COMMENTS

of

THE WASHINGTON LEGAL FOUNDATION

to the

FINANCIAL CRIMES ENFORCEMENT NETWORK

and the

U.S. DEPARTMENT OF THE TREASURY

Concerning

CUSTOMER DUE DILIGENCE REQUIREMENTS FOR FINANCIAL INSTITUTIONS (Docket ID No. 2014-18036)

Cory L. Andrews
Mark S. Chenoweth
WASHINGTON LEGAL FOUNDATION
2009 Massachusetts Ave., N.W.
Washington, D.C. 20036
(202) 588-0302

October 3, 2014

WASHINGTON LEGAL FOUNDATION
2009 Massachusetts Avenue, NW
Washington, DC 20036
(202) 588-0302

October 3, 2014

Policy Division
Financial Crimes Enforcement Network
Docket ID No. 2014-18036
P.O. Box 39
Vienna, VA 22183

Re: RIN 1506-AB25; Comments Concerning Proposed Amendments to the Bank Secrecy Act Regulations—Customer Due Diligence Requirements for Financial Institutions

Dear Sir/Madam:

Pursuant to the public notice published at 79 Fed. Reg. 45151 (August 4, 2014), the Washington Legal Foundation (WLF) appreciates this opportunity to offer comments to the Financial Crimes Enforcement Network (FinCEN) in response to the agency's notice of proposed rulemaking regarding customer due diligence requirements for financial institutions subject to an existing customer identification program (CIP) requirement.[1]

I. Interests of WLF

Founded in 1977, the Washington Legal Foundation is a public-interest law firm and policy center based in Washington, D.C. with supporters throughout the United States. WLF devotes a substantial portion of its resources to defending and promoting free enterprise, individual and business civil liberties, a limited and accountable government, and the rule of law. To that end, WLF regularly engages in original and *amicus* litigation in a wide variety of federal regulatory matters. For example, WLF routinely participates in litigation to ensure that federal agencies are not permitted to exercise powers that Congress cannot plausibly be understood to have granted them. *See, e.g., Util. Air Regulatory Group v. EPA*, 134 S. Ct. 2427 (2014); *FDA v. Brown &*

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

Williamson Tobacco Corp., 529 U.S. 120 (2000); *Am. Farm Bureau Fed'n v. EPA*, No. 13-4079 (3d. Cir. dec. pending). In addition, WLF routinely litigates in regulatory cases to ensure that undue deference is not accorded to federal regulatory agencies. *See, e.g.*, *Christopher v. SmithKline Beecham Corp.*, 132 S. Ct. 2156 (2012); *Alexander v. Sandoval*, 532 U.S. 275 (2001); *Pharm. Research & Mfrs. of Am. v. Thompson*, 362 F.3d 817 (D.C. Cir. 2004).

In addition, WLF's Legal Studies Division, the publishing arm of WLF, frequently produces and distributes articles on a wide array of legal issues related to data privacy. *See, e.g.*, Robert M. McKenna and Scott Lindlaw, *Targeting Harm From a Breach: Plaintiffs' Lawyers Get Creative in Data Privacy Suits*, WLF LEGAL BACKGROUNDER, February 7, 2014; Raymond T. Nimmer, *Privacy & Personal Data Security: The Next Litigation Frontier?*, WLF LEGAL OPINION LETTER, JANUARY 16, 2009.

WLF is concerned that FinCEN's proposal, by requiring financial institutions to obtain the social security number and date of birth for each beneficial owner of a legal entity, would unnecessarily increase the regulatory burden and cost on the financial industry. Because financial institutions are unable to verify the accuracy of the data they collect, the rule will is likely to have no effect on bad actors but will disproportionately intrude on the privacy of honest business people, placing them at increased risk of identity theft if their information should be compromised. The proposed rule would also force financial institutions to collect and safeguard information that would expose them to greater liability under federal law if their secured networks are breached

II. The Proposed Rule

The proposed rule would apply to all banks, brokers or dealers in securities, mutual funds, and futures commission merchants and introducing brokers in commodities. The rule identifies four key, minimum elements of a financial institution's customer due diligence: (1) identifying and verifying the identity of customers; (2) identifying and verifying the identity of individuals who are "beneficial owners" of legal entity customers; (3) understanding the nature and purpose of customer relationships; and (4) conducting ongoing monitoring to maintain and update customer information and to identify and report suspicious transactions. FinCEN asserts that item (1) is already satisfied by existing CIP requirements, and that items (3) and (4) are intended to be consistent with and clarify financial institutions' current suspicious activity reporting and anti-money laundering obligations. Item (2), however, regarding the individual beneficial owners of "legal entity customers," is acknowledged as a new requirement.

Under the proposal, the "beneficial owner" of a legal entity is defined as any natural person who owns, directly or indirectly, 25 percent or more of a legal entity, as well as anyone who controls, manages, or directs the legal entity (such as a CEO, COO, CFO or General Partner). Using a standardized form that is part of the proposed rulemaking, FinCEN would require covered financial institutions to collect the name, date of birth, address, and social security number (or passport number/similar identification for foreign persons) of each beneficial owner whenever a new account is opened for a legal entity.[2]

III. WLF's Concerns

The collection of highly sensitive information, especially date of birth and social security number, for each beneficial owner of a legal entity goes well beyond any existing risk-based approaches that most financial institutions use. Currently, most financial institutions collect the names of beneficial owners, but do not as a matter of course collect and store their date of birth and social security number. Collecting the date of birth and social security number for each beneficial owner—even those of entities displaying no risk factors for money laundering or criminal activity—is of very little benefit to the government since financial institutions are not obliged under the proposed rule to verify the accuracy of the data they collect (nor could they). Bad actors know they can provide false information and will not hesitate to do so. For honest business people, however, this data collection intrudes on their privacy and places them at increased risk of identity theft if their information should be compromised.

Indeed, requiring the individual owners of small and closely-held companies to provide their date of birth and social security number increases the risk that they will become victims of identity theft. This concern is particularly acute for owners of small and closely-held companies who are targets of great interest to identity thieves, because their names are often tied to not only their personal accounts but also the accounts of their companies. Requiring banks and brokers to obtain and store the date of birth and social security number of a small business owner any time his or her company opens an account thus increases the risk that identity thieves will obtain the personal information of these individuals while providing no offsetting benefit to financial institutions or government.

This concern that identity thieves might more easily obtain and use the personal information financial institutions would collect (and share with the government) on each

[2] *See* Appendix A to the proposed rule.

beneficial owner under FinCEN's proposed rule could be obtained and used by identity thieves is fully justified by recent events. Indeed, given the Federal Trade Commission's aggressive policy of prosecuting, under Section 5 of the FTC Act, legitimate businesses who are themselves victimized by data security breaches, *see, e.g. FTC v. Wyndham Worldwide Corp.*, No. 13-cv-1887 (D. N.J. 2013), the proposed rule would force financial institutions to engage in conduct that would expose them to even greater liability under federal law if their secured networks are ever breached. Recent reports of a coordinated attack against JPMorgan Chase & Co., and at least four other banks, by Russian hackers in late August is the latest in a steady string of cyberattacks compromising the personal and financial information of U.S. businesses and individuals. The attacks began in June 2014, when hackers used a flaw in one of JPMorgan's public websites to dig into its computer network to access client and employee information, and went uninterrupted until mid-August.[3] Although the investigation is ongoing and many details of the attack remain unknown, published reports indicate that once inside the system hackers used malicious software to steal gigabytes of information, including customer account data.[4] What makes the attack all the more troubling is that JPMorgan maintains one of the most sophisticated cyber-security systems on Wall Street, with more than 1,000 employees and $250 million dedicated to the effort.[5]

Several other recent data breaches have compromised individuals' personal information from the computer systems of government agencies,[6] financial institutions,[7]

---

[3] *See* Jordan Robertson and Michael Riley, *JPMorgan Hack Said to Span Months Via Multiple Flaws*, BLOOMBERG, August 29, 2014.

[4] *Id.*

[5] *Id.*

[6] According to the United States Government Accountability Office (GAO), "[t]he number of reported information security incidents involving personally identifiable information has more than doubled over the last several years" climbing from 10,481 in 2009 to 25,566 in 2013. *See* Statement of Gregory C. Wilshusen, Director of Information Security, United States Government Accountability Office: Testimony Before the Committee on Homeland Security and Governmental Affairs, U.S. Senate April 2, 2014 at http://www.gao.gov/assets/670/662227.pdf.

These security breaches have included some staggering incidents such as the Department of Veterans Affairs report that computer equipment containing personally identifiable information "on about 26.5 million veterans and active duty members of the military was stolen from the home of a VA employee." *Id.* The Federal Retirement Thrift Investment Board reported in 2012 that the social security numbers and other personally

and a litany of large companies.[8] Given the identity theft risks inherent in such practices, FinCEN's proposal appears strikingly inconsistent with the trend to move away from the use and collection of social security numbers for personal identification.[9]

This requirement disproportionately affects small and closely-held business owners because the proposed rule excludes publicly-traded companies from divulging even the names of their beneficial owners. FinCEN's proposal does not contemplate a process by which the beneficial owners of small and closely-held companies can protect their most sensitive identity information. Nor does FinCEN consider less intrusive forms of identification—such as a driver's license number—that pose less risk of identity theft. Although FinCEN explains the value of having financial institutions collect uniform data on beneficial owners, it never explains the imperative for categorically requiring the

---

identifiable information of plan participants were accessed by hackers through "a sophisticated cyber-attack on the computer of a contractor that provided services to the Thrift Savings Plan." Another recent GAO study cited the Consumer Financial Protection Bureau (CFPB) for collecting financial data on up to 600 million consumer credit card accounts without sufficient security or privacy protections in place. *See* United States Government Accountability Office Report, *Consumer Financial Protection Bureau: Some Privacy Security Procedures for Data Collections Should Continue Being Enhanced*, September 2014, at http://www.gao.gov/assets/670/666000.pdf.

[7] According to the Identity Theft Resource Center, based on media reports, from 2005-2013 a total of 786,789 personal identity records held by financial institutions were compromised due to hacking, insider theft, employee or subcontractor negligence, and other causes.

[8] There have been several much-publicized incidents of data breaches at large companies, including the data breach last holiday season at Target that compromised nearly 40 million credit and debit card records. *See* Anne D'Innocenzio, *Target Data Breach Cost Banks More than $200 Million*, HUFFINGTON POST, February 18, 2014. But that breach paled in comparison to the 56 million credit and debit cards that were compromised during a five-month-long attack on Home Depot's payment terminals. *See* Robin Sidel, *Home Depot's 56 Million Card Breach Bigger Than Target's*, THE WALL STREET JOURNAL, September 18, 2014.

[9] For example, the Intelligence Reform and Terrorism Prevention Act of 2004 amended the Social Security Act to expressly prohibit States or their political subdivisions from displaying, electronically or otherwise "a social security account number (or any derivative of such number) on any driver's license motor vehicle registration, or personal identification" issued by States to an individual for identification. Section 7214, PUBLIC LAW 108–458—108th CONG. (Dec. 17, 2004).

collection of the date of birth and social security number of a business owner, including those who may already be known to a financial institution.

Nor does the proposed rule offer a rationale for singling out small and closely-held companies. If there are criteria that make such entities greater risks, the rule does not elaborate on those criteria. If publicly traded companies, including those for which one individual owns more than 25, need not report this information, there can be no justification for demanding such information from small and closely-held companies across the board. Indeed, where a new institutional customer is personally well-known to the bank, this information is wholly superfluous. Likewise, where an account is utterly devoid of suspicious activity, the collection of this data serves no purpose.

IV. Conclusion

Given the low incremental utility to financial institutions and the government of collecting sensitive, personal data on beneficial owners of small and closely held companies, FinCEN should jettison the required collection of the birth dates and social security numbers and propose less intrusive and lower-risk means of identification for beneficial owners. It should also reconsider whether such information needs to be collected at all.

Respectfully submitted,

/s/ Cory L. Andrews
Cory L. Andrews
Senior Litigation Counsel

/s/ Mark S. Chenoweth
Mark S. Chenoweth
General Counsel