licensed institutions in the financial services sector. FinTech firms like NetSpend, InComm, and GreenDot engage in services that are so diverse that it might be difficult for its founders and shareholders to appreciate the legal consequences that arise from its decision to undertake those services. For instances, the three companies' reliance on prepaid cards might lead regulators to ask questions about the applicability to banking laws and regulations to their transactions.[66] Such as, for instance, when consumers are loading funds into their NetSpend, InComm, and GreenDot prepaid cards regulators will ask themselves whether those funds automatically become deposits and the FinTech companies' actions amount to deposit taking. Similarly, the regulators will ask themselves whether people's use of iPhones to deposit funds into their credit cards or bank accounts amounts to a deposit when the entity in question holds the funds for a few seconds or minutes as it verifies the sender's details.[67] Therefore, there are obviously great deals of instances within this new paradigm of online banking that require overview, possibly regulation, and at the very least a deeper examination of what possible pratfalls might occur.

However, another contentious point is that regulators' categorization of these transactions as deposits means that they are subject to the safeguards enshrined under the Federal Deposit Insurance Corporation law. Section

66. *See* Douglas, *supra* note 11, at 21.

67. *See* PRICEWATERHOUSECOOPERS, PEER PRESSURE: HOW PEER-TO-PEER LENDING PLATFORMS ARE TRANSFORMING THE CONSUMER LENDING INDUSTRY 13-14 (2015), http://www.pwc.com/us/en/consumer-finance/publications/assets/peer-to-peer-lending.pdf.

1813(m)(l) of the Federal Deposit Insurance Act[68] establishes the FDIC and insures the deposits that customers have given banks. Therefore, the categorization of the funds sent to FinTech firms as deposits means that they would qualify for insurance under the Federal Deposit Insurance Act. These legal issues arise in the interaction between FinTech firms and the laws developed to regulate the conduct of firms in the financial services industry.

B. *Lending Laws*

Lending laws provide further illustration on the legal hurdles FinTech firms will encounter while engaging in the business of providing peer-to-peer lending services to their customers. Statistics indicate that the practice of peer-to-peer lending among FinTech firms is on the rise. According to recent statistics, FinTech peer-to-peer lenders like SoFi, Lending Club, and Prosper are some of the leading FinTech firms in the peer-to-peer lending business.[69] The statistics suggest that these companies issued more than $5.5 billion in loans in 2014, with forecasts indicating that the total amount expended on peer-to-peer lending services expected to exceed $150 billion by 2025.[70] In the course of performing their peer-to-peer lending services, the companies differentiate themselves from conventional banks and lending companies in the manner in which technology plays a significant role in enabling the companies to identify lenders. The companies use complex proprietary algorithms, sources of online data, and other financial technology innovations. This demonstrates the sheer complexity of the issue at hand, as well as the importance of keeping tabs on what they new companies are doing in regards to lending situations.

While the amount of money that these FinTech firms are lending out as loans is increasing and attempts to differentiate their services have been successful, the FinTech firms have not achieved significant success in their quest to circumvent legal hurdles. These firms have experienced challenges in responding to legal hurdles arising from the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, the Real Estate Settlement Procedures Act, the Fair Housing Act, and the Equal Credit Opportunity Act. Many have argued that these laws apply to FinTech firms engaging in the business of peer-to-peer lending because they regulate the character of the activity the company engages in rather than the character of the company.[71] However, they have experienced challenges in explaining whether the fees and

68. *Id.*
69. *See* Douglas, *supra* note 11, at 26-27.
70. *Id.*
71. *Id.*

interests that Fintech firms levy to their customers are subject to the Federal cap on interests on loans. Regulatory agencies at the state level have also encountered challenges in their quest to explain how the state usury caps apply to FinTech firms that engage in peer-to-peer lending.

This is generally a good situation to be in to protect consumers, yet the greater challenges lay ahead. Indeed, various cases have demonstrated the types of challenges FinTech firms will experience in their quest to deliver their peer-to-peer lending services. In *CashCall Inc. v. Morrissey*,[72] the Virginia Supreme Court of Appeals handled a case where a FinTech firm faced a challenge regarding its lending activities. *CashCall*, a peer-to-peer lending firm from California, had partnered with a bank South Dakota and began providing small, but high-interest unsecured loans to customers in different states around the US, including Virginia. The attorney general in West Virginia argued that the FinTech firms lending practices amounted to nothing more than a "rent-a-bank program" targeted at circumventing consumer protection legislations and State usury statutes.[73] The appeal court in West Virginia made a ruling in support of the attorney general's arguments. The court argued that the FinTech firm's money lending activities violated the West Virginia Credit Protection Act.[74] This ruling demonstrated the challenges that FinTech firms pose to the laws enacted to regulate conventional banks. Their practice goes outside the boundaries of those laws, thereby undermining the ability of regulatory agencies to determine whether existing banking laws are applicable to them. Online transactions are by nature outside normal, and different from the already established banking industry or specific money based situations most people are familiar with.

The 2015 case of *North Carolina v. Western Sky Financial*[75] offers further insight into how the peer-to-peer lending activities of FinTech firms can pose difficulties to regulatory agencies. In this case, a court in North Carolina evaluated whether the lending practices of a FinTech firm (Western Sky Financial) targeting communities in the Cheyenne River Indian Reservation were lawful. Western Sky Financial issued loans of between $850 and $10,000 to members of the community. In those loans, it charged interest rates that ranged from 86% to 342.86%.[76] The loan had a repayment period of between 12 months and 84 months and stated that disputes arising from the loan agreement would be subject to the Cheyenne River Indian Reservation Laws rather than federal laws or state laws. North Carolina's usury law stated that the maximum interest rate that lenders could levy on

72. CashCall Inc. v. Morrissey, 2015 U.S. Lexis 2991 (2015).
73. *Id*.
74. *Id*.
75. North Carolina v. Western Sky Financial, LLC, 2015 NCBC Lexis 87 (2015).
76. *Id*.

their customers was 25%.[77] The court was considering whether the practices of the FinTech firm violated this law. The court ruled that the peer-to-peer lending practices of the company violated the laws that North Carolina had enacted to protect consumers.

This is a grossly unfair business practices that caused difficulties for consumers in a variety of ways due to the exorbitantly high interest rates and penalties involved in the loan process. Luckily, the court argued that FinTech firm's practices suggested that its objective in circumventing North Carolina's lending laws was to saddle consumers in state with loans that they could not pay.[78] This would sink the consumers into a debt cycle that would generate significant profit for Western Sky Financial for many years. In this case, the lending practices paused difficulties to regulatory agencies because the company opted to include clauses in the loan agreement that ousted the jurisdiction of federal and state laws. This move meant that the customers of the FinTech firm could not hide behind the safeguards of consumer protection laws in North Carolina. The court ruled that this practice was unlawful and ordered Western Sky Finance to make a $9 million refund to its customers. Thankfully, the courts were able to establish this legal precedent and thus make it theoretically more difficult to harm consumers, common everyday working class people looking for loans, and created a means to redressing these negligent, harmful practices by these companies.

These cases did not go unnoticed by these emerging companies. The ruling in *North Carolina v. Western Sky Financial*[79] demonstrated that most FinTech firms are aware of existing banking laws that regulate their services. However, they are reluctant to abide by those statutes because of the fear that they will undermine their long-term profitability. Therefore, they take the Western Sky Finance route of restricting consumers' ability to resort to state and federal banking regulations by including clauses in their contracts with their customers that purport to oust the jurisdiction of state and federal banking laws and state and federal consumer protection laws. They believe that these clauses will legitimize their activities. However, as the ruling in *North Carolina v. Western Sky Financial*[80] suggests that the FinTech firms cannot oust the jurisdiction of these laws. In fact, courts will treat the clauses as evidence that the companies did not harbor good intentions at the time when they were entering into their agreement with their potential customers. This evidence of lack of good faith will influence courts to set aside the agreements that the companies have with their customers and ask them to refund the money.

77. *Id.*
78. *Id.*
79. *Id.*
80. *Id.*

Further, the ruling in *North Carolina v. Western Sky Finance* suggests that FinTech firms' decision to operate outside conventional banking laws and regulations is deliberate. The companies are aware that conventional banking laws may make it harder for them to maintain their high revenues. Therefore, they develop strategies targeted at ensuring that their activities do not fall within existing banking laws and regulations. This practice makes them susceptible to legal risks because regulatory agencies will still regard them as financial services institutions whenever they are assessing their compliance with banking laws and regulations. In many instances, courts will side with regulatory agencies and rule that FinTech firms are violating banking legislations. In the rare occasion, the courts will rule in favor of the FinTech firms by arguing that the firms can operate outside existing regulatory controls. *Madden v. Midland Funding*[81] is one example of a case where the court ruled in favor of a FinTech firm. In this case, the Second Circuit Court ruled that the National Bank Act preempted Maddox's usury claims under the Fair Debt Collection Practices Act because Midland Funding was not a bank, a subsidiary of a bank, or the affiliate of a bank.

C. *Summary*

The foregoing discussion has demonstrated how FinTech firms are infringing on banking laws in their quest to deliver services to their customers. The discussion suggests that at the heart of these violations is the perception among FinTech firms that they are technology companies rather than financial services companies. This perception has led most of the companies to violate existing banking legislations in their deposit taking and lending services. The discussion has suggested that the companies' services violate deposit-taking laws whenever customers decide to use them as a convenient substitute for ordinary bank accounts. This is particularly common in instances where the companies provide services like prepaid cards to their customers. These services violate section 24 of the National Banking Act, which states that banks are the only institution that has the legal authority to engage in the business of taking customer deposits. Section 31 of the Texas Finance Code also highlights the exclusive deposit-taking role of banks in its definition of banks. The section states that banks are the institutions that engage in the business of receiving deposits from customers. Therefore, the legislation categorizes all institutions (including deposit-taking FinTech firms) that take deposits from their customers as banks. This categorization implies that deposit-taking FinTech firms will be vulnerable to legal action if they deliver their services to consumers in Texas

81. Madden v. Midland Funding, LLC, 786 F.3d 246 (2nd Cir. 2015).

without applying for the relevant financial services license. There is no doubt whatsoever these new firms are violating existing laws, have done so without consent of any legally mandated political body, and that these actions constitute actions that can and have harmed consumers.

In addition to the violation of the deposit-taking laws, the discussion suggested that FinTech firms violate lending laws through the excessive fees they charge their customers. Statistics on their service of companies like SoFi, Western Financial, Prosper, and Lending Club indicate that the companies lent as much as $5.5 billion in 2014, with the figures indicating that the figures could rise to $150 billion by 2025. These statistics suggest that these FinTech firms are enhancing people's access to loans, but the reality is that they are violating banking laws and consumer protection laws through their high interest rates. In fact, a large percentage of the FinTech firms that specialize in lending levy interests that exceed the limits outlined in consumer protection and banking laws. The case of *North Carolina v. Western Sky Finance*[82] demonstrated how a FinTech firm violated North Carolina's consumer protection laws by issuing loans with interests that ranged between 86% and 342%.[83] The repayment period for the loans ranged from 12 months to 84 months. This practice violated North Carolina's usury laws, which prohibited lending firms in the state from issuing loans with interests that exceed 25%.[84] This violation led the court in ordering the company to issue a $9 million refund to its customers.

Like the deposit taking firms, these peer-to-peer lending FinTech firms erroneously believe that their services are not subject to consumer protection and banking services because their firms are technology firms. This is patently untrue, as the way they operate, as well as how they are perceived and used by their customers, is clearly that of a similar nature to banking institutions. As the ruling in *North Carolina v. Western Sky Finance* suggests, courts and regulatory agencies will categorize FinTech firms as financial services companies even when they try to hide behind their technological adaptations. This should not occur, as the foundation of law and protections are already in place to keep consumers from banking fraud. They should be allowed to not only continue but also incorporate the actions and tendencies of these FinTech firms to violate the law. In the next section, the author will evaluate how the practices of FinTech firms are violating the anti-money laundering legislation.

82. *Id.*
83. *Id.*
84. *Id.*

IV. FINTECH AND ANTI-MONEY LAUNDERING LEGISLATIONS

The overall aim of this study is to evaluate FinTech firms' compliance with AMLs. The previous sections furthered this objective by providing insightful background information on the services that FinTech firms are offering to their customers and the extent of FinTech firms' compliance with laws established to regulate companies in the financial services sector. This section will take the efforts to achieve the overall aim of the study, to stand a step further by outlining the anti-laundering laws in the US and discussing how FinTech firms violate those laws through their money transmitting services. In this section of the paper, the author will go into an intensive and extensive analysis of how the money transmission services comply with AML regulations, the Bank Secrecy Act, and other laws developed to prevent financial services institutions from engaging in money laundering. In the analysis of the compliance of FinTech firms with AMLs, the section will evaluate the specific attitude of courts towards the violations that FinTech firms commit, as well as the tendency of law-making bodies to create these acts of legal precedent in order to provide for greater protection for all consumers.

A. *Anti-Money Laundering Laws*

1. *The Bank Secrecy Act of 1970*

The Bank Secrecy Act of 1970[85] (BSA) is the principle legislation on issues related to money laundering. The BSA[86] prevents banks from engaging in anti-money laundering activities by imposing on them strong compliance obligations. These compliance obligations include reporting requirements and record keeping requirements. Section 17.15 of the legislation states that the institutions and individuals that are subject to the AML provisions in the law are dealers in commodities, dealers in securities, brokers, thrifts, forex companies, private bankers, trust companies, US branches of non-US banks, US agencies of non-US banks, and US banks.

2. *Currency Transaction Report*

The BSA outlines the reporting procedures for US financial institutions. The law states that financial institutions must file a Currency Transaction

85. Bank Secrecy Act, Titles I and II of Pub. L. 91-508, as amended, codified at 12 U.S.C. § 1829b, 12 U.S.C. § 1951-1959, and 31 U.S.C. § 5311-5332.

86. The Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act of 1970 (31 U.S.C. § 5311et seq.).

Report (CTR) for all currency transactions exceeding $10,000.[87] The BSA defines currency transaction as any type of transaction involving the physical transfer or transmission of currency from one person to another. The BSA states that examples of financial transactions include currency transfers, currency exchanges, currency withdrawals, currency deposits, and other types of payment. Section 103.22 of the BSA outlines the type of information that the financial institution must incorporate into the CTR.[88] This information includes the name of the individual, his street address, taxpayer identification number or social security number, and date of birth. All of these details are put in place for very good reasons: to protect the consumer and provide for ways to keep their personal information from being used by external forces intent on harming their financial foundation.

Furthermore, these laws provide increased security. For example, the section goes ahead and states the additional information that the financial institution ought to furnish to comply with the reporting requirements under the BSA.[89] Its states that it is not enough for the financial institution to publish a notation indicating, "We know the customer." The financial institution must state the customer's account number, his taxpayer identification number (for non-U.S. residents), his social security number (for citizens), the amount in question, and the transactions or business activities giving rise to that money.[90] Further, the BSA reduces the risk of money laundering by stating the deadline for filing the CTRs. The law states that financial institutions must file the CTRs within 15 days of the date when the reportable transaction occurred. In this case, the reportable transaction is one where the sum in the transaction exceeded $10,000.

3. *Organizations Exempt from Filing CTR*

In addition to these reporting requirements, Section 103.11 of the BSA outlines the organizations and institutions that are exempt from the reporting requirements under the statute. These organizations include banks in relation to their domestic operations, the domestic subsidiary of a listed company that is not a bank, a company (other than a bank) that has listed its equity or stock on the NASDAQ, American, or New York stock exchanges, all institutions that are exercising the authority of government within the US, and all local, state or federal government agencies.[91] Other entities that are

87. *See* 31 C.F.R. § 103.11(b).

88. *See* 31 C.F.R. § 103.22 (requirement for money services businesses to file currency transaction reports).

89. *Id.*

90. *Id.*

91. *See* 31 C.F.R. § 103.11(uu) states: "Money services business. Each agent, agency, branch, or office within the United States of any person doing business, whether or not on a regular basis or as an

exempt from the reporting requirements listed in the BSA are the ones that fall into a category known as non-listed business. This category covers organizations where more than 50% of their revenue emanates from business activities that are ineligible for the reporting requirements under the BSA.[92] These ineligible businesses include investment bankers, investment advisors, accounting firms, pharmacies, law firms, mobile homes, farm equipment firms, aircraft firms, and non-bank financial institutions that specialize in the delivery of money services (check cashers and currency exchange), telegraph services, and currency exchange services.[93] Other ineligible businesses include trade union organizations, gaming service companies, auction companies, bus, aircraft, and ship chartering services, real estate brokerage services, and pawn broking services. All these services are exempt from the reporting requirements outlined under the BSA. Businesses falling within the "ineligible businesses" category can continue their operations without facing the risk of falling foul of the BSA for failing to report receipt of $10,000 or more during a single transaction.

4. *FinCEN Form*

Apart from the reporting requirements related to transactions that exceed the $10,000 threshold, the BSA outlines other instances where financial institutions ought to publish reports. One of these situations relates to the transfer, transmission, or transportation of money into and outside the US. Section 103.23 of the BSA states that financial institutions wishing to mail, transfer, ship, or physically transport more than $10,000 out of the US or into the US ought to file the Financial Crimes Enforcement Network (FinCEN) form.[94] Filing of this form is an attempt to comply with the US Customs and Treasury department rules on the disclosure of money transported into and outside the US.[95] However, the provision establishes certain exemptions against the rule that financial institutions must report the shipment, mailing, or transfer of money into and out of the US. One of these exemptions is the rule stating that financial institutions should not file the

organized business concern, in one or more of the capacities listed in paragraphs (uu)(1) through (uu)(6) of this section." 31 C.F.R. § 103.11(uu) (5) states: "Money transmitter--(i) In general. Money transmitter: (A) Any person, whether or not licensed or required to be licensed, who engages as a business in accepting currency, or funds denominated in currency, and transmits the currency or funds, or the value of the currency or funds, by any means through a financial agency or institution, a Federal Reserve Bank or other facility of one or more Federal Reserve Banks, the Board of Governors of the Federal Reserve System, or both, or an electronic funds transfer network; or (B) Any other person engaged as a business in the transfer of funds."

92. *Id.*

93. *Id.*

94. Now codified at 31 U.S.C. § 5317(c).

95. *Id.*

form if they are transporting the money through a common carrier or the postal service.[96] Another exemption to the rule of filing the form relates to instances where a bank is transferring money belonging to a customer who has a deposit relationship with the bank.[97] In this instance, the bank will be exempt from the reporting requirement if the general sum is transferred to the customer or when they are consistent with the customer's general conduct of business on behalf of the customer.

This latter exemption is important because the BSA qualifies it in a way that suggests that financial institutions will only be exempt from reporting requirements if evidence suggests that that has been the general business activity that the customer has been engaging in. This suggests that banks will be exempt if the customer orders it to transmit similar sums to overseas accounts on a regular basis.[98] However, where the overseas transactions are rare, the financial institution has the obligation to file FinCEN Form 105 every time it transfers money on behalf of the customer into or outside the US.[99] Further, the BSA states that, where the financial institutions' investigations reveal that the transfer of money into or out of the US is outside the customer's customary practices, the institution will have conduct further investigations on the customer's business practices and file a Suspicious Activity Report (SAR) with the FinCEN.[100] These requirements on filing SAR offer an illustration on the seriousness with which the government deals with the issue of money laundering. The filing of the SAR indicates that the US government is ready to investigate all cases where people are attempting to use financial institutions as a conduit for laundering money. Therefore, the US government has implemented this measure to ensure that the prompt investigation of all issues that may violate AML legislations.

---

96. *See* 31 C.F.R. § 103.41. The registration requirement applies to all money services businesses (whether or not licensed as a money services business by any state) except the U.S. Postal Service; agencies of the United States, of any state, or of any political subdivision of a state; issuers, sellers, or redeemers of stored value, or any person that is a money services business solely because that person serves as an agent of another money services business (however, a money services business that engages in activities described in § 103.11(uu) both on its own behalf and as an agent for others is required to register).

97. *Id*.

98. *See* BRUCE ZAGARIS, INTERNATIONAL WHITE COLLAR CRIME: CASES AND MATERIALS 94-95 (2015).

99. *See* 31 U.S.C. § 5316. A Report of International Transportation of Currency or Monetary Instruments (CMIR) must be filed by each person who physically transports, mails, or ships, or causes to be physically transported, mailed, or shipped currency or other monetary instruments in an aggregate amount exceeding $10,000 at one time from the United States to any place outside the United States or into the United States from any place outside the United States (FinCEN Form 105).

100. *Id*.

5. *Sale of Monetary Instruments*

The sale of monetary instruments is also subject to the reporting requirements of the BSA. Section 103.29 of the BSA prohibits financial institutions from participating in the sale of monetary instruments whose value range between $3,000 and $10,000.[101] The section states that financial institutions should only engage in such transactions if they have obtained and recorded information that identifies the purchaser as well as the specific transaction relating to that money. The section states that monetary instruments include traveler's checks, money orders, cashier checks, bank drafts, and bank checks.[102] The section also states that it is not enough for the bank to collect information on the purchaser of the financial instrument.[103] The financial institution must take the efforts to identify the purchaser a step further by verifying his identity.[104] Thereafter, the section lists the types of information that it considers pertinent to the verification of the purchaser's identity.[105] This information includes the purchaser's name, the date of purchase, the types of monetary instruments purchased, the serial numbers of all the purchased instruments, and the dollar amount in each of the instruments.[106] In instances where the individual purchasing the financial instrument does not have an account with the financial institution, it must request additional information to assist with the verification efforts.[107] The additional information includes the purchaser's address, the purchaser's social security number, the purchaser's date of birth, and the evidence of the verification of the address and name of the purchaser.

In many cases, evidence of verification will manifest in the form of a driver's license. The section recognizes that individuals might attempt to violate this reporting requirement by engaging in the piecemeal purchase of financial instruments. Therefore, it states that financial institutions ought to aggregate the purchase for purposes of reporting. These particular safeguards in place are some of the many forms of protection already built into the system of banking, financial record keeping, and nearly all forms of monetary control governments and regulatory institutions have created. They exist for the specific purpose of protecting one's identity, their banking information, and to provide ways to keep their purchasing potential at a

101. *See* 31 C.F.R. § 103.29 (requirement for money services businesses that sell money orders, traveler's checks, or other instruments for cash to verify the identity of the customer and create and maintain a record of each cash purchase between $3,000 and $10,000, inclusive).

102. *Id.*

103. *Id.*

104. *Id.*

105. *Id.*

106. *Id.*

107. *Id.*

high level.

6. *Customer Identification Program Requirements*

The customer identification program (CIP) requirements under section 103.121 of the BSA are also important considerations that financial services firms ought to implement. The section states that banks must formulate and implement board-approved CIP procedures.[108] The section states that the CIP must be written and the appropriate for the size and operations of the bank. However, it sets out the minimum issues that each CIP must cover to comply with AML laws and prevent people from laundering money.[109] One of the issues outlined in the section relates to the methodology and process developed for verifying the customer's identity.[110] The section states that the methodology and process used in the verification ought to be practicable and reasonable.[111] The practicableness and reasonableness of the identification process will be important in ensuring that the regulatory agencies do not impose onerous burdens on financial institutions. The drafters of the law were aware that institutions lack the capacity to make fool proof identity checks. Therefore, they have use the test of reasonableness and practicableness to assess whether the actions of the CIP meets this standard. A CIP identification process will not be reasonable and practicable if forces the bank to incur significant expenses in its quest to purchase, install, or maintain it. Further, the program will not be reasonable and practicable if it forces the financial institution to alter a significant proportion of its services in order to accommodate the verification program.

Besides the requirement for formulating a program for identifying and verifying the identity of customers, section 103.121 of the BSA outlines other issues that must feature in the CIP.[112] One of these issues relates to the processes put in place to ensure that the financial institutions respond effectively to situations where it cannot verify a customer's identity with reasonable certainty. The section states that financial institutions ought to outline the actions that it will implement in the event that they cannot identify a customer's identity.[113] The section states that the bank must state how it will respond to circumstances in which they are unable to verify the identity of a customer. It states that the explanation ought to include the types of concrete actions they will take to respond to situations where they

108. *See* 31 U.S.C. § 5318(l) and 31 C.F.R. § 103.121 (for banks, savings associations, credit unions, and certain non-federally regulated banks).
109. *Id.*
110. *Id.*
111. *Id.*
112. *Id.*
113. *Id.*

cannot identify the customer's identity.[114] Further, the section states that the CIP ought to outline the procedures that the financial institution has put in place to maintain appropriate records of processes implemented to verify a customer's identity. Additionally, the section stipulates that the CIP ought to provide the procedures the company will implement to verify the names of customers against terror lists. Finally, the section states that the CIP should outline the measures it will take to ensure that the customer has adequate time to verify his identity. The latter process is important because it seeks to protect customers from arbitrary business policies and processes that might undermine the smooth functioning of their business activities. Whether this facet of the situation is the singular goal of all FinTech firms is of course impossible to determine yet there is actually no legitimate basis for assuming it is not. It is much safer for consumers to assume the worst, in fact, to better approach the subject in order to enhance the already established laws, regulations, and other mandates in place.

7. *Customer Due Diligence*

The customer due diligence (CDD) program is another concept under the BSA that companies ought to implement to comply with its AML requirements. The BSA states that the CDD is an important component of the AML program in which financial institutions adopt controls, procedures, and policies targeted at identifying customers that have a high risk of money laundering and terrorist financing.[115] The BSA states that the objective of the CDD program is to enhance the degree of vigilance in issues related to terrorist financing and money laundering. It believes that enhanced vigilance will significantly limit customers' ability to use US financial institutions as a conduit for laundering money and financing terrorists.[116] Indeed, regulators confirm this when they argue that one of the benefits of an effective CDD program is to identify and address suspicious activity in a swift manner. Further, they argue that the CDD program is effective in enabling financial institutions to avoid criminal exposure from individuals who are attempting to use their services as a platform for the perpetuation of criminal activities. In essence, the purpose of the CDD is to enhance financial institutions' ability to comply with the rules and regulations established under the BSA.

B. Title 18 U.S.C

In addition to the BSA, federal law lists money laundering as a criminal

114. *Id.*
115. *Id.*
116. *Id.*

offence. Title 18 of the United States Code lists money laundering as one of the criminal offences in the US penal code. Section 1956 of Title 18 of the U.S. Code states that the practice of laundering monetary instruments is a criminal offense.[117] Section 1956 of Title 18 lists three instances where an individual or organization will violate the prohibition against the laundering of monetary instruments. This is simply one of the many instances of legally binding mandates passed down through the legislation involved within this paradigm.

The first of the three categories of AML violations is in section 1956(1)(a)(1) of Title 18. Section 1956(a)(1)(A) of Title 18 states that any individual or company that conducts a financial transaction in the full knowledge that the money that is the subject of that transaction is the proceed of an unlawful criminal activity violates the section on laundering of monetary instruments if the objective of the transaction was to aid its owners in violating sections 7201 and/or 7206 of the Internal Revenue Code of 1986.[118] The section adds that the individual will still violate AMLs if the objective of dealing in the funds is to promote the continued prevalence of the unlawful activity. The section states that this individual or organization will be liable fine not exceeding $500,000 or a fine two times the value of the property that is the subject of the transaction, whichever is greater. Further, the section states that courts have the power to issue a two-year sentence in addition to the fine or in exchange for the monetary compensation. In the context of FinTech operations, a FinTech firm will violate section 1956(1)(a)(1)(A) of Title 18 by knowingly dealing with the proceeds of a crime in a way that aids its owners in violating sections 7201 and 7206 of the Internal Revenue Code of 1986.[119] A FinTech firm will also violate the section by dealing in the proceeds of a crime in a way that encourages perpetrators of that crime to continue engaging in it. This will be the case where the FinTech firm assists Mexican drug cartels in transferring funds from Mexico to banks in the US. In such a scenario, courts will punish the company by imposing a $500,000 fine or a proposing a financial penalty that is twice as high as the value of the property that is subject to the financial transaction.

The second of the three categories of AML violations in Title 18 of the U.S.C is in section 1956(1)(a)(1)(B). Section 1956(1)(a)(1)(B) of Title 18 states that any person or organization that with the knowledge that the property that is the subject of a financial transaction is the proceed of an unlawful either conducts or tries to conduct a financial transaction related to the proceeds of that transaction in the knowledge that the objective is to

117. *See* U.S. Code: Title 18-Crimes and Criminal Procedure, Pub. L. 114-38 (2016).
118. *See* ZAGARIS, *supra* note 98, at 90-91.
119. *See id*.

conceal, the control, the ownership, the source, or the nature of the unlawful activity will be liable to a $500,000 fine or the penalty that is two times the value of the property in that transaction. This category of money laundering is different from the first category because it caters to cases where the individual dealing in the proceeds of the unlawful transaction is aware that the proceeds are unlawful and attempts to deal in it to conceal its source. The law will categorize such an action as money laundering and will expose the individual engaging in the act to a two-year prison term and/or a fine of $500,000 or a penalty two times the value of property that was the subject of the unlawful activity.[120] In the context of the activities of FinTech firms, violation of this provision would occur when a firm decides to use its services as a conduit for concealing the source, control, ownership, or the nature of unlawful activity related to it. In such a case, the firm in question will be liable because it is aware of the link between the money and an unlawful criminal activity. It will also be liable because it uses its services to deal with the money in a way that undermines regulatory agencies' ability to know its control, its origin, or its source.

The third category of AML violation is in section 1956(2) of Title 18 U.S. Section 1956(2) states that any person or organization that transfers, transmits, or attempts to transfer a monetary instrument from the US to a country outside the US with the objective of furthering a criminal activity violates the law against the laundering of financial instruments.[121] The section adds that organizations and individuals will commit the offenses listed under section 1956(2) of Title 18 U.S.C if they knowingly transmit, transport, or transfer the proceeds of an unlawful activity with the objective of circumventing the reporting requirements listed under Federal or State legislations. Further, the individuals or organizations will violate section 1956(2) if they knowingly transfer, transmit, or transport the proceeds of an unlawful activity with the objective of concealing the control, the ownership, the source, the location, or the nature of that criminal activity. The section adds that all individuals violating section 1956(2) of Title 18 will be liable to a $500,000 or a figure that is two times the value of the transmitted, transferred, or transported property.

In addition to the stated AML provisions of Title 18 of the U.S.C, an analysis of section 1956 demonstrates that it sets the criterion for burden of proof in the event that a firm or individual has violated those provisions. The section states that the law enforcement officer arresting the individual or indicting the organization that has violated the third category of AML violation needs only to state that it is true that the individual or organization

120. *Id.*
121. *Id.* at 90.

knew that the money was the proceeds of an unlawful activity.[122] Once the law enforcement officer has made a positive statement to that effect, the burden will shift to the arrested individual or indicted organization to prove that it did not know that the funds were the proceeds of an unlawful activity.[123] Regarding the first and second categories of AML violations, section 1956 states that the law enforcement officer will satisfy his burden of proof by demonstrating that the proceeds of an unlawful activity constituted a significant proportion of the financial transaction.[124] The section states that the law enforcement officer will satisfy this burden in three simple steps. The first step will be to show that those proceeds were part of a series of dependent or parallel transactions.[125] The second step would be to demonstrate that any one of those transactions could have involved the sums of money categorized as the proceeds of an unlawful activity.[126] The final step will be to show that the series of transactions involving the unlawful criminal activity were part of a single arrangement or plan.[127] Once the law enforcement officers have proved these three issues, the burden will shift to the arrested individual or indicted organization. The arrested individual or indicted organization will have to prove that it did not have knowledge that the funds it was dealing in were proceeds of an unlawful activity. Secondly, it will have the burden of proving that the transaction was not part of a single arrangement to either circumvent reporting procedures or conceal the source, control, ownership, location, or nature of the unlawful activity.

The takeaway from this section on the issues that law enforcement officers ought to prove is that the law has placed a low burden of proof. The purpose of such a low burden is to make it easier for law enforcement officers to prove companies or individuals' involvement in the violation of AML. Placing a higher burden of proof threshold on law enforcement officers would have undermined their ability to prosecute AML cases because companies and individuals engaging in the activity would have put in place elaborate measures to conceal their activities. The low burden of proof threshold provides law enforcement officers with sufficient room to prosecute organizations even in situations where it might be extremely difficult for them to establish a company's connection with money laundering activities. Another factor accounting for the low burden of proof threshold is the fact that prosecutors at the justice department and law enforcement officers may not have access to the information they need to

122. *Id.*
123. *See id.* at 92-93.
124. *Id.*
125. *Id.*
126. *Id.*
127. *Id.*

sustain a case against individuals or organizations violating AML legislations. Most of the information is in the custody of the individual or organization engaging in money laundering. Therefore, their chances of undermining the credibility of the evidence presented against them by destroying it would be extremely high. The low burden of proof threshold makes it easier for prosecutors at the justice department and law enforcement officers to present evidence that is necessary to sustain a conviction.

This underscores the very real need for not just a different set of legally mandated circumstances to create a standard of adherence to already established laws but rather an enforcement of what is in the books currently. In addition, though, since this is a completely unprecedented form of monetary transference (FinTech firms' primary functioning as it were), new laws may need to be created in order to handle the vagaries within this framework of operation. This is similar to when new technologies are unlocked in other industries, such as television and film in regards to the internet. Writers, actors, directors, etc., receive compensation through various means, of course; yet with the advent of the creation of the internet, new modes of structuring contracts, as well as determining how residuals are paid to these members of the industry, had to be developed to compensate for the way various agencies were using the internet to broadcast all films and television entities. For all FinTech related operations, a new set of legal standards should be developed to account for the variety of circumstances created therein. As will be seen in this continued report, this should happen to assist the process of conducting further investigation into the subject matter to correct certain acts of harm that are occurring too often due to how FinTech firm conduct their financial business.

C. *FinTech Firms' AML Compliance*

Extensive evidence suggests that FinTech firms do not comply with the outlined AML legislations when delivering services to their customers. Recent evidence on FinCEN cases against FinTech firms suggests that these companies are reluctant to comply with AML laws. The case of Ripple Labs Inc. provides an illustration of the extent of the failure of FinTech firms to comply with AML laws. Ripple Labs Inc. provides Ripple protocol, an open-source distributed payment network that enables payments to merchants, consumers, and developers. Its payment protocol transforms payments to work like communications.[128] On May 5, 2015, FinCEN and Ripple Labs Inc. agreed to an out of court settlement in which the latter

128. *See* Trevor I. Kiviat, *Beyond Bitcoin: Issues in Regulating Blockchain Transactions*, 65 DUKE L.J. 569, 589-94 (2015).

corporation agreed to pay a civil fine of $700,000.[129] Ripple Labs agreed to pay the fine because evidence suggested that it repeatedly violated federal AML by failing to register its financial services business, failing to implement an AML program, and failing to report suspicious financial transactions to FinCEN.[130] In the evidence, FinCEN argued that Ripple Labs violated BSA regulations by failing to conduct appropriate and credible "know your customer" procedures on a financial transaction worth $250,000. Roger Ver, the customer requesting for the financial transaction, had pleaded guilty to a charge of selling explosives in violation of federal laws.[131] FinCEN investigators argued that the company's failure to report this transaction proved its reluctance to comply with AML provisions that required it to report suspicious transactions.

In addition to the fine, Ripple Labs agreed to implement several changes that it believed were necessary for improving its compliance with existing AML provisions. As part of the settlement, Ripple Labs stated that it would institute a process in which it would implement an AML compliance program that is consistent with the standards set in the financial services sector.[132] Further, the company agreed to comply with AML laws by registering its virtual currency service as a money service and hiring external auditors to evaluate the extent of its compliance with existing AML laws every two years. Additionally, the company agreed to adjust its software protocol to ensure that it can monitor suspicious transactions that might violate AML laws. This latter proposal on adjusting the software protocol caught many FinTech firms that offer virtual currency services by surprise because many argued that their software protocol and technologies were outside the reach of regulatory agencies like FinCEN.[133] They argued that those protocols and technological infrastructures were outside that reach because they were not operating within the scope of existing AML laws.[134] They defended that it was their money transmitting services (rather than their technological infrastructures) that were within the reach of existing AML laws.[135] These assertions suggested that Ripple Labs and other FinTech corporations are still reluctant to comply with the reporting requirements under the BSA.

---

129. *See* SIVON, *supra* note 21, at 1.

130. *Id.*

131. *See* Sarah Todd & Ian McKendry, *What Ripple's Fincen Fine Means for the Digital Currency Industry*, AM. BANKER (May 6, 2015), https://www.americanbanker.com/news/what-ripples-fincen-fine-means-for-the-digital-currency-industry.

132. *Id.*

133. *Id.*

134. *See* GOLDMAN SACHS GROUP, INC., PROFILES IN INNOVATION: BLOCKCHAIN 71-77 (2016), www.finyear.com/attachment/758923/.

135. *Id.*

The arguments about the software protocol as well as the technological infrastructure that Ripple Labs and other virtual currency firms operate on discloses some of the difficulties that the companies might face in their quest to comply with existing AML laws. An analysis of the business model for the operation of virtual currency firms demonstrates that anonymity and the desire to operate outside existing laws are among the unique selling points of firms operating in the virtual currencies sector. Firms in the industry attract their customers by informing them that they will safeguard their anonymity and that their currency will only exist in electronic form.[136] The virtual currency firms inform their customers that virtual currencies are not subject to regulations from a legal entity or a sovereign government.[137] The absence of sovereign backing and regulation from a legal entity means that the value of one virtual currency depends on adoption, trust, and perception.[138] On November 11, 2016, the value of one bitcoin was $714.22.[139] Such a high value means that it is easy for unscrupulous individuals to use the virtual currency industry as a platform for laundering money. In fact, their quest to launder money will become easier because of virtual currency firms' desire to guarantee the anonymity of their customers and their transactions. The guaranteed anonymity means that unscrupulous individuals can use the virtual currency industry to obtain money through unlawful activities. Indeed, FinCEN's claim that Ripple Labs failed to develop a "know your customer program" and report on a suspicious $250,000 transaction by an individual who had pleaded guilty to attempting to sell explosives offers sufficient proof of the extent to which the virtual currency platform is vulnerable to money laundering. The desire for anonymity and the claim that the value of the currency is not subject to external regulation is the evidence that these corporations are not complying with AML laws.

As noted in the previous section, the BSA imposes certain reporting requirements on institutions that provide financial services to their customers. The wording of the charge against Ripple Labs suggests that the company violated several AML provisions outlined in the BSA. One of the violated provisions was section 103.22 of the BSA. Section 103.22 of the BSA states that financial institutions must file a Currency Transaction Report (CTR) for all currency transactions exceeding $10,000. Section 103.22 of the BSA outlines the type of information that the financial institution must incorporate into the CTR.[140] This information includes the name of the

136. *See* Matthew Kien-Meng Ly, *Coining Bitcoin's "Legal-Bits": Examining the Regulatory Framework for Bitcoin and Virtual Currencies*, 27 HARV J.L. & TECH. 587, 588-90 (2014).

137. *Id.*

138. *Id.*

139. *See Bitcoin Price Index: Closing Price*, COINDESK, http://www.coindesk.com/price/ (last visited Jan. 4, 2017).

140. *See* 31 C.F.R. § 103.22.

individual, street address, taxpayer identification number or social security number, and date of birth. The section goes ahead and states the additional information that the financial institution ought to furnish to comply with the reporting requirements under the BSA. Another important AML provision that the company violated was the customer identification program (CIP) requirements under section 103.121 of the BSA. Section 103.121 of the BSA states that banks must formulate and implement board-approved CIP procedures.[141] The section states that the CIP must be written and be appropriate for the size and operations of the bank.[142] However, it sets out the minimum issues that each CIP must cover to comply with AML laws and prevent people from laundering money. One of the issues outlined in the section relates to the methodology and process developed for verifying the customer's identity. Obviously this is an important facet to overall security when someone is conducting financial transactions online with their personal information.

The particular section states that the methodology and process used in the verification ought to be practicable and reasonable. In the charge, FinCEN claims that the company failed to implement an AML program. This charge suggests that Ripple Labs failed to comply with the provision under section 103.121 of the BSA that required it to implement a CIP. Its failure to implement the program meant that it lacked the capacity to prevent people from using its services as a conduit for the laundering of financial instruments. Further, the failure to implement the CIP meant that the company lacked standards that could prevent the laundering of money. This is yet again a clear, reasonably enhanced demonstration that these institutions can and will conduct their personal financial business to improve their own profit margins regardless of how it might affect their customers.

Apart from the reporting requirements related to transactions that exceed the $10,000 threshold and the requirement for implementing the CIP, the wording of the charge against Ripple Labs suggests that the company violated another pertinent provision of the BSA. The wording of the charge suggests that Ripple Labs violated the provision relating to the transfer, transmission, or transportation of money into and outside the US. Section 103.23 of the BSA states that financial institutions wishing to mail, transfer, ship, or physically transport more than $10,000 out of the US or into the US ought to file the Financial Crimes Enforcement Network (FinCEN) form.[143] Section 103.23 stipulates that one of the exemptions to the rule on filing the FinCEN form relates to instances where a bank is transferring money

141. *See* 31 C.F.R. § 103.121.
142. *Id.*
143. *See* 31 U.S.C. § 5321(a).

belonging to a customer who has a deposit relationship with the bank.[144] In such instances, the bank will be exempt from the reporting requirement if the general sum transferred to the customer or on behalf of the customer is consistent with the customer's general conduct of business.

This exemption is important because the BSA qualifies it in a way that suggests that financial institutions will only be exempt from reporting requirements if evidence indicates that it is the general business activity that the customer has been constantly engaged in. This suggests that banks will be exempt if the customer orders it to transmit similar sums to overseas accounts on a regular basis. However, where the overseas transactions are rare, the financial institution has the obligation to file FinCEN Form 105 every time it transfers money on behalf of the customer into or outside the US. Further, the BSA states that, where the financial institutions' investigations reveal that the transfer of money into or out of the US is outside the customer's customary practices, the institution will have to conduct further investigations on the customer's business practices and file a Suspicious Activity Report (SAR) with the FinCEN.[145] Ripple Labs violated this provision when it failed to investigate and file an SAR on the investor who transferred $250,000.

Apart from Ripple Labs, the regulatory agencies have cracked the whip on other FinTech firms that specialize in the sale and transmission of virtual currencies. In 2013, the FBI arrested Ross Ulbricht, the founder of a virtual currency firm known as *Silk Road. Silk Road* was a virtual currency firm that specialized in the provision of virtual currencies for individuals wishing to purchase products in the online environment.[146] Immediately after the arrest, FBI investigators stated that Ulbricht founded the Silk Road as a conduit for the transfer of drugs. They argued that Ulbricht operated the *Silk Road* site under the nickname *Dread Pirate Roberts.* The FBI asserted that the lenient design of the *Silk Road* website meant that drug traffickers and computer hackers could use the site to sell their drugs or computer passwords and usernames in exchange for bitcoins.[147] The charges stated that Ulbricht received millions in commissions on the more than $1 billion worth of transactions on his site.[148] The FBI argued that most of those transactions are related to criminal activities and many were using the *Silk Road* site as an avenue for hiding the links between their money and unlawful activities. At the time when the FBI shut down the Silk Road website, it had more than

144. *Id.*
145. *Id.*
146. *See* Sam Frizell, *How the Feds Nabbed Alleged Silk Road Drug Kingpin 'Dread Pirate Roberts'*, TIME MAG. (Jan. 21, 2015), http://time.com/3673321/silk-road-dread-pirate-roberts/.
147. *Id.*
148. *Id.*

26,000 bitcoins.[149] Under the current exchange rate, one can argue that the bitcoins seized by the FBI is $18,000,000.

The arrest of Ulbricht and the subsequent closure of his *Silk Road* website demonstrate the extent of FinTech firms' reluctance to comply with AML laws. In fact, FinTech firms' response to Ulbricht's arrest demonstrates that they do not understand existing AML laws and the extent of their respective firms' compliance with those laws. Most FinTech investors argued that Ulbricht's arrest and subsequent closure of his firm was illegal because he was not a direct participant in the illegal activities that took place in his Silk Road website.[150] Further, they argued that the Silk Road did not qualify as a financial services company because they merely provided a platform for people to sell their goods.[151] This argument suggests that FinTech entrepreneurs failed to appreciate how the *Silk Road's* decision to exchange dollars for bitcoins and transfer bitcoins to sellers qualified as the provision of financial services. The firm's qualification as a financial services company meant that it had an obligation to comply with AML provisions under the BSA and title 18. It failed to comply with the AML provisions in the two laws by failing to implement CIP and processing financial transactions in the knowledge that they were the proceeds of an unlawful criminal activity.

An analysis of the claims against Ulbricht and the Silk Road demonstrates that they violated section 1956(1)(a)(1) of Title 18. Section 1956(a)(1)(A) of Title 18 states that any individual or company that conducts a financial transaction in the full knowledge that the money that is the subject of that transaction is the proceed of an unlawful criminal activity violates the section on laundering of monetary instruments if the objective of the transaction was to aid its owners in violating sections 7201 and/or 7206 of the Internal Revenue Code of 1986.[152] The section adds that the individual will still violate AMLs if the objective of dealing in the funds is to promote the continued prevalence of the unlawful activity. The section states that this individual or organization will be liable fine not exceeding $500,000 or a fine two times the value of the property that is the subject of

149. *See* Kashmir Hill, *The FBI's Plan for the Millions Worth of Bitcoins Seized from Silk Road*, FORBES (May 1, 2013), http://www.forbes.com/sites/kashmirhill/2013/10/04/fbi-silk-road-bitcoin-seizure/#188e0feb5c22.

150. U.S. Attorney's Office, *Manhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of "Silk Road" Website*, FBI (Oct. 25, 2013), https://archives.fbi.gov/archives/newyork/press-releases/2013/manhattan-u.s.-attorney-announces-seizure-of-additional-28-million-worth-of-bitcoins-belonging-to-ross-william-ulbricht-alleged-owner-and-operator-of-silk-road-website.

151. *Id*.

152. *See* U.S. Code: Title 18-Crimes and Criminal Procedure; ZAGARIS, *supra* note 98.

the transaction, whichever is greater.[153] In the context of the charge against Ulbricht, one can argue that he was aware of the nature of transactions taking place on his website. The FBI confirms this when it argued that more than $1 billion of revenue in the Silk Road website originated from the drug trafficking and other criminal activities.[154] Such a claim is evidence that Ulbricht knew about the transactions taking place on his website. In fact, the claim that he was masquerading under the nickname *Dread Pirate Roberts* is evidence that he knew about the transactions, but desired to conceal that knowledge.

In addition to violating the provision under section 1956 of Title 18, the wording of the charges suggests that Ulbricht violated three other AML provisions under the BSA. The first of these provisions is the provision related to the filing of the Currency Transaction Report (CTR) for all currency transactions exceeding $10,000. The BSA defines currency transaction as any type of transaction involving the physical transfer or transmission of currency from one person to another.[155] The BSA states that examples of financial transactions include currency transfers, currency exchanges, currency withdrawals, currency deposits, and other types of payment. Section 103.22 of the BSA outlines the type of information that the financial institution must incorporate into the CTR.[156] This information includes the name of the individual, his street address, taxpayer identification number or social security number, and date of birth. The section goes ahead and states the additional information that the financial institution ought to furnish to comply with the reporting requirements under the BSA.[157] An analysis of the activities of *Silk Road* suggests that it violated this provision by failing to file CTR reports on customers whose cumulative transactions surpassed $10,000. He failed to file this report yet evidence suggests that his company specialized in the provision of currency exchange services for customers who were buying and selling goods through the *Silk Road* website. Therefore, due to the complexity of any given financial enterprise of this nature, greater controls could perhaps alleviate the potential for harm.

The second AML provision violated by *Silk Road* is the provision on filing of FinCEN form. Section 103.23 states that firms in the financial services sector must file FinCEN forms whenever they are transferring, transmitting, or transporting money into and outside the US. Section 103.23 of the BSA states that financial institutions wishing to mail, transfer, ship, or

153. *Id.*
154. *See* Frizell, *supra* note 146.
155. *See* Bank Secrecy Act of 1970.
156. *Id.*
157. *Id.*

physically transport more than $10,000 out of the US or into the US ought to file the Financial Crimes Enforcement Network (FinCEN) form.[158] Filing of this form is an attempt to comply with the US Customs and Treasury department's rules on the disclosure of money transported into and outside the US.[159] The law exempts financial services companies from filing the FinCEN form in instances where they are transferring money belonging to a customer who has a deposit relationship with the bank. In these instances, the banks will be exempt from the reporting requirement if the general sum transferred to the customer or on behalf of the customer is consistent with the customer's general conduct of business. This exemption is important because the BSA qualifies it in a way that suggests that financial institutions will only be exempt from reporting requirements if evidence suggests that it is the general business activity that the customer has constantly been engaging in. This suggests that banks will be exempt if the customer orders it to transmit similar sums to overseas accounts on a regular basis.

However, where the overseas transactions are rare, the financial institutions have an obligation to file FinCEN Form 105 every time they transfer money on behalf of the customer into or outside the US. Further, the BSA states that, where the financial institutions' investigations reveal that the transfer of money into or out of the US is outside the customer's customary practices, the institution will have conduct further investigations on the customer's business practices and file a Suspicious Activity Report (SAR) with the FinCEN.[160] The charges against *Silk Road* demonstrate that the company violated this provision by failing to file the FinCEN form whenever it transferred bitcoins to customers outside the US. Further, it violated the law when it failed to file FinCEN forms for the transmission of money into the US. This are clearly established facts in the case, and could provide further increases in the way regulatory agencies conduct their investigations into these illegal activities, as well as give notice of intolerance in these actions.

The third AML provision violated by *Silk Road* is the provision on the customer identification program CIP. The CIP requirements under section 103.121 of the BSA states that financial institutions must formulate and implement board-approved CIP procedures.[161] The section states that the CIP must be written and the appropriate for the size and operations of the bank. However, it sets out the minimum issues that each CIP must cover to comply with AML laws and prevent people from laundering money. One of the issues outlined in the section relates to the methodology and process

158. *Id.*
159. *Id.*
160. *Id.*
161. *Id.*

developed for verifying the customer's identity. The section states that the methodology and process used in the verification ought to be practicable and reasonable.[162] Another issue that must appear in the CIP is the processes put in place to ensure that the financial institutions respond effectively to situations where it cannot verify a customer's identity with reasonable certainty. The section states that financial institutions ought to outline the actions that it will implement in the event that they cannot identify a customer's identity.[163] The section states that the bank must state how it will respond to circumstances, in which they are unable to verify the identity of a customer. It states that the explanation ought to include the types of concrete actions they will take to respond to situations where they cannot identify the customer's identity.[164] Further, the section states that the CIP ought to outline the procedures that the financial institution has put in place to maintain appropriate records of processes implemented to verify a customer's identity. Additionally, the section stipulates that the CIP ought to provide the procedures the company will implement to verify the names of customers against terror lists.[165] Finally, the section states that the CIP should outline the measures it will take to ensure that the customer has adequate time to verify his identity.[166] The wording of the charge against *Silk Road* suggests that it violated section 103.121 of the BSA by failing to implement a CIP. Customers on the company's site continued to transaction without disclosing their identity. The company knew that most of them were engaging in suspicious activities, but it failed to implement a system for identifying their identity and flag down customers who are engaging in suspicious activities like drug trafficking. This failure is an indication that the company was aware of the criminal activities taking place on its site, but it failed to report them because it believed that such an action would jeopardize its relationship with those customers.

Ripple Labs and *Silk Road* are not the only corporations in the virtual currency sector that have violated AML legislations. Other FinTech firms (like *Liberty Reserve*) from the sector continue to violate AML laws. In 2013, FBI investigators arrested Arthur Budovsky the co-founder of a Costa Rica based virtual currency company known as *Liberty Reserve*.[167] The firm

---

162. *Id.*
163. *Id.*
164. *Id.*
165. *Id.*
166. *Id.*
167. *See* U.S. Attorney's Office, Southern District of New York, *Liberty Reserve Founder Arthur Budovsky Sentenced in Manhattan Federal Court to 20 Years for Laundering Hundreds of Millions of Dollars Through His Global Digital Currency Business*, U.S. DEPARTMENT OF JUSTICE (May 6, 2016), https://www.justice.gov/usao-sdny/pr/liberty-reserve-founder-arthur-budovsky-sentenced-manhattan-federal-court-20-years.

specialized in the provision of online virtual currency services that violated AML statutes.[168] The FBI argued that *Liberty Reserve* permitted its customers to exchange their virtual currency with customers in the US without verifying their identity. *Liberty Reserve* did not ask its customers to provide their personal details or verify their identity.[169] These practices led the FBI to arrest the co-founder of the organization on grounds that it was violating US anti-laundering laws by failing to record its customers' names and allowing its customers to launder funds generated from criminal activities like credit card fraud, child pornography, identity theft, drug trafficking, and investment fraud.[170] According to a May 2016 Department of Justice press release, a Federal court in Manhattan sentenced Arthur Budovsky to 20 years after he pleaded guilty to a charge of laundering money by knowingly assisting its customers to transmit the proceeds of credit card fraud, child pornography, identity theft, drug trafficking, and investment fraud.[171] The charge against Budovsky stated that the FBI first arrested him in 2006 and instituted money-laundering-related charges against him for operating *GoldAge*, an unlicensed online money transfer business.[172] After the charges, Budovsky renounced his citizenship and moved to Costa Rica where he incorporated *Liberty Reserve.* Budovsky believed that the move to Costa Rica would insulate him and his company from AML-related charges.[173] From the outset, *Liberty Reserve* violated AML laws by delivering its services in a way that was inconsistent with US AML laws. At the height of its activities, *Liberty Reserve* handled transactions worth $300 million every month, with statistics indicating that a large proportion of the funds emanated from the US.[174] The charges suggested that Budovsky was aware that a significant percentage of the funds emanated from online-based high-yield investment programs in which American citizens generated large sums of money from their online investment and used FinTech firms like *Liberty Reserve* as a conduit for tax evasion.[175] The charges also suggested that Budovsky knew that some of its customers based in the US had used their *Liberty Reserve* accounts to launder the proceeds of their criminal activities whose value ranged from $250 million to $500 million.[176] The

168. *Id.*
169. *See* U.S. Attorney's Office, Southern District of New York, *supra* note 167.
170. *Id.*
171. *Id.*
172. Marc Santora, William K. Rashbaum & Nicole Perlroth, *Online Currency Exchange Accused of Laundering $6 Billion*, NEW YORK TIMES (May 28, 2013), http://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html?pagewanted=1&_r=0.
173. *Id.*
174. *Id.*
175. *Id.*
176. *Id.*

success Budovsky's conviction as well as the evidence presented against him offer sufficient proof of the extent of FinTech firms' involvement in the violation of AML laws.

Like the founder of *Liberty Reserve*, the founders of *BitInstant* and *Mt. Gox* faced charges related to the violation of AML provisions in the BSA. FBI investigators arrested Mr. Shrem, the founder of BitInstant, after their investigations showed that it had been receiving millions from customers with false identities. The investigations suggested that BitInstant had conducted internal reviews on some of these customers and discovered that some of them were using false identities, but did not comply with AML provisions in the BSA by submitting SARs to the regulators.[177] Further, the investigations suggested that *BitInstant* played an active role in assisting Silk Road to convert dollars for some of its customers.[178] Upon arrest, the FBI charged the founder of the company with several AML violations including operating an unlicensed money transfer service, conspiracy to commit money laundering, and failure to file FinCEN and SAR forms on its customers.[179] Shrem pleaded guilty to the charges and federal judge sentenced him to a prison term of two years.[180] In 2015, FBI investigators instituted charges against Karpeles, the founder of Mt. Gox, a company that specialized in the provision of bitcoin exchange services.

Though some of the accusations and subsequent charges might seem shocking or even rare, they are in fact commonplace within this framework of FinTechs and how they normally operate. For instance, the FBI instituted the charges against Karpeles after the company lost bitcoins worth $500 million.[181] Karpeles argued that Mt. Gox lost the bitcoins after a security flaw in the company's software left the bitcoins vulnerable to theft from hackers.[182] Subsequent investigations suggested that Mt. Gox had a weak security infrastructure that Karpeles had designed. Such an outcome suggested that the setup of the company made it vulnerable to attacks by individuals wishing to use its bitcoins as an avenue for laundering money.[183] The company's failure to register itself as a financial services firm meant that regulators could not protect its customers by reviewing its security protocols. It also meant that the company was violating AML provisions by failing to check the identity of its customers, failing to report suspicious

177. *See* Douglas, *supra* note 11, at 62.
178. *Id.*
179. *Id.*
180. *Id.*
181. *Id.*
182. *Id.*
183. Jeremy Bonney, *Mt. Gox Registers with FinCEN as a Money Services Business*, COINDESK (June 29, 2013), http://www.coindesk.com/mt-gox-registers-with-fincen-as-a-money-services-business/.

financial transactions, and failing to account for its customers' sources of funds. Such an outcome is evident that these companies are still facing challenges in their quest to comply with existing AML statutes and provisions. It suggests that most of these corporations will inadvertently violate AML laws and make them subject to Department of Justice investigations.

Certainly, an analysis of existing AML laws demonstrates that *Liberty Reserve*, *Mt. Gox*, and *BitInstant* violated AML laws in three different ways. Firstly, they violate AML laws by knowingly transmitting the proceeds of unlawful criminal activity in a way that undermines law enforcement officers' ability to trace the money. This is in complete contravention of section 1956 of Title 18. Secondly, the virtual currency FinTech firms violate AML laws by transmitting their customers' money in a way that enhances their ability to evade IRS detection. Again, they do this by maintaining the anonymity of their customers and preventing regulatory agencies from conducting audits on their activities. This practice of maintaining the anonymity of customers in ways that enhances their ability to evade tax violates section 1956(1)(a)(1) of Title 18. Section 1956(a)(1)(A) of Title 18 states that any individual or company that conducts a financial transaction in the full knowledge that the money that is the subject of that transaction is the proceed of an unlawful criminal activity violates the section on laundering of monetary instruments if the objective of the transaction was to aid its owners in violating sections 7201 and/or 7206 of the Internal Revenue Code of 1986[184]. Thirdly, the FinTech firms in the virtual currency sector violate AML laws by maintaining the anonymity of their customers and failing to report suspicious transactions, failing to implement CIPs, and failing to report on transactions whose cumulative value exceeds $10,000. Such practices contravene section 103.121 and section 103.23, which make it mandatory for all financial services firms to implement CIPs and file FinCEN forms.

While the initial discussion seems to suggest that FinTech firms in the virtual currency settings are the only organizations whose activities are violating AML laws, the reality is that FinTech firms in other sectors are also violating the statutes. FinTech corporations like Bond Street and OnDeck have experienced challenges in their quest to provide services to their customers because of the inconsistency between their practices and AML laws. OnDeck is a FinTech firm that specializes in providing loans to its customers.[185] Unlike ordinary banks, OnDeck relies on a complex series of algorithms to compute its customers' creditworthiness to determine whether

184. *See* U.S. Code: Title 18-Crimes and Criminal Procedure; ZAGARIS, *supra* note 98.
185. *See* Douglas, *supra* note 11, at 18-21.

they qualify for loan facilities.[186] Although the model of OnDeck's business means that it cannot run into some of the challenges that its counterparts in the virtual currency sector are facing, an analysis of the company's operations suggests that they may still violate existing AML laws.[187] OnDeck is operating a money business within the meaning outlined under the BSA, but it has not registered itself as a financial services companies. As the cases outlined in the analysis of the compliance of virtual currency firms suggest, the practice of operating a money services business without license violates AML laws.[188] It violates AML laws because the companies' failure to register their entities as money service businesses means that they cannot comply with the CIP and FinCEN requirements outlined under the BSA. Further, the practice implies that the companies cannot comply with the requirement for reporting suspicious financial transactions whenever they encounter them in their dealings with their customers. This type of outcome means OnDeck might face the same AML violation charges that companies in the virtual currency sector have faced.

Bond Street faces the same AML compliance challenges as OnDeck. Bond Street is a FinTech firm that specializes in the provision of loans to small businesses. The company uses the revenue it receives loan repayments as well as the money it receives from donors as the source of money for offering loans to its customers.[189] Like OnDeck, Bond Street has not registered its business as a financial services company because it regards itself as a technology company. The company argues that the earnings it generates from loans are not interest rates. It argues that it merely charges its customers facilitation fees to cover the costs of running the online lending business.[190] This argument might be true in the eyes of the founders of Bond Street. However, the charges preferred against FinTech firms operating in the virtual currency sector suggest that a firm's views about its nature of business activity has no bearing on the arguments of regulatory agencies on whether the firm's activities qualify as money services business.[191] Indeed, many virtual currency FinTech firms faced AML-related charges simply because of the consequences of their failure to register their business as a money services business. That failure undermined their ability to comply with the laws that require them to report on the identity of their customers. The failure curtailed their capacity to comply with AML provisions on the reporting of transactions whose value exceeds $10,000. That failure also

186. *Id.*
187. *Id.*
188. *Id.*
189. *See* Douglas, *supra* note 11, at 18.
190. *Id.*
191. Kelsey L. Penrose, *Banking on Bitcoin: Applying Anti-Money Laundering and Money Transmitter Laws*, 18 N.C. BANKING INST. 529, 543-44 (2014).

weakened their ability to comply with the AML provisions on the reporting of transactions that involve the transmission of funds into and out of the US. These consequences of failure to register services themselves as money services business mean that Bond Street is at a high risk of prosecution for violation of AML laws.

V. CONCLUSION

The aim of the study was to evaluate the extent to which FinTech firms are compliant with existing AML legislations. In the first section of the paper, the author provided background information on the study by evaluating the laws governing firms in the financial services industry and the extent to which FinTech firms are compliant with those services. This background information was important because it provided crucial details on whether FinTech firms qualified as financial services firms. A positive response to this question was evident that the services of FinTech firms would fall within the scope of the AML legislations. The second section of the paper went a step further by analyzing AML-laws and the extent of FinTech firms' compliance the provisions outlining the types of actions that FinTech firms ought to implement to comply with those provisions. Further, the analysis was pertinent because it outlined the extent of FinTech firms' compliance with existing AML laws. The analysis showed how FinTech firms are reluctant to comply with AML laws because they believe that their services are outside the scope of existing AML laws.

Additionally, the analysis demonstrated the types of actions that regulatory agencies have taken to guarantee the continued compliance of FinTech firms. Many of these actions were and continue to be within the scope of existing law and the primary thrust and purpose of this article is to demonstrate this is absolutely essential for the future. In addition, it is also important to understand how these businesses operate outside the law in order to develop procedures and regulations to assist in controlling, outlawing, and prosecuting these FinTech firms that break the laws and harm consumers. This has happened in many cases, certainly, yet there remains more work to be accomplished in regards to how establishing greater frameworks for study and control of these new tech firms.

A. *Significance of the Study*

At the end of the article, the author hoped to answer four research questions. The first question was whether FinTech firms are financial institutions. An analysis of the relevant provisions in Federal law as well as state law suggests that FinTech firms are financial services institutions. In

fact, the wording of the sections suggested that FinTech firms are banks. The analysis of federal laws suggested that some FinTech firms might qualify as banks because they engage in the business of taking deposits from their customers. Section 24 of the legislation states that banks are the only institutions in the country authorized to engage in the business of deposit taking. State laws affirm the exclusive responsibility of banks in deposit taking by stating that chartered commercial banks are the only institutions that can accept customer deposits. The state laws expressly exclude other institutions or businesses from taking deposits from customers. The New York Banking Law offers an illustration of the legal position on issues of deposit taking under state law. Section 96 of the New York Banking Law states that chartered banks are the only institutions that can receive deposits. Similarly, section 31 of the Texas Finance Code offers a definition of banks that underlines their exclusive role in receiving deposits from customers. The Texan law states that banking entails the activities of activing deposits from customers. The wording these federal and state laws suggests that FinTech firms are corporations that are subject to the laws that regulate financial services companies because most of them engage in the business of taking deposits from their customers. This shows quite clearly how vulnerable banking customers are in regards to their monetary transactions and how FinTech firms can harm them.

The second research question was whether FinTech firms' services are compliant with laws that govern financial institutions. The analysis suggested that the founders of FinTech firms believe that their firms do not qualify as banks or financial services companies. They argue that their companies are technology companies because the provision of financial services is just a small fraction of their core business. According to these founders, the core business of financial services firms is the provision of technology services and software protocols that enable their customers to provide perform financial transactions. This argument about core services of firms in the industry is the main factor accounting for the companies' low level of compliance with existing businesses. Many FinTech firms have failed to comply with state and federal government financial services regulations by registering their businesses as financial services companies. Therefore, they continue to violate existing state and federal government laws by continuing to offer deposit taking and peer-to-peer money lending services without the requisite licenses.

The 2015 case of *North Carolina v. Western Sky Financial*[192] offered insight into the extent of FinTech firms' failure to comply with existing laws. In this case, a court in North Carolina evaluated whether the lending

192. *See North Carolina v. Western Sky Financial, LL.C.*

practices of a FinTech firm (Western Sky Financial) targeting communities in the Cheyenne River Indian Reservation were lawful. Western Sky Financial issued loans of between $850 and $10,000 to members of the community. In those loans, it charged interest rates that ranged from 86% to 342.86%.[193] The loan had a repayment period of between 12 months and 84 months. The loan agreement stated that disputes arising from the loan agreement would be subject to the Cheyenne River Indian Reservation Laws rather than federal laws or state laws. North Carolina's usury law stated that the maximum interest rate that lenders could levy on their customers was 25%.[194] The court was considering whether the practices of the FinTech firm violated this law. The court ruled that the peer-to-peer lending practices of the company violated the laws that North Carolina had enacted to protect consumers. The court argued that FinTech firm's practices implied that its objective in circumventing North Carolina's lending laws was to saddle consumers in state with loans that they could not pay. This would sink the consumers into a debt cycle that would generate significant profit for Western Sky Financial for many years. In this case, the lending practices posed difficulties to regulatory agencies because the company opted to include clauses in the loan agreement that ousted the jurisdiction of federal and state laws. Such an outcome demonstrates how FinTech firms are violating existing financial services legislations and why the enactment of better means to discover their activities and then prosecute is so sorely needed. In time, it is reasonable to assume it will only get worse as more FinTech firms come online and continue to take advantage of banking customers.

The third research question related to the main AML laws governing financial institutions. The findings from the study indicated legislative institutions at the federal government and stage government levels have enacted many laws on AML, but the most important legislations are Bank Secrecy Act of 1970 and Title 18 of the U.S.C. The relevant provisions of the BSA are section 103.22, section 103.11, section 103.23, section 103.29, and section 103.121. Section 103.22 of the BSA outlines the procedures that financial services companies must follow when filing their Currency Transaction Report (CTR). The section states that the types of financial transactions leading to CTR include currency transfers, currency exchanges, currency withdrawals, and currency deposits. Section 103.11 of the BSA outlines the organizations and institutions that are exempt from the reporting requirements under the statute. These organizations include banks in relation to their domestic operations, the domestic subsidiary of a listed company

193. *Id.*
194. *Id.*

that is not a bank, a company (other than a bank) that has listed its equity or stock on the NASDAQ, American, or New York stock exchanges, all institutions that are exercising the authority of government within the US, and all local, state or federal government agencies. Section 103.23 of the BSA states that financial institutions wishing to mail, transfer, ship, or physically transport more than $10,000 out of the US or into the US ought to file the Financial Crimes Enforcement Network (FinCEN) form. The section also outlines circumstances under which companies must file a Suspicious Activity Report. Section 103.29 of the BSA prohibits financial institutions from participating in the sale of monetary instruments whose value range between $3,000 and $10,000. The section states that financial institutions should only engage in such transactions if they have obtained and recorded information that identifies the purchaser as well as the specific transaction relating to that money. Section 103.121 of the BSA outlines the requirements for organizations to developing the CIP. The section states that banks must formulate and implement board-approved CIP procedures. The section states that the CIP must be written and the appropriate for the size and operations of the bank.

The fourth and final research question is related to the extent of FinTech firms' compliance with AML laws. An analysis of the practices of FinTech firms demonstrates they lack the will to comply with AML laws. Most of the FinTech firms operating in the virtual currencies sector have exhibited a general reluctance to adhere to existing AML Evidence suggests that FBI agents have arrested a significant proportion of the founders of FinTech firms in the virtual currencies industry. The case of Ripple Labs offers insight into the extent of FinTech firms' failure to comply with AML laws. On May 5, 2015, FinCEN and Ripple Labs Inc. agreed to an out of court settlement in which the latter corporation agreed to pay a civil fine of $700,000.[195] Ripple Labs agreed to pay the fine because evidence suggested that it repeatedly violated federal AML by failing to register its financial services business, failing to implement an AML program, and failing to report suspicious financial transactions to FinCEN.[196] This should never be allowed to continue or even happen at all.

B. *Recommendations for Future Research*

Financial technology combines the traditional financial services and technology industries to provide customers with more immediate, convenient, or efficient financial services through electronic functions and

195. *See* SIVON, *supra* note 21, at 1.
196. *Id.*

new platforms. Not only has it changed the entire financial service environment, but it has also opened up the bottleneck in the traditional financial industry's development, and many innovative services have been born as a result. Financial technology not only challenges the profitability of financial institutions, but also increases the complexity of regulatory compliance in various financial services. In this rapidly changing legal environment, statute followers need to adjust and adapt more quickly than in the past, especially in terms of transparency requirements. To address the development trend in financial technology and encourage innovation in the field, the Financial Supervisory Commission R.O.C. (Taiwan) has drawn up the "Financial Technology Innovation Experimentation Act," which covers application, review, supervision, management, and consumer protection procedures for experiments in financial technology, as well as legal adjustments and the exclusion of legal liability during the experiment period. It is currently under review by the Legislative Yuan, and, if successful, it is expected that the legislation will be completed by May of this year.[197]

In fact, the Office of the Comptroller of the Currency (OCC), the United States' banking regulator, published a draft on March 15, 2017 for the issuance of banking business licenses to the financial technology industry, and is studying the feasibility of allowing financial technology companies to apply for banking business licenses.[198] The draft of the special licensing program proposed by the OCC requires financial technology companies to comply with specific regulations in the manner of traditional banks, including higher capital and liquidity regulations, and allows financial technology companies to apply for federal chartered licenses for online loans and payment processing, saving them the trouble of applying for licenses in every state. The US OCC's decision to issue business licenses to financial technology companies stems from a consideration of public interests as well as the following three reasons: (1) financial technology companies offer major financial services to millions of Americans in real-world transactions, and special-purpose business licenses can include these companies in the framework of unified standards, supervision, and management; (2) financial technology companies must provide financial products and services to consumers based on the federal law; and (3) financial technology companies

197. Executive Yuan, Republic of China (Taiwan) (中華民國行政院), *Executive Yuan Passes Bill on FinTech Innovation and Experimentation*, EXECUTIVE YUAN PRESS RELEASES (May 4, 2017), http://english.ey.gov.tw/News_Content2.aspx?n=8262ED7A25916ABF&sms=DD07AA2ECD4290A6&s=7454512BC704082B.

198. OFFICE OF THE COMPTROLLER OF THE CURRENCY (OCC), COMPTROLLER'S LICENSING MANUAL DRAFT SUPPLEMENT: EVALUATING CHARTER APPLICATIONS FROM FINANCIAL TECHNOLOGY COMPANIES (2017), https://www.occ.treas.gov/publications/publications-by-type/licensing-manuals/file-pub-lm-fintech-licensing-manual-supplement.pdf.

can promote the prosperity, modernization, and competitiveness of the financial system, thus increasing its power. In other words, the OCC's approach to financial technology companies supports responsible innovations and encourages the Inclusive Financial System. In addition, the US's Commodity Futures Trading Commission (CFTC) is also interested in promoting the development of the emerging financial technology industry so as to allow the industry to take a big step forward in the US federal financial system. The current Acting Chairman of the CFTC, J. Christopher Giancarlo, says that he has requested the financial technology unit under the CFTC to study how the organization can promote the development of the financial technology industry, and to develop in the following three major areas: (1) using financial and technological innovation to make the CFTC a more effective regulatory body; (2) using financial and technological innovation to help the CFTC establish regulations required for the digital financial market; and (3) ensuring that the CFTC can, in addition to supervising financial markets, promote innovation in the US financial technology industry.[199]

Traditionally, and no doubt due to the fact that Taiwan's financial industry is chartered to ensure financial policy stability and the protection of market mechanisms, Taiwan's financial regulators may have been given too much power, including strong intervention and guidance capacities and a mechanism for bureaucratic review. This may very easily result in financial institutions' lack of investment in new technologies and incentive for creating new businesses. Furthermore, as Taiwan adopts a codified civil law system, unless clearly stipulated or authorized by law, regulators will not have the right to loosen the laws and regulations for specific industry participants. In view of the fact that new entrepreneurs are often engaged in cross-sector operations, in addition to cross-sector operations among banking, insurance, and securities, it would not be unusual for them to be involved in the legal aspects of telecommunications and other highly regulated industries. Specifically, the core of the problem is still with the regulatory policy's objectives and strategies. In the regulatory aspect, Taiwan's laws and regulations are still relatively strict with many controls, and its "normative-based supervision" is not conducive to competition. In addition to maintain the financial order, the regulators need to recognize that the rapid evolution of information technology and the financial industry necessitates the transition of regulatory policy from the old idea of being "financial institution-oriented" to the new idea of being "financial transaction-oriented," and financial regulators and financial policy makers must understand that the global financial capital competition is not only a

199. *Remarks of Acting Chairman J. Christopher Giancarlo before the 42nd Annual International Futures Industry Conference in Boca Raton, FL*, U.S. COMMODITY FUTURES TRADING COMMISSION (Mar. 15, 2017), http://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo-20.

competition for high-end talent and high-quality customers, but a competition as to the speed of the financial systems' enhancement. For example, in the new "The Act Governing Electronic Payment Institutions" passed in 2015, the approval system is still adopted, and there are still a number of thresholds limiting the access to the electronic payment market.[200]

The regulators need to recognize that the essence of financial technology is the integration of emerging technologies and financial services, and need to adopt classified and differentiated management in the regulatory environment and adopt a "control of neutrality" and "principle-based supervision" model, in order to not limit market participants' intention of investing in financial technology and the market competition. In the mean time, financial consumer protection and fraud prevention mechanisms, such as prudent reviews of money laundering and precautionary measures to prevent tax avoidance, must not be abandoned. If the government prioritizes the enhancement of comprehensive financial ability and expands the digital financial territory, highly supervised, large financial institutions should bear some of the responsibility for a self-benefiting and altruistic innovation due to their existing credit histories, sizes, risk control, and resource mobilization abilities, and appropriate policies should be designed for checks and balances. Specifically, in the development of financial technology, attention should be paid to a balance among the multiple objectives of financial innovation, the stability of the existing financial system, and the enhancement of the popularity and fairness of financial resources, as well as the establishment of a positive interactive symbiosis model between the financial industry and the financial technology innovation industry in order to combine the strengths of both and jointly promote innovation in financial technology and the transformation of financial services. In view of this, as the development of financial technology has become mainstreamed, designing a supervisory and legal system without hindering innovation, and creating a win-win environment for both the regulators and the financial technology industry will be an important piece of the puzzle presented by the development of financial technology.

---

200. *See* Dianzi Zhifu Jigou Guanli Tiaoli (電子支付機構管理條例) [The Act Governing Electronic Payment Institutions] § 3 (promulgated Mar. 4, 2015, effective Mar. 5, 2015, as amended June 14, 2017) (Taiwan). ("The term electronic payment institution as used in this Act shall mean a company approved by the competent authority to accept, through a network or electronic payment platform, the registration and opening of an account by users that keeps track of their funds transfer and funds deposit records (referred to as e-payment account hereunder), and use electronic equipment to convey the receipt/payment information via connection to engage in the following businesses in the capacity of an intermediary between payers and recipients, . . .").

REFERENCES

31 C.F.R. § 103.11(b).

31 C.F.R. § 103.11(uu).

31 C.F.R. § 103.121.

31 C.F.R. § 103.22.

31 C.F.R. § 103.29.

31 C.F.R. § 103.41.

31 U.S.C. § 5316.

31 U.S.C. § 5317(c).

31 U.S.C. § 5318(l).

31 U.S.C. § 5321(a).

31 U.S.C. § 5311.

Avergun, J. & Kukowski, C. (2016, April 5). Complying with AML Laws: Challenges for the Fintech Industry. *Crowdfund Insider*. Retrieved from http://www.crowdfundinsider.com/2016/04/83845-complying-with-aml-laws-challenges-for-the-fintech-industry/.

Bank Secrecy Act, 12 U.S.C. § 1829b, 12 U.S.C. §§ 1951-1959 & 31 U.S.C. §§ 5311-5332.

Barefoot, A. S. (2016). Letter of Comment: White Paper on Responsible Innovation. *Jo Ann Barefoot Group LLC*. Retrieved from https://www.occ.gov/topics/responsible-innovation/comments/comment-circle-financial.pdf.

Basel Committee on Banking Supervision (2012). *Core Principles for Effective Banking Supervision*. Switzerland: Bank for International Settlements.

Batiz-Lazo, B. & Wood, D. (2002). Diffusion of Information Technology Innovations within Retail Banking: An Historical Review. In L. A. Joia (Ed.), *IT-Based Management: Challenges and Solutions*. (pp. 235-255). New York: Idea Group Inc.

Bonney, J. (2013, June 29). Mt. Gox Registers with FinCEN as a Money Services Business. *Coindesk*. Retrieved from http://www.coindesk.com/mt-gox-registers-with-fincen-as-a-money-services-business/.

Burges Salmon LLP (2016). *Supporting the Development and Adoption of RegTech: No Better Time for a Call for Input*. Retrieved from https://www.burges-salmon.com/-/media/files/publications/open-access/supporting_the_development_and_adoption_of_regtech_no_better_tim

e_for_a_call_for_input.pdf.

CashCall Inc. v. Morrissey, 2015 U.S. Lexis 2991 (2015).

CNET News.com. (n.d.). DigiCash Files Chapter 11. Retrieved from https://www.cnet.com/news/digicash-files-chapter-11/.

CoinDesk (n.d.). Bitcoin Price Index: Closing Price. Retrieved from http://www.coindesk.com/price/.

Dianzi Zhifu Jigou Guanli Tiaoli (電子支付機構管理條例) [The Act Governing Electronic Payment Institutions], March 5, 2015, as amended June 14, 2017 (Taiwan).

Douglas, J. L. (2016). New Wine into Old Bottles: Fintech Meets the Bank Regulatory World. *North Carolina Banking Institute, 20*, 17-65. Retrieved from http://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=1391&context=ncbi.

Executive Yuan, Republic of China (Taiwan) (中華民國行政院) (2017, May 4). Executive Yuan Passes Bill on Fintech Innovation and Experimentation. *Executive Yuan Press Releases*. Retrieved from http://english.ey.gov.tw/News_Content2.aspx?n=8262ED7A25916ABF&sms=DD07AA2ECD4290A6&s=7454512BC704082B.

Eyers, J. (2016, June 20). Welcome to the New World of 'RegTech'. *Financial Review*. Retrieved from http://www.afr.com/technology/welcome-to-the-new-world-of-regtech-20160619-gpmj6k.

Federal Deposit Insurance Corporation (n.d.). Retrieved from https://www.fdic.gov/.

Financial Conduct Authority (2016). *Call for Input on Supporting the Development and Adopters of RegTech*. Retrieved from https://www.fca.org.uk/publication/feedback/fs-16-04.pdf.

Finextra Research Ltd. (2016). *A Roadmap for FinTech Standards: Executive Report.* Retrieved from https://www.bsigroup.com/LocalFiles/en-GB/PAS/Homepage/FIN_BSI_short_final.pdf.

Frizell, S. (2015, January 21). How the Feds Nabbed Alleged Silk Road Drug Kingpin 'Dread Pirate Roberts'. *Time Mag.* Retrieved from http://time.com/3673321/silk-road-dread-pirate-roberts/.

Goldman Sachs Group, Inc. (2016). *Profiles in Innovation: Blockchain*. Retrieved from www.finyear.com/attachment/758923/.

González, A. G. (2004). PayPal: the Legal Status of C2C Payment Systems.

Computer Law & Security Review, 20(4), 293-299.

Gutierrez, D. (2014, October 20). Big Data for Finance-Security and Regulatory Compliance Considerations. *InsideBIGDATA*. Retrieved from http://insidebigdata.com/2014/10/20/big-data-finance-security-regulatory-compliance-considerations/.

Hill, K. (2013, May 1). The FBI's Plan for the Millions Worth of Bitcoins Seized From Silk Road. *Forbes*. Retrieved from http://www.forbes.com/sites/kashmirhill/2013/10/04/fbi-silk-road-bitcoin-seizure/#188e0feb5c22.

Hughes, S. J. (1996). A Call for International Legal Standards for Emerging Retail Electronic Payment Systems. *Annual Review of Banking Law, 15*, 197-206.

Information Ventures Partners (2014). *Disruptions Driving FinTech Investing.* New York: Information Ventures Partners.

Institute of International Finance (2016). *Regtech in Financial Services: Technology Solutions for Compliance and Reporting*. Washington, DC: Institute of International Finance.

Kalakota, R. & Whinston, A. B. (1999). *Frontiers of Electronic Commerce*. MA: Addison-Wesley.

Kaminski, C. (2003). Online Peer-to-Peer Payments: Paypal Primes the Pump, Will Banks Follow?. *North Carolina Banking Institute, 7*(1), 378-385.

Kiviat, T. I. (2015). Beyond Bitcoin: Issues in Regulating Blockchain Transactions. *Duke Law Journal, 65*, 569-594.

Ly, M. K.-M. (2014). Coining Bitcoin's "Legal-Bits": Examining the Regulatory Framework for Bitcoin and Virtual Currencies. *Harvard Journal of Law & Technology, 27*(2), 587-608.

Madden v. Midland Funding, LLC, 786 F.3d 246 (2nd Cir. 2015).

McMillan LLP (2016). *Fintech at the Crossroads: Regulating the Revolution*. Retrieved from http://www.mcmillan.ca/Files/191422_Fintech%20at%20the%20Crossroads%20-%20Regulating%20the%20Revolution.pdf.

National Bank Act, 12 U.S.C. §§ 85-86 (1964).

North Carolina v. Western Sky Financial, LLC, 2015 NCBC Lexis 87 (2015).

Office of the Comptroller of the Currency (2017). *Comptroller's Licensing Manual Draft Supplement: Evaluating Charter Applications from Financial Technology Companies*. Retrieved from

https://www.occ.treas.gov/publications/publications-by-type/licensing-manuals/file-pub-lm-fintech-licensing-manual-supplement.pdf.

Peirce, M. & O'Mahony D. (2007). *Scalable, Secure Cash Payment for WWW Resources with the PayMe Protocol Set*. Ireland: Trinity College.

Penrose K. L. (2014). Banking on Bitcoin: Applying Anti-Money Laundering and Money Transmitter Laws. *North Carolina Banking Institute, 18*(2), 529-544.

PriceWaterHouseCoopers (2015). *Peer Pressure: How Peer-to-Peer Lending Platforms are Transforming the Consumer Lending Industry.* Retrieved from http://www.pwc.com/us/en/consumer-finance/publications/assets/peer-to-peer-lending.pdf.

Santora, M., Rashbaum, W. K. & Perlroth, N. (2013, May 28). Online Currency Exchange Accused of Laundering $6 Billion. *New York Times*. Retrieved from http://www.nytimes.com/2013/05/29/nyregion/liberty-reserve-operators-accused-of-money-laundering.html?pagewanted=1&_r=0.

Sironi, P. (2016). My Robo Advisor Was an iPod-Applying the Lessons from Other Sectors to FinTech Disruption. In S. Christi & J. Barberis (Eds.), *The FinTech Book: The Financial Technology Handbook for Investors*. (pp. 152-159). New York: Wiley.

Sivon, J. (2015). *Fintech and the Existing Legal Framework for Anti-Money Laundering and Counter-Terrorism Financing*. Retrieved from http://www.bsnlawfirm.com/newsletter/OP1506_Sivon.pdf.

Taft J. P. (2002). Internet-Based Payment Systems: An Overview of the Regulatory and Compliance Issues. *Consumer Finance Law Quarterly Report, 56*, 42-47.

Texas Financial Code § 393.222 (2005).

Todd, S. & McKendry, I. (2015, May 6). What Ripple's FinCEN Fine Means for the Digital Currency Industry. *American Banker*. Retrieved from https://www.americanbanker.com/news/what-ripples-fincen-fine-means-for-the-digital-currency-industry.

U.S. Attorney's Office (2013, October 25). Manhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of "Silk Road" Website. *FBI*. Retrieved from https://archives.fbi.gov/archives/newyork/press-releases/2013/manhattan-u.s.-attorney-announces-seizure-of-additional-28-million-worth-of-bitcoins-belonging-to-ross-william-ulbricht-alleged-owner-and-operator-o

f-silk-road-website.

U.S. Attorney's Office, Southern District of New York (2016, May 6). Liberty Reserve founder Arthur Budovsky Sentenced in Manhattan Federal Court to 20 Years for Laundering Hundreds of Millions of Dollars through His Global Digital Currency Business. *U.S. Department of Justice*. Retrieved from https://www.justice.gov/usao-sdny/pr/liberty-reserve-founder-arthur-budovsky-sentenced-manhattan-federal-court-20-years.

U.S. Code Title 18-Crimes and Criminal Procedure, Pub. L. 114-38 (2016).

U.S. Commodity Futures Trading Commission (2017, March 15). Remarks of Acting Chairman J. Christopher Giancarlo before the 42nd Annual International Futures Industry Conference in Boca Raton, FL. Retrieved from http://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo-20.

U.S. Department of the Treasury (2016). *Opportunities and Challenges in Online Marketplace Lending*. Washington DC: U.S. Department of the Treasury.

Xu, X. M., Duan, Y. & Li, Y. (2002). IT-Enabled Strategic Marketing Management, in IT-Based Management: Challenges and Solutions. In L. A. Joia (Ed.), *IT-Based Management: Challenges and Solutions*. (pp. 217-234). New York: Idea Group Inc.

Zagaris, B. (2015). *International White Collar Crime: Cases and Materials.* Washington, DC: Cambridge University Press.

金融科技創新與反洗錢防制規範

吳 盈 德

摘 要

金融科技創新在全球金融服務業尚未意識到之下，已經迅速的崛起和成長。本文分析了金融科技創新產業在美國的反洗錢防制法的遵循現況。首先，主要兩項法律涉及與洗錢防制有關的規範，這兩項法律是1970年的銀行保密法和組織犯罪控制法。銀行保密法為關於洗錢問題的專門性法律，該法規範了銀行和其他金融服務機構必須遵守的規定，以確保其服務符合反洗錢防制法。然而，組織犯罪控制法僅規範及定義利用金融工具的洗錢犯罪。再者，金融科技創新公司並不會主動遵守反洗錢防制法，因為大多數的金融科技創新公司並不認為自己是金融服務業。事實上，他們的商業模式與現有的反洗錢防制法規定並不一致，然而這種不願意遵守反洗錢防制法的做法使他們面臨訴訟，相關資料顯示，部分業者因為未能遵守反洗錢防制規範，而被判處20年刑期。最後，本論文以法制規定的綜合討論及要件評析作為結論。

關鍵詞： 金融科技、反洗錢防制法、銀行保密法、組織犯罪控制法、反洗錢防制規範