Brooklyn Journal of Corporate, Financial & Commercial Law

Volume 10 | Issue 2 Article 7

2016

The Sixth Pillar of Anti-Money Laundering Compliance: Balancing Effective Enforcement with Financial Privacy

Maria A. de Dios

THE SIXTH PILLAR OF ANTI-MONEY LAUNDERING COMPLIANCE: BALANCING EFFECTIVE ENFORCEMENT WITH FINANCIAL PRIVACY

ABSTRACT

The U.S. government has responded to the increase of financial crimes, including money laundering and terrorist financing, by requiring that financial institutions implement anti-money laundering compliance programs within their institutions. Most recently, the Financial Crimes Enforcement Network exercised its regulatory powers, as authorized by the Treasury Department, by proposing regulations that now explicitly add customer due diligence to the preexisting anti-money laundering regime. The policy behind the government's legislative and regulatory measures is clear—financial institutions must ensure that they are protected from and not aiding in the illegal efforts of criminals. The complexity and insidiousness of these financial crimes makes it difficult for the government to act solely and without the compliance of financial institutions. Although national security and the protection of the global economy are urgent priorities, all legislative actions or considerations need to be sensitive to personal privacy.

This Note examines the criminal activity and legislative history that has necessitated the proposal of such regulations, the burdens that compliance places on financial institutions, and the technology that aids these financial institutions in their compliance efforts. As a result of these compliance obligations and the potential penalties for non-compliance, customer privacy is not always guaranteed. Existing privacy laws do not sufficiently ensure that customer financial information is adequately protected; rather, these privacy laws allow privacy invasions for the sake of compliance with anti-money laundering legislation and, as a result, are often inadequate and insufficient when compared to international privacy schemes. It is important to find a balance between the need to protect national security, the requirements placed on financial institutions, and the rights customers have to financial privacy. The global nature of financial networks and of these illicit activities warrants concerted efforts by governments domestically and abroad to ensure that compliance does not result in unwarranted financial privacy invasions.

Until a global system can be established, this Note proposes that the currently proposed regulations be amended to mandate privacy programs within financial institutions. Financial institutions should develop privacy policies and procedures that will work with their already existing anti-money laundering compliance programs and should ensure that their compliance and privacy focused personnel coordinate their efforts so that

regulatory compliance neither detrimentally impacts the way they conduct their business nor betrays their customers' right to privacy.

INTRODUCTION

On the evening of May 2, 2011, President Barack Obama addressed the United States and the world to report that the United States successfully "conducted an operation that killed Osama bin Laden, the leader of al Qaeda, and [the] terrorist . . . responsible for the murder of thousands of innocent men, women, and children."[1] Unfortunately, this announcement did not bring an end to terrorism. The news today is flooded with reports on the Islamic State of Iraq and al-Sham or the Levant (Islamic State),[2] a terrorist group with a "nihilistic view and genocidal agenda."[3] David Cohen, the Treasury Department's Undersecretary for Terrorism and Financial Intelligence, acknowledged that the Islamic State might be the best-funded terrorist group ever confronted.[4] The Islamic State is a different type of beast. It has not responded to typical efforts to cut terrorist financing through the international system, specifically because of its quick adaptability to disruptions to its illicit activities and funding.[5] The U.S. Department of the Treasury (Treasury Department) has estimated that in 2014, the Islamic State made about one to three million dollars per day.[6] Its funding comes from oil, donations from "wealthy sympathizers,"[7] kidnappings, and "unregistered charitable organizations."[8] The Treasury Department has sanctioned individuals that have financed the Islamic State and other terrorist groups.[9] However, it still remains uncertain what impact these sanctions actually have, because much of the Islamic State's funds are derived from criminal activities. As it stands, these sanctions are "designed

1. Macon Phillips, *Osama Bin Laden Dead*, THE WHITE HOUSE BLOG (May 2, 2011, 12:16 AM), http://www.whitehouse.gov/blog/2011/05/02/osama-bin-laden-dead.

2. *See, e.g.*, Ray Sanchez, *ISIS, ISIL or the Islamic State?*, CNN (Jan. 23, 2015, 6:00 PM), http://www.cnn.com/2014/09/09/world/meast/isis-isil-islamic-state/index.html. The group's name varies by those using it. The Government has referred to the terrorist group as ISIL, while much of the media uses ISIS. The group refers to itself as the Islamic State.

3. John Kerry, *To Defeat Terror, We Need the World's Help*, N.Y. TIMES, Aug. 30, 2014, at A21.

4. Ana Swanson, *How the Islamic State Makes its Money*, THE WASH. POST (Nov. 18, 2015), https://www.washingtonpost.com/news/wonk/wp/2015/11/18/how-isis-makes-its-money/.

5. *Id.*

6. *Id.*

7. Scott Bronstein & Drew Griffin, *Self-Funded and Deep-Rooted: How ISIS Makes its Millions*, CNN: WORLD (Oct. 7, 2014, 9:54 AM), http://www.cnn.com/2014/10/06/world/meast/isis-funding/.

8. Swanson, *supra* note 4.

9. Julie Hirschfeld Davis, *Treasury Imposes Terrorism Sanctions*, N.Y. TIMES (Sept. 24, 2014), http://www.nytimes.com/2014/09/25/world/middleeast/treasury-imposes-terrorism-sanctions-on-those-linked-to-islamic-state.html.

to publicly expose key players in the group, with the goal of isolating them and restricting their access to money and freedom of movement."[10]

Government efforts to deter terrorist financing and money laundering are not new. In 1970, Congress enacted the first of its anti-money laundering (AML) legislation, the Currency and Foreign Transactions Reporting Act, commonly referred to as the Bank Secrecy Act (BSA).[11] After the September 11, 2001 terrorist attacks (9/11) against the United States, President Bush signed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Patriot Act).[12] Title III of the Patriot Act, the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001, amended the BSA and focused on money laundering and terrorist financing.[13] Under the BSA, as amended by Title III of the Patriot Act, the Secretary of the Treasury is authorized to issue regulations establishing AML programs within financial institutions to assist with various matters, including counterterrorism.[14]

The Financial Crimes Enforcement Network (FinCEN) is a bureau within the Treasury Department that "safeguard[s] the financial system from illicit use and combat[s] money laundering and promote[s] national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities."[15] FinCEN's Director has been authorized by the Treasury Department to "implement, administer, and enforce compliance with the BSA and associated regulations."[16] FinCEN, recently proposed rules that impose various reporting requirements and obligations on financial institutions, including mandatory customer due diligence (CDD) procedures for the purpose of assisting with BSA compliance efforts.[17] FinCEN's proposed rules now explicitly mandate that financial institutions know their customers because "both who they are and what transactions they conduct—is a critical aspect of combating all forms of illicit financial activity," which includes terrorist financing and "the evasion to more traditional financial crimes."[18] These rules, though necessary for combating financial crimes, pose a danger to client privacy rights, despite having the Gramm-Leach-Bliley Act

---

10. *Id.*

11. Currency and Foreign Transactions Reporting Act, Pub. L. No. 91-508, 84 Stat. 1114 (1970) (codified as amended in scattered sections of 12 & 31 U.S.C.).

12. USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered sections of 18 U.S.C. (2012)).

13. *Id.*

14. *What We Do*, U.S. DEP'T OF TREASURY: FIN. CRIMES ENFORCEMENT NETWORK, http://www.fincen.gov/about_fincen/wwd/ (last visited Nov. 3, 2015).

15. *Id.*

16. *Id.*

17. Customer Due Diligence Requirements for Financial Institutions, 79 Fed. Reg. 45,151, 45,152 (proposed Aug. 4, 2014) (to be codified at 31 C.F.R. pts. 1010, 1020, 1023, 1024, 1026).

18. *Id.*

(GLBA)[19] in place to deal with financial privacy. Congress, in Title V of the GLBA, acknowledged that financial institutions have a duty to respect and protect the privacy of their customers.[20] Though the GLBA protects privacy rights in certain respects, it permits financial reporting to comply with FinCEN's requests.[21]

Because of the sophistication of terrorist groups like the Islamic State, distinguishing the legitimacy of funding to terrorist groups is not easy.[22] For example, donations "from the Persian Gulf and other sympathetic corners of the world, witnessing the humanitarian crisis in Syria, have been funneling money to the most effective forces fighting . . . [the Islamic State]."[23] Determining whether funds have been transferred for the purposes of aiding Syrian refugees or supporting terrorism has proven difficult.[24] As two experts in the field have explained in a *New York Times* editorial:

> [The Islamic State] is also a leader in using new technologies and social media to raise awareness and reach individual donors. Appeals for donations (or investments) are tweeted while money is raised and sent via the Internet, then withdrawn in the form of bags of cash to be transported into the war zones . . . . If we hope to constrict these global and local fund-raising streams, and the dangerous ambitions of terrorist groups, we need a renewed campaign against terrorist financing.[25]

As these terrorist groups continue to develop and become more sophisticated, the U.S. government will need to advance its initiatives combating terrorist financing and money laundering. In fact, this process has already begun. Many government agencies, and now even financial institutions, have been using computerized technology such as that provided by Palantir Technologies, Inc. (Palantir).[26] Palantir provides data mining and analysis programs that can assist the government with counterterrorism efforts[27] and help with "unraveling complex financial crimes."[28] Because of Palantir's superior technological capabilities, it can quickly assist financial

---

19. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 and 15 U.S.C.).

20. *Id.* § 501(a)

21. David E. Teitelbaum & Karl F. Kaufmann, *Current Developments in Anti-Money Laundering Laws*, 58 BUS. L. 1149, 1155 (2002).

22. *See* Juan C. Zarate & Thomas M. Sanderson, *How the Terrorists Got Rich: In Iraq and Syria, ISIS Militants Are Flush With Funds*, N.Y. TIMES (June 28, 2014), http://www.nytimes.com/2014/06/29/opinion/sunday/in-iraq-and-syria-isis-militants-are-flush-with-funds.html?_r=0.

23. *Id.*

24. *See id.*

25. *Id.*

26. PALANTIR, https://www.palantir.com (last visited Nov. 3, 2015).

27. Ashlee Vance & Brad Stone, *Palantir, the War on Terror's Secret Weapon*, BUS. WK. MAG. (Nov. 22, 2011), http://www.businessweek.com/magazine/palantir-the-vanguard-of-cyberterror-security-11222011.html.

28. *About*, PALANTIR, http://www.palantir.com/about/ (last visited Mar. 10, 2016).

institutions in their compliance efforts. This leaves open the question of how well privacy is really protected since neither the GLBA nor FinCEN's proposed rules adequately address this problem.

Regulators and financial institutions must be constantly vigilant in balancing their concurrent obligations to navigate between the *Scylla* of compliance, on the one hand, and the *Charybdis* of privacy obligations to customers, on the other.[29] While national security is of utmost importance, the protection of client privacy rights is also imperative and must not be quickly disregarded. The government should consider these privacy interests when refining its AML laws.

This Note examines the privacy law implications facing financial institutions' adoption of CDD programs consistent with FinCEN's proposed regulations. Part I of this Note examines the legislative history behind FinCEN's proposed rules, which attempt to establish a uniform system of CDD requirements for financial institutions, and then analyze them. Part II discusses the current requirements that require financial institutions to know their customers, and will review Palantir as a new tool that financial institutions increasingly use to aggregate the information necessary to comply with AML program requirements. Part III analyzes the history of financial privacy rights, focusing on the GLBA, and then will discuss the potential invasions of customer privacy that may result from complying with CDD regulations. This Note concludes that because more coherent and standardized regulation of privacy in the United States seems unlikely, FinCEN should take active steps to mandate all financial institutions to have privacy groups responsible for testing and auditing their institution's compliance procedures and policies to ensure that they more diligently safeguard customer privacy in conformity with international privacy law.

I. LEGISLATIVE HISTORY

A. AML LEGISLATION'S BEGINNINGS

The increasing rampancy of illicit activity from money laundering, terrorist financing, and drug trafficking—nationally and globally—has compromised financial institutions and necessitated the creation of legislation intended to safeguard against such crimes.[30] Initially, the Treasury Department, Securities and Exchange Commission, and

---

29. *Scylla and Charybdis*, ENCYCLOPAEDIA BRITANNICA, www.britannica.com/EBchecked/topic/530331/Scylla-and-Charybdis (last updated June 16, 2015). Scylla and Charybdis are "two immortal and irresistible monsters who beset the narrow waters traversed by the hero Odysseus in his wanderings described in Homer's, *Odyssey*, Book XII . . . . To be "between Scylla and Charybdis" means to be caught between two equally unpleasant alternatives." *Id.*

30. *See* Mark E. Plotkin & B.J. Sanford, *Patriot Act: Customer's View of "Know Your Customer"—Section 326 of the U.S.A. Patriot Act*, 1 BLOOMBERG CORP. L.J. 670, 671 (2006).

Department of Justice lobbied Congress for legislation requiring banks to keep records that would assist with their fight against organized crime.[31] While concerns about the potential invasion of financial privacy and the burden on financial institutions were considered, Congress quickly devalued their importance as "law enforcement concerns . . . outweighed the burden[s] to financial institutions."[32]

As a result, the BSA was enacted and is considered "the fundamental U.S. statute aimed at deterring and detecting . . . financial crimes."[33] Originally, under the BSA, banks were required to maintain records[34] that would assist with investigations and proceedings related to financial crimes.[35] Specifically, "[t]he BSA was designed to help identify the source, volume, and movement of currency and other monetary instruments transported or transmitted into or out of the United States or deposited in financial institutions."[36] The BSA's requirements for AML compliance programs within financial institutions were supposed to help the government and its regulators work toward achieving their goals of ultimately protecting against the increase in financial crimes.[37] Inconsistent application of these requirements, however, meant that BSA's actual impact was hardly felt for the first ten years after its enactment.[38] In response to its "ineffectiveness," Congress responded by enacting a multitude of other money laundering legislation.[39] Much like the BSA, however, the costs and effort that compliance with such legislation requires continue to burden the financial industry and have yet to be proven effective.[40]

As the evolving climate with respect to financial crimes prompted the enactment of legislation and, in turn, active government involvement, a need for more stringent regulation of financial institutions led to the

---

31. Daniel Mulligan, Comment, *Know Your Customer Regulations and the International Banking System: Towards a General Self-Regulatory Regime*, 22 FORDHAM INT'L L.J. 2324, 2336 (1998).

32. *Id.* at 2338.

33. Plotkin & Sanford, *supra* note 30, at 671.

34. *Statutes & Regulations: Bank Secrecy Act*, U.S. DEP'T TREASURY: FIN. CRIMES ENFORCEMENT NETWORK, www.FinCEN.gov/statutes_regs/bsa/ (last visited Nov. 3, 2015). The BSA "requires financial institutions to keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding $10,000 (daily aggregate amount), and to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities." *Id.*

35. Plotkin & Sanford, *supra* note 30, at 671.

36. FED. FIN. INSTITUTIONS EXAMINATION COUNCIL, BANK SECRECY ACT/ANTI-MONEY LAUNDERING EXAMINATION MANUAL 7 (2010) [hereinafter FFIEC MANUAL], http://www.ffiec.gov/bsa_aml_infobase/documents/bsa_aml_man_2010.pdf.

37. *See id.*

38. Mulligan, *supra* note 31, at 2340.

39. *Id.* at 2340–44 (discussing the Money Laundering Control Act of 1986, the Financial Institutions Reform, Recovery and Enforcement Act of 1989, the Comprehensive Drug Abuse Prevention and Control Act of 1970, and the Anti-Drug Abuse Act of 1988).

40. *Id.* at 2344.

proposed "Know Your Customer" (KYC) regulations.[41] KYC guidelines were not codified, but the Treasury Department still delegated authority to federal agencies to require that financial institutions establish and maintain internal procedures in compliance with the BSA reporting requirements.[42] Initial efforts at mandating KYC regulations obligated financial institutions to identify customers and the sources of their funds, analyze transactional behaviors of customers, monitor customer activity against patterns, and report suspicious activities or discrepancies in patterns to the government.[43] Failure to act carefully and diligently in implementation of these requirements resulted in criminal and civil liability for financial institutions.[44] The concern regarding the financial burdens imposed on financial institutions,[45] when coupled with the increased potential for criminal liability,[46] resulted in "overwhelming public opposition" to the KYC regulations.[47] Ultimately, the concern that KYC obligations would result in a "massive invasion of financial privacy" led to withdrawal of the KYC proposals.[48] Despite their withdrawal, the concern remains, "as KYC principles are imbedded in the U.S. anti-money laundering regime."[49] As such, many financial institutions have voluntarily adopted these measures, viewing them as necessary to ensure their compliance with the suspicious activity reporting requirements that federal regulators impose.[50] The regulatory outlook for financial institutions became even more burdensome following the terrorist attacks on 9/11.

9/11 prompted further action by the U.S. government. Congress enacted the Patriot Act[51] five weeks after these attacks, with the intention of "providing law enforcement and intelligence agencies the tools to deter and apprehend terrorists."[52] Title III of the Patriot Act amended the BSA by imposing additional requirements originally considered prior to 9/11,

---

41. *Financial Privacy, Reporting Requirements Under the Bank Secrecy Act and the "Know Your Customer" Regulations: Hearing Before the H. General Oversight/Financial Institutions Subcommittees Joint Hearing on Bank Secrecy Act Reporting Requirements*, 106th Cong. (1999) (statement of Gregory Nojeim, Legislative Counsel, American Civil Liberties Union) [hereinafter *Financial Privacy Hearing*], https://www.aclu.org/technology-and-liberty/financial-privacy-reporting-requirements-under-bank-secrecy-act.

42. Mulligan, *supra* note 31, at 2359.

43. *Financial Privacy Hearing*, *supra* note 41.

44. Mulligan, *supra* note 31, at 2364.

45. H.R. REP. NO. 101-446, at 25 (1990) (stating that "Congress must recognize that compliance by the financial community with the Bank Secrecy Act is difficult and costly").

46. Mulligan, *supra* note 31, at 2364.

47. *Financial Privacy Hearing*, *supra* note 41; *see also* Mulligan, *supra* note 31, at 2364–65 (discussing the "overwhelming negative reactions to the proposed regulations.").

48. *Financial Privacy Hearing*, *supra* note 41.

49. Mulligan, *supra* note 31, at 2326 (citing 12 C.F.R. § 21.21 (1999)).

50. *Financial Privacy Hearing*, *supra* note 41.

51. USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended in scattered sections of 18 U.S.C. (2012)).

52. Plotkin & Sanford, *supra* note 30, at 670.

"transform[ing] the BSA enforcement climate and elevat[ing] the rigor with which existing BSA requirements were applied."[53] Against the emotional backdrop of 9/11, enactment of Title III allowed for the implementation of KYC processes that had been widely criticized prior to 9/11.[54] Specifically, section 326 of Title III authorized the Secretary of the Treasury to establish regulations that would force financial institutions to discharge reasonable procedures designed to verify customer identity at account opening, maintain records of information necessary for customer identification, and compare identified persons to known lists of suspected terrorists provided by government agencies.[55]

In 2003, FinCEN, along with various agencies, issued joint final rules[56] that implemented section 326 of the Patriot Act, and required financial institutions to establish a Customer Identification Program (CIP) within their institutions.[57] CIP requires sufficient customer identification at account opening and appropriate procedures to verify customer identities.[58] In addition to CIP procedures, financial institutions must collect any customer information that will assist with CDD compliance.[59] CDD, unlike the CIP requirement, is not explicitly required by section 326 of the Patriot Act, "but rather is imposed on [financial institutions] by their regulators as part of the supervisory process."[60] Because CDD procedures are not specifically mandated by regulation, there is a lack of consistency with respect to the policies and procedures used among financial institutions when implementing them.[61] It is with this legislative and regulatory background that FinCEN's recently proposed CDD rules must be analyzed.

B. FINCEN AND ITS RECENTLY PROPOSED RULES

FinCEN commenced operations in 1990 and provides an analytical network across U.S. government agencies that aids in domestic and

---

53. *Id.* at 671.

54. *See id.* at 672 (discussing 9/11's "political momentum" in allowing for KYC's re-consideration).

55. USA PATRIOT Act § 326.

56. Joint Final Rule: Customer Identification Program for Banks, Savings Associations, Credit Unions and Certain Non-Federally Regulated Banks, 68 Fed. Reg. 25,090 (2003).

57. John Coyle, *The Legality of Banking the Undocumented,* 22 GEO. IMMIGR. L.J. 21, 26 (2007).

58. *The Bank Secrecy Act and the USA PATRIOT Act Before H. Comm. on Int'l Rel.*, 108th Cong. (2004) [hereinafter *BSA Hearing*] (testimony of Herbert A. Biern, Senior Associate Director of Banking Supervision and Regulation), http://www.federalreserve.gov/boarddocs/testimony/2004/20041117/ ("The CIP must include account-opening procedures that specify the identifying information that will be obtained from each customer, and it must include reasonable and practical risk-based procedures for verifying the customer's identity.").

59. Plotkin & Sanford, *supra* note 30, at 677.

60. *Id.*

61. *See id.* (stating that "each bank has been left to devise its own CDD program based on a mix of guidance from regulators, advice from counsel and consultants, and the lessons of its own experience").

international law enforcement efforts against financial crimes (e.g., money laundering and terrorist financing).[62] With its investigative functions comes the responsibility to collect and analyze financial information that will enable it to generate suspect lists to provide to the appropriate law enforcement agency.[63] FinCEN also has regulatory powers that come from the BSA:

> which authorizes the Secretary of the Treasury (Secretary) to require financial institutions to keep records and file reports that 'have a high degree of usefulness in criminal . . . investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, . . . to protect against international terrorism.' The Secretary has delegated to the Director of FinCEN the authority to implement, administer and enforce compliance with the BSA and associated regulations.[64]

In 2012, FinCEN issued an Advance Notice of Proposed Rulemaking (ANPRM),[65] and in August 2014, it issued the Notice of Proposed Rulemaking (NPRM).[66] FinCEN promulgated the ANPRM and subsequent NPRM for the purposes of addressing and resolving financial institutions' inconsistent efforts at establishing CDD programs.[67]

The ANPRM was intended to "codify, clarify, consolidate, and strengthen existing CDD regulatory requirements and supervisory expectations."[68] FinCEN released this ANPRM to give financial institutions, covered and not covered by the proposed regulation, an opportunity to submit comments regarding FinCEN's intention to explicitly require the implementation of CDD programs within financial institutions.[69] According to FinCEN, the need for regulation results from "[t]he requirement that a financial institution know its customers, and the risks presented by its customers, [which] is basic and fundamental to the development and implementation of an effective BSA/AML compliance program."[70] FinCEN issued its ANPRM to address the inconsistencies

---

62. Matthew N. Kleiman, Comment, *The Right to Financial Privacy Versus Computerized Law Enforcement: A New Fight in an Old Battle*, 86 NW. U. L. REV. 1169, 1172 (1992).

63. *Id.*

64. Customer Due Diligence Requirements for Financial Institutions, 77 Fed. Reg. 13,046, 13,046 (proposed March 5, 2012) (to be codified at 31 C.F.R. ch. X).

65. *Id.*

66. *See* Customer Due Diligence Requirements for Financial Institutions, 79 Fed. Reg. 45,151, 45,152 (proposed Aug. 4, 2014) (to be codified at 31 C.F.R. pts. 1010, 1020, 1023, 1024, 1026).

67. *Id.* at 45,154 (stating that "[a]t public hearings held after the comment period to the ANPRM . . . financial institutions described widely divergent CDD practices . . . . FinCEN believes that this disparity adversely affects efforts to mitigate risk and can promote an uneven playing field across and within financial sectors").

68. Customer Due Diligence Requirements for Financial Institutions, 77 Fed. Reg. at 13,046.

69. *Id.* at 13,046–47. Up until the ANPRM, there has been no regulation explicitly mandating the implementation of a specific type of CDD program. Instead, it is implicit in regulations requiring these institutions to implement BSA compliance programs intended to comport with recordkeeping and reporting obligations under the BSA.

70. *Id.*

plaguing CDD policies across institutions, believing that its explicit CDD rules would assist in government efforts to safeguard the country's financial system against financial crimes.[71]

The financial industry responded negatively to the ANPRM and FinCEN subsequently conducted roundtable meetings across the country to solicit feedback from members of the industry.[72] Industry members criticized the proposed rule for "the potential costs and practical challenges associated with a categorical requirement to obtain beneficial ownership information."[73] Private sector individuals emphasized primarily the burdens an additional requirement of identifying beneficial ownership would have. In response, on August 4, 2014, FinCEN released its NPRM, which addressed the primary qualms of commentators, but no mention of customer privacy rights was made in the proposed rules. Financial privacy concerns again took a backseat as the financial sector's focus on economic burdens arising from the implementation of FinCEN's regulation proved to be more controversial.[74] FinCEN rationalized the proposed regulations in the NPRM by articulating the advantages of improved CDD requirements.[75]

The NPRM aims to amend existing AML requirements with "explicit rules."[76] Before FinCEN's NPRM, the agency's AML regulatory framework had four pillars that include: (i) the creation of internal policies, procedures, and controls; (ii) the appointment of a compliance officer; (iii) ongoing training for employees; and (iv) the implementation of an independent audit program for purposes of testing procedures.[77] The NPRM seeks to add a fifth pillar to AML compliance programs. This fifth pillar is intended to supplement the existing four pillars already set forth by federal functional regulators or appointed self-regulatory organizations[78] and the BSA,[79] as amended by Title III, section 352 of the Patriot Act.[80] The fifth pillar's four elements of CDD require: (i) identification and verification of customer identity; (ii) identification and verification of beneficial owners of legal entities; (iii) understanding the nature and purpose of customer

71. *See id.* (discussing FinCEN's belief that an explicit rule would strengthen CDD expectations and enhance efforts to combat illicit crimes).

72. *Financial Services Flash Report: FinCEN Issues Long-Awaited NPR: Beneficial Ownership, Customer Due Diligence and a Fifth Pillar of AML Compliance*, PROTIVITI (Aug. 5, 2014), http://www.protiviti.com/en-US/Documents/Regulatory-Reports/Financial-Reporting/Financial-Services-Flash-Report-FinCEN-NPR-%20Beneficial-Ownership-CDD-080514-Protiviti.pdf.

73. Customer Due Diligence Requirements for Financial Institutions, 79 Fed. Reg. 45,151, 45,154 (proposed Aug. 4, 2014).

74. Robert S. Pasley, *Privacy Rights v. Anti-Money Laundering Enforcement*, 6 N.C. BANKING INST. 147, 150 (2002).

75. Customer Due Diligence Requirements for Financial Institutions, 79 Fed. Reg. at 45,153.

76. *Id.* at 45,152.

77. 31 U.S.C. § 5318(h)(1)(A)–(D) (2012).

78. Customer Due Diligence Requirements for Financial Institutions, 79 Fed. Reg. at 45,166.

79. 31 U.S.C. § 5318(h)(1).

80. USA PATRIOT Act, Pub. L. No. 107-56, § 352, 115 Stat. 272, 322 (2001) (codified as amended in scattered sections of 18 U.S.C. (2012)).

relationships; and (iv) ongoing monitoring and updating of customer identification for the purposes of identifying and reporting suspicious transactions.[81] Financial institutions that must comply with the regulations should conduct a risk-management assessment, "consistent with their obligation to identify and report suspicious activities."[82] Explicitly adding CDD as a fifth pillar allows FinCEN to further its mission of safeguarding against money laundering and terrorist financing.[83] FinCEN released its final rules as this Note went to press.[84] Part II explains how FinCEN's proposed rule fits within the broader AML regulatory framework.

II. COMPLIANCE

A. CURRENT MEASURES EMPLOYED BY FINANCIAL INSTITUTIONS

Money laundering and terrorist financing are two primary reasons for the creation of AML legislation (i.e., the BSA and the Patriot Act). Under the BSA, financial institutions are responsible for developing and implementing procedures to aid in the detection and prevention of money laundering and terrorist financing.[85] The goal is to deprive money launderers and terrorists of their ability to conceal their money trail and ultimately minimize and prevent their ability to do harm—without money, they cannot continue their illicit crimes.[86] To assist with efforts to identify money laundering, terrorist financing, and other illicit activity, financial institutions "[u]nder the [BSA], . . . must develop administer, and maintain a program that ensures compliance with the BSA and its implementing regulations, . . . and each federal banking agency, including the Federal Reserve, has specific rules requiring such programs."[87]

Under the traditional BSA framework, financial institutions must file a Currency Transaction Report (CTR) for each transaction in excess of $10,000.[88] In response to 9/11 and the enactment of the Patriot Act, KYC measures that had been considered and rejected well before 9/11 were accepted to supplement the BSA.[89] KYC has two principal components:[90] "a CIP with risk-based procedures that enable the institution to form a

81. Customer Due Diligence Requirements for Financial Institutions, 79 Fed. Reg. at 45,155.

82. *Id.* at 45,165.

83. *Id.* at 45,152.

84. Customer Due Diligence for Financial Institutions, 81 Fed. Reg. 29,398 (May 11, 2016) (31 C.F.R. pts. 1010, 1020, 1023, et al.). The final rules are effective as of July 11, 2016 and require that all covered financial institutions comply by May 11, 2018.

85. Richard D. Horn & Shelby J. Kelley, *The Bank Secrecy Act: Are There Still Secrets in Banking?*, 1 PRIV. & DATA SEC. L.J. 781, 782 (2006).

86. *Id.*

87. *BSA Hearing*, *supra* note 58.

88. 31 C.F.R. § 103.22 (2008).

89. Plotkin & Sanford, *supra* note 30, at 671–72. ("The 9/11 terrorist attacks added new political momentum to [KYC's] consideration.").

90. *Id.*

reasonable belief that it knows the true identity of its customers"[91] and CDD.[92] The obligations under a CIP include aggregation of identifying information, verification of customer identities, maintenance of records of all identifying information and documentation, comparison of such identifying information with government lists, and notification to customers that the information is required.[93] To assist in the identification of suspicious activity, financial institutions are encouraged to implement a CDD program that determines risk levels associated with accounts and transactions, and gathers information.[94] As noted earlier, CDD "is not mentioned in any law or regulation, but rather is imposed on [financial institutions] by their regulators as part of the supervisory process."[95]

While CIP is for customer identity verification, CDD is intended to enable financial institutions to anticipate customer behavior and help identify customers whose risk levels warrant the possible termination of the business relationship.[96] Financial institutions have inconsistently applied CDD procedures because of the lack of direction and specificity regarding what CDD programs require.[97] Moreover, financial institutions with international clientele face heightened CDD and enhanced due diligence compliance requirements under section 312 of the Patriot Act.[98] These additional requirements include the maintenance of additional records or reports and identification of foreign beneficial owners.[99]

Furthermore, financial institutions must report criminal or suspicious activity, known or suspected, to the government by way of a suspicious activity report.[100] A suspicious activity report is required when there is: (1) suspected "insider abuse involving any amount[;]" (2) a violation "aggregating $5,000 or more where a suspect can be identified[;]" (3) a violation "aggregating $25,000 or more regardless of potential suspects[;]" or (4) a transaction "aggregating $5,000 or more that involve potential money laundering or violate the Bank Secrecy Act."[101]

---

91. FFIEC MANUAL, *supra* note 36, app., R-2.
92. Plotkin & Sanford, *supra* note 30, at 672.
93. 31 C.F.R. § 103.121(b)(2)–(5).
94. *BSA Hearing*, *supra* note 58.
95. Plotkin & Sanford, *supra* note 30, at 677.
96. *Id.*
97. *Id.* ("[E]ach bank has been left to devise its own CDD program based on a mix of guidance from regulators, advice from counsel and consultants, and the lessons of its own experience.").
98. *See* Alan E. Sorcher, *Lost in Implementation: Financial Institutions Face Challenges Complying with Anti-Money Laundering Laws*, 18 TRANSNAT'L L. 395, 401–402 (2005) (discussing more extensive due diligence procedures for foreign financial institutions).
99. Eric J. Gouvin, *Bringing Out the Big Guns: The USA Patriot Act, Money Laundering, and the War on Terrorism*, 55 BAYLOR L. REV. 955, 972 (2003) (outlining the special measures required of financial institutions for its foreign accounts).
100. *BSA Hearing*, *supra* note 58.
101. 12 C.F.R. § 21.11(c)(1)–(4) (2005).

B. ADVENT OF TECHNOLOGY: NEW TOOLS TO ASSIST WITH REGULATION COMPLIANCE

FinCEN: (1) gathers financial records and data from agencies at all levels; (2) analyzes the records and data for evidence of any financial crimes; and (3) provides its findings to law enforcement agencies domestically and internationally.[102] Central to FinCEN's operations is a database that accumulates any and all information that will aid in effective law enforcement.[103] The system's sophistication allows it to "perform as many as eighty searches simultaneously, and can serve two hundred users at a time."[104] FinCEN's analytical role in helping to combat financial crimes assists law enforcement personnel with their investigations.[105] Financial institutions simultaneously provide FinCEN and other federal supervisory agencies with reports of suspicious activities, an activity that Congress has recognized places a "substantial burden" on these institutions.[106]

Palantir has quickly "become the go-to company for mining massive data sets for intelligence and law enforcement applications . . . [because it] turns messy swamps of information into intuitively visualized maps, histograms and link charts."[107] Palantir's technological capabilities have been actively utilized by the Department of Defense, the Central Intelligence Agency, the Federal Bureau of Investigation, the Army, and even financial institutions.[108] It has aided the government in "forensic analysis of roadside bombs and predicting insurgent attacks."[109] More recently, Palantir:

> [has] emerg[ed] from the shadow world of spies and special ops to take corporate America by storm. The same tools that can predict ambushes in Iraq . . . [have] saved [financial institutions like JP Morgan Chase] hundreds of millions of dollars by addressing issues from cyberfraud to distressed mortgages. A Palantir user at a bank can, in seconds, see connections between a Nigerian Internet protocol address, a proxy server somewhere within the U.S. and payments flowing out from a hijacked home equity line of credit, just as military customers piece together fingerprints on artillery shell fragments, location data, anonymous tips and social media to track down Afghani bombmakers.[110]

---

102. Kleiman, *supra* note 62, at 1190–91.
103. *Id.* at 1191.
104. *Id.*
105. *Id.* at 1191–92.
106. Mulligan, *supra* note 31, at 2362.
107. Andy Greenberg, *How A 'Deviant' Philosopher Built Palantir, A CIA-Funded Data-Mining Juggernaut*, FORBES MAG. (Aug. 14, 2013, 10:10 AM), http://www.forbes.com/sites/andygreenberg/2013/08/14/agent-of-intelligence-how-a-deviant-philosopher-built-palantir-a-cia-funded-data-mining-juggernaut/.
108. Vance & Stone, *supra* note 27.
109. Greenberg, *supra* note 107.
110. *Id.*

In 2014, after settling insider trading charges, SAC Capital Advisors (SAC), an asset management firm in search of ways to improve its compliance and surveillance systems, hired Palantir.[111] SAC hired Palantir to help the company detect improper activity, while also allowing SAC to map out and understand the varying sources of information entering the firm.[112] Palantir has also assisted JP Morgan Chase in its efforts to detect fraud.[113]

Palantir's Palantir Metropolis platform,[114] aids financial institutions in ways that can be analogized to FinCEN's efforts at aiding law enforcement agencies. Just as FinCEN's role is "strictly analytical,"[115] Palantir Metropolis is a data-mining platform used to analyze massive amounts of information, and allows for "data integration, information management and quantitative analytics. The software connects to commercial, proprietary and public data sets and discovers trends, relationships and anomalies, including predictive analytics."[116] The platform looks at various sources of data to pull "disparate information into a unified quantitative analysis environment."[117] With the data collected and evaluated by analysts, the user is able to refer to visualizations that include charts and tables that "interact seamlessly to provide a holistic view of all integrated data of interest."[118] The program allows for real-time updates of information and data, providing the user with the means to analyze massive amounts of data that require an intelligence or competitive analysis in a variety of contexts.[119]

Because reporting suspicious activity requires that financial institutions review customer transactions and identify BSA reportable behavior, Palantir can efficiently assist with the transaction monitoring that had initially been completed manually or by other software.[120] With the superior capabilities of such a high-functioning program, however, it becomes difficult to track threats to privacy. The deprivation of privacy that is a

111. Svea Herbst-Bayliss, *Cohen's SAC Taps Analytics Firm Palantir to Monitor Employees*, REUTERS (Mar. 19, 2014), www.reuters.com/article/2014/03/19/hedgefunds-sac-idUSL2N0MG22Q20140319.

112. *Id.*

113. *A (Pretty) Complete History of Palantir*, SOCIAL CALCULATIONS BLOG (Aug. 11, 2015), http://www.socialcalculations.com/2015/08/a-pretty-complete-history-of-palantir.html.

114. *Metropolis*, PALANTIR, https://www.palantir.com/palantir-metropolis/ (last visited Feb. 17, 2016) [hereinafter *Metropolis*, PALANTIR].

115. Kleiman, *supra* note 62, at 1191–92 (FinCEN's role is strictly analytical because it "first accumulates financial records of individuals and business entities from as wide a range of sources as possible" and then "compares these financial records with 'models' constructed by FinCEN analysts designed to reflect transactional patterns indicative of money-laundering and other financial crimes," to be provided to law enforcement agencies.).

116. *Palantir Metropolis*, CRUNCHBASE, www.crunchbase.com/product/palantir-finance (last visited on Nov. 3, 2015).

117. *Metropolis*, PALANTIR, *supra* note 114.

118. *Id.*

119. *The Palantir Technologies Model, Lights and Shadows on a Case of Success*, INFOSEC INST. (July 9, 2013) resources.infosecinstitute.com/the-palantir-technologies-model-lights-and-shadows-on-a-case-of-success/.

120. *See* Horn & Kelley, *supra* note 85, at 791.

concern with FinCEN,[121] is also implicated because Palantir allows its customers (e.g., the government and financial institutions) to see detailed information about its customers.[122] Part III discusses the privacy laws that the government must consider when it tries to update its AML regulations.

III. PRIVACY

A. CURRENT FINANCIAL PRIVACY PROTECTIONS

Money laundering's effects on "global financial systems" threatens national and international security.[123] Money laundering fuels illegal drug and arms dealing, corruption, and terrorism.[124] It allows criminal enterprises to thrive and grow.[125] Criminal sophistication has increased as the modern financial services industry has become globalized and more technologically advanced.[126] Additionally, the constantly evolving threat of terrorism and terrorist financing leads to increased vulnerabilities and makes it imperative that the United States adapt its systems, laws, and policies to combat any residual effects and risks posed by such criminal activity.[127] These are just a few of the justifications for requiring financial institutions to comply with AML compliance regimes.

Unfortunately, "[t]he record keeping and reporting requirements of the BSA have spawned a vast regulatory and law enforcement network with unprecedented access to . . . private financial information."[128] The road to AML compliance has not been straightforward.[129] Before 9/11, government and private groups criticized the BSA "as legislating an unjustified and unreasonable level of federal government intrusion into the private financial affairs of its citizens."[130] Many believed that the BSA was a "massive financial surveillance system" that did not balance the needs of law

121. *See* Kleiman, *supra* note 62, at 1197 (discussing the debates stemming from the increased power afforded to FinCEN for the purposes of uncover financial crimes. The government has increased FinCEN's powers "at the expense of individual privacy rights" and has "fueled the fires of debate between law enforcement and privacy advocates.").

122. Greenberg, *supra* note 107.

123. *Money Laundering and Financial Crimes*, U.S. DEP'T OF STATE, www.state.gov/j/inl/rls/nrcrpt/2000/959.htm (last visited on Feb. 20, 2016).

124. *Id.*

125. *Id.*

126. *Id.* ("Modern financial systems, in addition to facilitating legitimate commerce, permit criminals to order the transfer of millions of dollars instantly, using personal computers and satellite dishes.")

127. *2015 National Terrorist Financing Risk Assessment*, DEP'T OF THE TREASURY (June 12, 2015) https://www.treasury.gov/resource-center/terrorist-illicit-finance/Documents/National%20Terrorist%20Financing%20Risk%20Assessment%20%E2%80%93%2006-12-2015.pdf [hereinafter *NTFRA*].

128. Horn & Kelley, *supra* note 85, at 781.

129. *Id.*

130. *Id.* at 785.

enforcement with those of financial institutions and their customers.[131] After 9/11, however, it became more politically acceptable for the government to increase its AML efforts, recognizing that "world stability is increasingly threatened by sophisticated criminal organizations and their creative implementation of money laundering schemes."[132] Logically, as a result of 9/11, privacy became an afterthought because the protection of the country and its citizens against terrorists was imperative.[133]

While implementation of an AML compliance program was a commendable and rational policy, Congress understood that client privacy rights needed protection too and enacted the Privacy Act of 1974 (Privacy Act) to limit the federal government's abuse of information access.[134] The Privacy Act, however, did not go far enough—it addressed issues in privacy law, but failed to address concerns with respect to financial privacy.[135] The Privacy Act's reach is limited to federal agencies and does not cover private entities, like financial institutions, which have access to significant amounts of client information.[136] This leaves great potential for continued abuse of financial information.[137] The protection of financial information is imperative because an individual's bank account can divulge intimate details about that person's life.[138]

In response to judicial decisions that prioritized compliance with the BSA over financial privacy and determined that there could be no expectation of privacy with respect to bank records,[139] Congress passed the Right to Financial Privacy Act (Financial Privacy Act) of 1978.[140] The Financial Privacy Act limited the circumstances under which financial institutions would be able to disclose customer records to the federal government[141] (e.g., customer consent or pursuant to a subpoena).[142] Additionally, it "attempt[ed] to replicate a form of constitutional protection" by balancing a customer's privacy interests with government law enforcement interests.[143] The Financial Privacy Act regulated the flow

131. *Id.*

132. Fletcher N. Baldwin, Jr., *Money Laundering and Wire Transfers: When the New Regulations Take Effect Will They Help?*, 14 DICK. J. INT'L. L. 413, 413 (1996).

133. Pasley, *supra* note 74, at 154–55 (discussing the security changes that have resulted from 9/11).

134. Kleiman, *supra* note 62, at 1183.

135. *See id.* at 1185.

136. *See id.* at 1185–86.

137. *Id.*

138. Pasley, *supra* note 74, at 152.

139. *See* United States v. Miller, 425 U.S. 435, 443 (1976). The Supreme Court found no expectation of privacy in financial records because the information contained therein has been provided by customers in the ordinary course of business and is inherently part of commerce.

140. Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3641, 3697-710 (1978) (codified as amended at 12 U.S.C. § 3401–3422 (2012)).

141. Pasley, *supra* note 74, at 217.

142. Gouvin, *supra* note 99, at 966.

143. Kleiman, *supra* note 62, at 1187–88

of information between the government and financial institutions and it required strict procedures regulating the exchange of financial information between government agencies.[144]

The GLBA, also known as the Financial Services Modernization Act of 1999, was legislation intended to encourage competition in the financial industry by allowing for affiliation and information sharing among financial institutions.[145] The initial version of the GLBA did not consider customer privacy concerns and "became a lightening [sic] rod for consumers' fear of their increasing loss of privacy in an electronically integrated world."[146] Debates ensued.[147] The financial industry wanted fewer impediments to their information sharing.[148] Privacy proponents, on the other hand, wanted increased customer protection with an expanded definition of what constituted nonpublic personal information.[149] What resulted was the final version of the GLBA, with its Title V outlining the compromise between the two sides of the privacy debate.[150] Prior to the GLBA's enactment, federal law had failed to ensure financial privacy in any meaningful way.[151] The few preexisting federal statutes (i.e., Privacy Act and Financial Privacy Act), when considered in conjunction with common law and state law, failed to offer sufficiently broad protections for financial privacy rights.[152] The GLBA's provisions were designed to resolve this deficiency by requiring the establishment of "minimum federal safeguards for the capture, use, and sharing of financial information about customers by a wide range of businesses."[153]

Title V addresses these financial privacy concerns and Subtitle A of Title V specifically addresses financial institutions' obligations with respect to the disclosure of customers' nonpublic personal information to unaffiliated third parties.[154] Under Subtitle A, financial institutions must provide "a clear statement describing the institution's policies and practices with respect to the sharing of customer information with third parties, and

144. *Id.* at 1188–89.

145. Kathleen A. Hardee, *The Gramm-Leach-Bliley Act: Five Years After Implementation, Does the Emperor Wear Clothes?*, 39 CREIGHTON L. REV. 915, 915 (2005).

146. *Id.* at 916.

147. *Id.*

148. *Id.* ("Each lawyer of safeguards was seen as an impediment to accomplishing the initial goal of the GLBA, to facilitate the free flow of information.").

149. *Id.*

150. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 12 & 15 U.S.C.).

151. *See* David W. Roderer, *Tentative Steps Toward Financial Privacy*, 4 N.C. BANKING INST. 209 (2000) ("In most part, the concept of privacy pertaining to personal financial information has remained legally undeveloped, and seemingly beyond public consciousness or concern.").

152. *See id.* at 210 (discussing the piecemeal and inconsistent nature of existing privacy standards on both state and federal levels).

153. *Id.* at 209.

154. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, §§ 501–503, 113 Stat. 1338, 1436–1439 (1999) (codified as amended in scattered sections of 12 & 15 U.S.C.).

their procedures for protecting the security and confidentiality of customer information."[155] Financial institutions are also required to provide customers with notice regarding the information they collect and that customers may "opt out" of disclosure to unaffiliated third parties.[156] Congress outlined these obligations, but gave administrative agencies the responsibility of specifically outlining details for compliance with Title V and with monitoring such compliance.[157] Congress, however, provided these agencies little guidance as to the appropriate way to implement Title V.[158]

B. WHY THE GLBA IS ILLUSORY AND INSUFFICIENT

While Title V of the GLBA did assuage initial concerns about financial privacy, it is not without criticism. First, the GLBA states that an opt-out must be provided to customers before any nonpublic personal information is disclosed to unaffiliated third parties, and if a customer elects to keep his or her nonpublic personal information private, the financial institution must honor the request.[159] A customer's inaction or failure to affirmatively opt-out, however, provides financial institutions with implied consent to disclose the customer's nonpublic personal information to unaffiliated third parties.[160] Additionally, these opt-out requirements have exceptions.[161] Financial institutions are allowed, for example, to disclose information without customer consent when unaffiliated third parties have been recruited or have contracted to perform services on its behalf.[162] Financial institutions may also share information with unaffiliated parties without consent for "a proposed or actual sale, merger, transfer, or exchange of all or a portion of a business or operating unit" and for "required institutional risk control."[163]

---

155. Steven R. Roach & William R. Schuerman, Jr., *Privacy Year in Review: Recent Developments in the Gramm-Leach Bliley Act, Fair Credit Reporting Act, and Other Acts Affecting Financial Privacy*, 1 I/S J. L. & POL'Y INFO. SOC'Y 385, 388 (2005); *see also* Gramm-Leach-Bliley Act, §§ 501–503.

156. Roach & Schuerman, *supra* note 155, at 388; *see also* Gramm-Leach-Bliley Act, §§ 501–503; Hardee, *supra* note 145, at 919 ("The opt-out notice must be given initially when the customer relationship is created, followed by annual privacy notices in each year in which the customer relationship continues. These notices must disclose the types of nonpublic personal information the financial institution collects, as well as the types of information that the financial institution discloses to third parties. If nonpublic personal information is to be disclosed to third parties, the financial institution must then also give its customer an 'opt-out' that clearly informs the customer of his or her right to elect to keep personal information private.").

157. Hardee, *supra* note 145, at 919; Gramm-Leach-Bliley Act §§ 504–505.

158. Hardee, *supra* note 145, at 919–20.

159. *Id*. at 919; Gramm-Leach-Bliley Act § 502.

160. Jolina C. Cuaresma, *The Gramm-Leach-Bliley Act*, 17 BERKELEY TECH. L.J. 497, 504 (2002).

161. Gramm-Leach-Bliley Act § 502; *see also* Cuaresma, *supra* note 160.

162. Gramm-Leach-Bliley Act § 502(b)(2).

163. *Id*. § 502(e).

Second, as discussed above, implementation of the GLBA is left to administrative agencies, but Congress's insufficient and overly general guidance that these agencies prescribe "such regulations as may be necessary to carry out the purposes of this subtitle with respect to the financial institutions subject to their jurisdiction"[164] is problematic. Banking agencies struggled to coordinate their interagency agreement, and while they eventually adopted joint regulations, each agency also provided its own separate regulations.[165] Federal functional regulators also collaborated to develop regulations consistent with their obligations, but these regulations were developed separately.[166] And the GLBA has granted the Federal Trade Commission (FTC) the broadest authority under the GLBA, providing it with the "catch-all responsibility of implementation and enforcement"[167] for "any other financial institution or other person that is not subject to the jurisdiction of any agency or authority under . . . this subsection."[168] These agencies and federal functional regulators have broad discretion in establishing guidelines and remedies, but there is no overseeing body or enforcer. As a result, remedies for any infringements are still lacking.[169]

Third, because 9/11 has stressed the importance of increased national security, the GLBA explicitly provides another exception when invasions of financial privacy are in response to "judicial process or government regulatory authorities having jurisdiction over the financial institution for examination, compliance, or other purposes as authorized by law."[170] This exception is an important one when reviewing the AML landscape because it allows for unadulterated access to financial information in response to compliance efforts. Whether such access leads to unwarranted and unnecessary intrusions becomes an issue to consider. When federal banking agencies proposed their initial rules for KYC in 1998, complaints against the proposal flooded the office of federal regulators.[171] Eventually, the rules were withdrawn.[172] The Patriot Act brought with it "a new version" of KYC that presumably subjected every customer of a financial institution to CIP and CDD.[173] Additionally, the Patriot Act increased sanctions on financial institutions for failure to comply with the provisions.[174] As a result, "[f]or customers, the scope of the intrusion [was] disconcerting; [and] for

164. *Id.* § 504.
165. *See* Hardee, *supra* note 145, at 921–22.
166. *See id.* at 924.
167. *Id.* at 924.
168. Gramm-Leach-Bliley Act § 505.
169. *See* Roderer, *supra* note 151, at 213.
170. Gramm-Leach-Bliley Act § 502(e)(8); *see also* Teitelbaum & Kaufman, *supra* note 21, at 1155.
171. Gouvin, *supra* note 99, at 969.
172. *Id.* at 970.
173. *Id.* at 970–71.
174. *Id.* at 972.

financial institutions, the consequences of non-compliance [were] staggering."[175] Despite the potential for privacy intrusions, these actions are covered by the GLBA's exception.[176]

The creation of FinCEN, for the purpose of assisting law enforcement investigation of financial crimes[177] caused more debate between government officials and advocates of privacy rights.[178] What resulted were "several legislative and administrative attempts to confer greater powers upon the agency . . . seek[ing] to eliminate statutory restrictions on FinCEN's operations by amending the federal privacy statutes which govern administrative use of personal financial information."[179] Again, privacy rights were sacrificed for the furtherance of FinCEN's objectives.[180] FinCEN overcame any statutory or regulatory hurdles in favor of privacy rights and most recently proposed rules that add CDD as a fifth pillar to BSA compliance.[181] This further implicates issues regarding privacy intrusions. The proposed rule explicitly mandates identification and customer verification (including beneficial owners), and requires financial institutions to understand the rationale for customer relationships while simultaneously conducting ongoing monitoring.[182] This rule will advance consistent implementation of CDD efforts across financial institutions,[183] but disregards privacy. Prior to 9/11, KYC regulations were criticized for "inappropriately and unnecessarily infring[ing] on the privacy rights of bank customers."[184] Despite this criticism, regulators have enforced KYC regulations without the substantial modifications that groups such as the American Civil Liberties Union have requested.[185]

Concerns about the burdens on financial institutions[186] will not subside because these rules require additional verification and identification of beneficial owners and continued monitoring and reporting of suspicious transactions.[187] With these continued (and arguably increased) obligations on financial institutions, the need for more efficient or sophisticated technological programs that assist with the identification, monitoring, and

175. Horn & Kelley, *supra* note 85.

176. Gramm-Leach-Bliley Act, Pub. L. No. 106-102, § 502(8), 113 Stat. 1338, 1438–1439 (1999) (codified at 15 U.S.C. § 6802); *see also* Teitelbaum & Kaufman, *supra* note 21, at 1155.

177. Kleiman, *supra* note 62, at 1172.

178. *Id.*

179. *Id.* at 1173.

180. *Id.* at 1174.

181. Customer Due Diligence Requirements for Financial Institutions, 79 Fed. Reg. 45,151, 45,166 (proposed Aug. 4, 2014) (to be codified at 31 C.F.R. pts. 1010, 1020, 1023, 1024, 1026).

182. *Id.* at 45,152.

183. *Id.* at 45,153.

184. *Financial Privacy Hearing*, *supra* note 41.

185. *Id.*

186. Mulligan, *supra* note 31, at 2338.

187. Customer Due Diligence Requirements for Financial Institutions, 79 Fed. Reg. 45,151, 45,152.

reporting requirements will only become more obvious. This will result in the continued reliance on programs like Palantir Metropolis and similar platforms, which have the ability to access vast amounts of information instantly across national and international borders.

As a result, the sophistication of technology will continue to affect privacy protection.[188] This leads to the last problem to address: money laundering and terrorist financing are global in nature, which makes it necessary for the United States to work with the rest of the world to ensure that its efforts are in concert with international efforts.[189] This is not limited to rules and regulations related to illegal financial activities. The United States is behind in its efforts to protect its citizens' right to privacy, as its privacy regime is far less protective in comparison to international privacy laws.[190]

International financial crimes involve a level of complexity that requires a joint effort by all nations to gather and analyze data from various sources, both domestically and abroad.[191] Financial institutions will need software like Palantir's to aid in its compliance efforts, which proves problematic and terrifying precisely because it is a program that works so well and provides its clients with access to a wide range of information.[192] The program's ability to assist its clients in their surveillance efforts and to assist in mining massive amounts of data has become a great concern to privacy advocates, resulting in the prospect of a "true totalitarian nightmare, monitoring the activities of innocent Americans on a mass scale."[193] In response to concerns about the increased risk to privacy created by using programs like those developed by Palantir, Palantir has itself assembled the Palantir Council of Advisors on Privacy and Civil Liberties, a group of experts working together to address privacy issues arising with the platform's continued use and development.[194] Palantir, acknowledging the importance of privacy and civil liberties, has made the protection of these

188. Kleiman, *supra* note 62, at 1171–72 ("Increasing hardware capacities, growing software sophistication, and innovative application of existing technologies have undermined attempts to create a stable framework of privacy protection.").

189. Roach, *supra* note 155, at 435 ("The challenges facing the United States in preventing illegal financing are enormously complex and encompass numerous organizations throughout the world. Current U.S. statutes appear sufficient to regulate and monitor formal financial institutions in U.S. and Western Europe, but struggle to maintain the same control over the informal networks found elsewhere in the world.").

190. *See* Kyle T. Sammin, *Any Port in a Storm: The Safe Harbor, The Gramm-Leach-Bliley Act, and the Problem of Privacy in Financial Services*, 36 GEO. WASH. INT'L L. REV. 653, 653 (2004).

191. Roach, *supra* note 155, at 435.

192. Greenberg, *supra* note 107.

193. *Id.*

194. John Grant, *Going International With the Palantir Council of Advisors on Privacy and Civil Liberties*, PALANTIR (Jan. 29, 2014), https://www.palantir.com/2014/01/going-international-with-the-palantir-council-of-advisors-on-privacy-and-civil-liberties/.

rights a core commitment.[195] Unfortunately, Palantir's efforts alone are insufficient to protect privacy—the government must also act.

Technology will continue to advance and more programs will be developed to assist with data collection and monitoring on a global scale. It is therefore important and necessary to consider how international privacy laws are implicated. The European Union (EU) and the United States have long had fundamentally different views on privacy, with the EU placing greater value on an individual's human right to privacy. The EU's Data Privacy Directive requires companies operating in the EU or using the data of the EU's citizens to comply with its privacy regulations as standardized by the data privacy laws of its Member States.[196]

The EU and the United States established a Safe Harbor Agreement (Safe Harbor) that permits continued trade between the two, while allowing for compromise with respect to the EU Data Privacy Directive's requirements.[197] The Safe Harbor did not require modification to U.S. privacy laws, but instead, required that U.S. companies self-certify their self-enforcement of data protection schemes that would provide privacy protections equivalent to those that the EU Data Privacy Directive provides.[198] This Safe Harbor applied only to those companies under the jurisdiction of the FTC and the Department of Transportation, and excluded the financial services industry.[199] Despite this exclusion, the EU declared that the GLBA was insufficient when compared to the requirements established under the Safe Harbor.[200]

Even more problematic than the EU's unwillingness to view the GLBA as sufficient financial privacy protection[201] was the European Court of Justice's recent invalidation of the 15-year-old Safe Harbor.[202] The EU's disapproval of U.S. privacy protections and the resulting invalidation of the only legal mechanism in place to protect extraterritorial data transfers makes it even more imperative that privacy regulations, including the GLBA, be reconsidered and modified.

---

195. PALANTIR TECHS., A CORE COMMITMENT PROTECTING PRIVACY AND CIVIL LIBERTIES (2012), https://www.palantir.com/wp-assets/wp-content/uploads/2012/06/ProtectingPrivacy_CivilLiberties_2012.pdf.

196. *See* Sammin, *supra* note 190, at 653.

197. *Id.*

198. *Id.* at 657–58.

199. *Id.* at 654–58.

200. *Id.*

201. *Id.*

202. Court of Justice of the European Union, Press Release No 117/15, The Court of Justice Declares That the Commission's US Safe Harbour Decision Is Invalid (Oct. 6, 2015), http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf.

C. RECOMMENDED SOLUTION FOR THE PRIVACY PROBLEM

KYC regulations and FinCEN's proposed rules continuously require financial institutions to gather information about their customers, to create risk profiles, and determine trends in their behavior.[203] Regulations also necessitate the monitoring of transactions so that financial institutions may report suspicious activity.[204] FinCEN's recent rules were proposed with no mention of customer privacy rights, indicating that these enforcement efforts will likely continue on course, to the detriment of customers. FinCEN's justifications are rational: it seeks to promote consistent efforts at implementation within financial sectors; it seeks to aid law enforcement and regulators in obtaining information necessary for their examinations and investigations; it hopes to help financial institutions "assess and mitigate risk" as they work to comply with AML requirements; and it ultimately seeks to aid in the identification of accounts linked to illicit crimes and national security threats.[205] Unfortunately, though the goals of these rules are commendable, the rules themselves are not complete.

Customer privacy rights have consistently taken a backseat to the goals of AML compliance and economic efficiency.[206] While the GLBA was a step in the direction of reconsidering financial privacy, the need for information continues to trump privacy considerations,[207] especially after considering all of the GLBA's shortcomings.[208] "[T]he momentum for increased privacy rights [came] to a halt in light of the . . . concern over national security."[209] FinCEN's proposed rules continue to further the message that privacy will not be a primary consideration for financial institutions, if a consideration at all. To work toward resolving the lack of attention to privacy rights, regulators should modify the AML framework to specifically address financial privacy.

Currently, the first four pillars are concerned with compliance efforts and in ensuring that financial institutions are complying with regulations.[210] The fifth pillar, as proposed by FinCEN, further solidifies compliance requirements.[211] Unfortunately, these five pillars, when taken in totality, still fail to address and resolve the negative effects that these compliance procedures will have against the financial privacy rights of customers; they fall short because they fail to address or provide privacy protections.

---

203. *See* Horn, *supra* note 85, at 787.

204. *Id*. at 791.

205. Customer Due Diligence Requirements for Financial Institutions, 79 Fed. Reg. 45,151, 45,153 (proposed Aug. 4, 2014) (to be codified at 31 C.F.R. pts. 1010, 1020, 1023, 1024, 1026).

206. *See* Cuaresma, *supra* note 160, at 510.

207. *Id*. at 515.

208. *See supra* Part III.B.

209. Cuaresma, *supra note* 160, at 517.

210. *See* Customer Due Diligence Requirements for Financial Institutions, 79 Fed. Reg. at 45,166.

211. *See id*.

This being the case, a sixth pillar of AML privacy compliance can be added to work hand-in-hand with the other five. This sixth pillar should be mirrored after the FTC's GLBA regulations, and more specifically, its Standards for Safeguarding Customer Information (Safeguards Rule).[212] The FTC's Safeguards Rule requires that financial institutions develop and describe to customers its program for protecting customer information.[213] FinCEN should mirror the elements of the Safeguards Rule to establish privacy safeguards and procedures that are cognizant of the compliance requirements of the AML framework, while simultaneously ensuring that the access to and reporting of this information is not done in a way that overreaches and neglects privacy rights.

The proposed sixth pillar would require that Chief Compliance Officer's within financial institutions appoint, and work hand-in-hand with, either a Chief Privacy and Information Officer or employees specifically designated to focus on privacy and security issues. These privacy employees will be responsible for monitoring compliance programs for risks and inadequacies and for implementing measures to ensure their conformity with current privacy regulations, at both the domestic and international levels. In light of the enhanced due diligence requirement with respect to foreign clients,[214] it is imperative that privacy employees within these institutions are also specialists in the privacy laws of other nations to guarantee compliance with regulations beyond those of the AML regime of the United States.

Additionally, these privacy employees should assist in transparency efforts for the sake of increasing customer awareness, and they should be responsible for ensuring that the scope of compliance programs does not reach beyond what is necessitated by law—that the information gathered is not used for purposes outside the scope of compliance with AML regulations. This will require that privacy groups also review the processes and procedures employed by their service providers to ensure that all service providers implement and maintain consistent safeguards. Privacy teams must work with compliance groups to ensure that the efforts are handled seamlessly. Beyond their work within the financial institutions, privacy officers should be required to annually certify the propriety of their privacy program—a designated body should also be created to review these certifications.

Until the federal government prioritizes financial privacy by requiring that government agencies and officials work closely with private sector individuals and international regimes to ensure uniform and sound privacy programs, starting with financial institutions directly seems like a necessary

212. Standards for Safeguarding Customer Information, 16 C.F.R. § 314 (2002).
213. *Id.*
214. Sorcher, *supra* note 98, at 402.

and proactive start. While the financial costs associated with hiring these officers and employees may be burdensome, it will be a positive step in ensuring that privacy, and even security, is addressed in anticipation of the constantly evolving privacy landscape.

CONCLUSION

Terrorism, money laundering, and illicit crimes have not subsided and have instead invaded global markets.[215] The inherently global nature of these illicit activities has necessitated the implementation of a robust AML compliance regime within financial institutions.[216] The policies and rationale are logical—it is important to ensure that financial institutions are protected against and not aiding in the abuses of terrorist organizations and money launderers.[217]

However, with compliance comes the potential risk that financial institutions seeking to avoid any penalties associated with failed compliance will gather information beyond the scope of what is necessitated by law. This risk can be further exacerbated by the capabilities of the technology that is aiding these financial institutions in their compliance efforts.[218] What results is an inadequate regulatory framework that addresses AML compliance and privacy protection separately, rather than concurrently. Because information, and more specifically, financial data, is intrinsically extraterritorial, the two regimes can no longer work independently. AML regulation is undoubtedly necessary and important, but privacy rights are also important. Financial privacy need not be sacrificed for the sake of compliance with regulations. Palantir has taken steps to commit itself to privacy and civil liberties efforts and the U.S. government should do the same.[219] Regulators should similarly work with privacy advocates in resolving these tensions.

Unfortunately, in light of the continuous debate over privacy and financial privacy, a sound resolution for the United States does not seem imminent. Until multinational reconciliation of these two regulatory frameworks—AML regulation and privacy regulation—can be accomplished, FinCEN should take steps to enhance and improve its AML framework by accounting for customer privacy rights. A sixth pillar should be added to FinCEN's proposed rules; one that will require that financial institutions employ privacy specialists who will be responsible for auditing internal and external programs, as well as developing safeguards to minimize risks, and who will be constantly vigilant of AML, privacy issues,

---

215. *See generally* Money Laundering and Financial Crimes, *supra* note 123.

216. *See id.*; *see also* NTFRA, *supra* note 127.

217. *See* Money Laundering and Financial Crimes, *supra* note 123; *see also* NTFRA, *supra* note 127.

218. *See supra* Part II.B.

219. *See generally* Grant, *supra* note 194.

and laws domestically and abroad to ensure that regulatory compliance satisfies the transnational nature of both.

Maria A. de Dios[*]

* B.A., Bryn Mawr College, 2007; J.D. Candidate, Brooklyn Law School, 2016. Thank you to the Executive Board and Staff of the *Brooklyn Journal of Corporate, Financial & Commercial Law* for all of their hard work in preparing this Note for publication. A special thank you to Dean Nicholas Allard, Professor Jonathan Askin, Professor James Fanto, and Steven Ballew for their guidance and encouragement as I explored the ideas behind this Note. Lastly, thank you to my family and friends for their unwavering love and support and for being my strength and inspiration throughout this journey.