



December 22, 2010

James H. Freis, Director
Financial Crimes Enforcement Network
Department of the Treasury
P.O. Box 39
Vienna, Virginia 22183

Attention: Cross-Border Transmittal of Funds

Dear Director Reis,

The Electronic Frontier Foundation (“EFF”) respectfully submits these comments in response to the notice of proposed rulemaking published by the Financial Crimes Enforcement Network (“FinCEN”) on September 27, 2010. EFF is a non-profit, public interest organization dedicated to defending and advocating for free speech, privacy, innovation, government transparency, and consumer rights in the digital world.

I. Introduction

On September 27, 2010, the Department of Treasury’s Financial Crimes Enforcement Network (FinCEN) published a notice of proposed rulemaking setting forth new reporting requirements for cross-border electronic transmittal of funds (“CBETFs”).¹ Promulgated in conjunction with FinCEN’s ongoing efforts to combat money laundering and terrorist financing, the new requirements would substantially expand financial institutions’ obligations to report financial transactions to FinCEN; this substantial expansion, in turn, may compromise the privacy rights of law-abiding American citizens and foreign nationals living in the United States. Under the proposed rules, FinCEN would require disclosure of a donation to the International

¹ Cross-Border Electronic Transmittal of Funds, 75 Fed. Reg. 60377 (proposed September 27, 2010).

Red Cross and a remittance sent to family members living overseas. The Constitution, however, generally guards this type of information from compelled government disclosure.²

While money laundering and terrorist financing are legitimate problems, our government's response to these crimes must be measured: new law enforcement techniques must be implemented with caution and must be balanced with the legitimate privacy interests of Americans in their finances, associations, and family relationships. Based on our analysis of these proposed regulations and on records we received from FinCEN in response to a recent FOIA request, we believe these regulations tip the balance too far against the privacy rights of American citizens.

EFF objects to the proposed regulations on two grounds. First, FinCEN has not shown the proposed reporting requirements are reasonably necessary to prevent money laundering and terrorist financing. The rules, as a whole, may be ineffective in preventing terrorist financing, and, at minimum, are unnecessarily overbroad. Second, it appears that FinCEN has not adequately assessed the proposed regulations' threat to citizens' privacy. While FinCEN affirmatively sought the perspectives of law enforcement agencies and the financial industry, the opinions of privacy advocates were not solicited when developing the proposed rule. Moreover, FinCEN has not shown that sufficient technical or security analyses have been performed on the electronic transfer and storage requirements for such vast quantities of sensitive information.

In light of these objections, EFF respectfully urges FinCEN to reconsider the proposed regulations and their necessity in the agency's ongoing efforts to combat financial crime.

² See, e.g., *NAACP v. Alabama*, 357 U.S. 449 (1958) (holding the First Amendment requires a compelling interest for state government to mandate disclosure of rank and file membership lists of NAACP).

II. Current Regulations, Proposed Regulations, and EFF's FOIA Request

Current Regulations

FinCEN currently requires banks and nonbank financial institutions to collect and retain information on certain foreign and domestic funds transfers and transmittals of funds (the "Funds Transfer Rule"), as well as to include certain information on funds transfers and transfers of funds between banks and nonbank financial institutions (the "Travel Rule").³

Under the Funds Transfer Rule, for any transfer of \$3,000 or more, banks and nonbank financial institutions must retain, and make available upon request by federal law enforcement agencies, the name, address and account number of both the sender and recipient, the amount of the transfer, any instructions accompanying the transfer, among other relevant information. Under the Travel Rule, similar information to that retained under the Funds Transfer Rule must be included in any transfer of funds when "a financial institution act[s] as the [sender's] financial institution" when processing a funds-transfer.⁴

In conjunction with the two rules specifically governing funds transfers, the Bank Secrecy Act requires financial institutions to report to FinCEN cash transactions exceeding \$10,000 and to file suspicious activity reports ("SARs") with FinCEN when a financial institution suspects activity indicative of a financial crime.⁵

Proposed Regulations

The proposed rules substantially expand the obligation of financial institutions to report financial transactions and citizens' sensitive financial information to the government. Under the

³ 31 CFR 103.33(e) (2009) ("Funds Transfer Rule" for banks); 31 CFR 103.33(f) (2009) ("Funds Transfer Rule" for nonbank financial institutions); 31 CFR 103.33(g) (2009) ("Travel Rule").

⁴ Cross-Border Electronic Transmittal of Funds, 75 Fed. Reg. 60377, 60378 (proposed September 27, 2010).

⁵ Bank Secrecy Act, 51 U.S.C. §§ 5311-5314e; 31 C.F.R. § 103.22 (Currency transaction reports); 31 C.F.R. § 103.18 (Suspicious activity reports).

proposed rules, financial institutions would be required to report *all* cross-border electronic funds transfers (“CBEFTs”) to FinCEN, while money transmitters will be required to report all transfers at or above a \$1,000 threshold.⁶ Each CBETF report would contain similar information to that required under the Funds Transfer Rule and the Travel Rule.⁷ The reporting requirements for money transmitters would additionally require the disclosure of the sender’s U.S. taxpayer identification number, alien identification number, or passport number and country of issuance.⁸

A second, but related, proposed rule would require banks to annually submit to FinCEN all account numbers — along with the accountholder’s U.S. tax identification number — used to originate or receive CBETFs.⁹

EFF’s FOIA Request

Following the publication of FinCEN’s notice of the proposed rulemaking, EFF submitted to the agency a request under the Freedom of Information Act (“FOIA”) on September 29, 2010 for the following categories of information:

1. Communications or meetings between any employees or officials within FinCEN concerning the development and drafting of the proposed rule, to the extent that the records reflect the agency’s rationale for the proposed rule as published;
2. Communications or meetings between employees or officials of FinCEN and officials or employees of other government agencies concerning the development or drafting of the proposed rule, to the extent that the records reflect the agency’s rationale for the proposed rule as published;
3. Communications or meetings between employees or officials of FinCEN and any representative, official, or employee of financial-services companies, financial-services groups or organizations, or financial-services consortiums (including, but not limited to the Society for Worldwide Interbank Financial Telecommunication) concerning the development or drafting of the proposed rule;

⁶ Cross-Border Electronic Transmittal of Funds, 75 Fed. Reg. 60377, 60384 (proposed September 27, 2010).

⁷ *Id.* at 60385.

⁸ *Id.*

⁹ *Id.* at 60387.

4. Communications or meetings between employees or officials of FinCEN and any data security or technical analysts or experts concerning the data and security requirements of the proposed rule;
5. Communications or meetings between employees or officials of FinCEN and representatives of foreign governments concerning the proposed rule;
6. Factual material supporting the assertion in the proposed rule that the agency has experienced “[an] inability to conduct proactive analysis on the information currently recorded by banks [which] hinders law enforcement’s ability to identify significant relationships to active targets;” and
7. Any evaluation of the adequacy (or inadequacy) of provisions contained in the Patriot Act granting the government the authority to obtain any wire transfer data from banks concerning individuals who are suspected of money laundering or terrorist activity.

FinCEN released nearly one thousand pages of documents in response to our FOIA request.¹⁰ Our analysis of these documents — in conjunction with the implications created from the absence of some categories of information altogether — form the basis for the perspectives expressed in this comment.

III. Concerns with the Proposed Rules

As described above, EFF recognizes that money laundering and terrorism financing are, indeed, legitimate problems, necessitating well-tailored solutions that strike an appropriate balance between protecting the privacy of law-abiding citizens and the law enforcement need for such private, sensitive information. The proposed rules, however, go too far. For the reasons further explained below, EFF urges FinCEN to reconsider the proposed regulations.

¹⁰ The vast majority of documents released, however, were already publicly available. EFF filed an appeal challenging FinCEN’s limited response on November 30, 2010.

FinCEN Has Not Adequately Demonstrated the Proposed Rules are “Reasonably Necessary”

The Intelligence Reform and Terrorism Prevention Act of 2004 (“IRTPA”)¹¹ directs the Secretary of the Treasury to promulgate regulations governing reporting of CBEFTs that the “Secretary determines . . . [are] reasonably necessary to conduct the efforts of the Secretary against money laundering and terrorist financing.”¹² Even under this ample standard, the sweeping breadth of the proposed regulations cannot be said to be “reasonably necessary.” The proposed reporting regime likely would not have helped prevent the attacks of 9/11 or other terrorist incidents, and FinCEN’s own assessment of law enforcement need demonstrates that the proposed threshold for reporting is unnecessary. For these reasons, the proposed rules are not “reasonably necessary” to further the agency’s mission of combating financial crime.

First, there is no indication that FinCEN’s proposed regulations will actually deter or prevent terrorist financing. Congress passed the IRTPA in response to the 9/11 Commission’s findings that, leading up to the 9/11 attacks, various breakdowns occurred in the gathering and sharing of intelligence information.¹³ Specifically, with regard to funding of the attacks on 9/11, the Commission found that \$400,000–\$500,000 was used to finance the attacks. The attackers obtained their funds in a variety of ways, including “deposits of cash or travelers checks” and by accessing foreign bank accounts “through ATM and credit card transactions.”¹⁴ The Commission specifically noted that the attackers relied on nearly \$50,000 in traveler’s checks and cash and

¹¹ Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 368 (codified as amended in scattered sections).

¹² 31 U.S.C. § 5318(n)(1).

¹³ See generally, National Commission on Terrorist Attacks upon the United States, *The Final Report of the National Commission on Terrorist Attacks upon the United States* (9/11 Commission Report) (July 22, 2004), available at <http://govinfo.library.unt.edu/911/report/911Report.pdf>.

¹⁴ National Commission on Terrorist Attacks upon the United States, *Terrorist Financing Staff Monograph*, 3 (2004).

approximately \$30,000 in ATM withdrawals from foreign banks.¹⁵ FinCEN's proposed changes to financial institutions' reporting requirements would not have detected these funds transfers. There is no evidence that FinCEN's proposed regulations would have any effect on subsequent terrorist financing within the United States: terrorists could readily circumvent the proposed rules using financing methods already in use before the 9/11 attacks.

Setting aside the efficacy of the proposed regulations as a whole, FinCEN has not shown that the threshold for reporting, as currently proposed, is "reasonably necessary" to further the agency's efforts in combating money laundering or terrorism financing.

With regards to the attacks on 9/11, of the nearly \$130,000 transferred via twelve CBETFs, only three were below the current \$3,000 record-keeping requirement.¹⁷ Of those twelve CBETFs, however, most were significantly above the current reporting requirements, including transfers of \$10,000, \$20,000, and \$70,000¹⁸ — all transactions that should have triggered scrutiny under current Bank Secrecy Act reporting requirements. If this evidence suggests any conclusions, it is that either, first, current reporting requirements were sufficient, but insufficiently implemented by financial institutions; or, second, that law enforcement was not adequately equipped to assess the data already available. This evidence does not necessarily suggest, however, that law enforcement could benefit from obtaining information on *all* CBETFs. To the contrary, it might suggest that receiving 750 million new CBETF reports annually would only further compound law enforcement's struggle to adequately utilize and analyze the data already available by statute.¹⁹

¹⁵ *Id.* at 135 - 38.

¹⁷ National Commission on Terrorist Attacks upon the United States, *Terrorist Financing Staff Monograph*, 134-5 (2004).

¹⁸ *Id.*

¹⁹ *See* Cross-Border Electronic Transmittal of Funds, 75 Fed. Reg. 60377, 60388 (proposed September 27, 2010).

FinCEN’s own survey of law enforcement agencies determined that “[t]he basic information already obtained and maintained by U.S. financial institutions pursuant to the Funds Transfer Rule, including the \$3,000 recordkeeping threshold, provides sufficient basis for meaningful data analysis.”²⁰ Nevertheless, FinCEN opted to mandate reporting for *all* CBEFTs performed by financial institutions, even in the absence of a demonstrated law enforcement need for the information. At minimum, the reporting threshold for financial institutions in the proposed regulations cannot be justified as “reasonably necessary” to deter money laundering or terrorism financing.

Given the questionable efficacy of the proposed regulations in their entirety and the demonstrable overbreadth of the proposed reporting threshold, EFF respectfully requests FinCEN to carefully reconsider the necessity of the proposed rules.

FinCEN Has Not Adequately Assessed the Privacy Implications of the Proposed Rule

The proposed regulations will require greatly increased disclosure of the sensitive financial information of law-abiding American citizens to FinCEN and other government agencies. Most law-abiding Americans do not want their name, address, and bank account information disclosed to any third-party, let alone government law enforcement officials.²² Thus, government agencies should proceed with caution when crafting regulations mandating the disclosure of this sensitive information. Based upon analysis of the documents FinCEN provided to EFF, it does not appear that FinCEN has adequately assessed the privacy implications of the proposed regulations: First, while FinCEN actively solicited the opinions of various “stakeholders” — financial institutions, law enforcement officials, and even agencies of foreign

²⁰ *Id.* at 60380.

²² See Christopher Slobogin & Joseph Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at “Understandings Recognized and Permitted by Society,”* 42 DUKE L.J. 727 (1993) (noting, according to survey results, that “the scenario involving government perusal of bank records received a high ranking” in terms of its intrusiveness).

governments — when drafting the proposed regulations, the perspective of privacy experts and advocates was not sought. And, second, because FinCEN has not completed the data security certification for the proposed rules, as mandated by the Intelligence Reform and Terrorism Prevention Act, it is impossible to provide a comprehensive assessment of the sufficiency of FinCEN’s proposed regulations. Thus, in light of these significant implications for citizen and consumer privacy, EFF respectfully requests FinCEN to reconsider the proposed rules.

Citizens’ Privacy Rights were Inadequately Represented when Drafting the Proposed Rule

Because these proposed rules’ implicate American citizens’ privacy, FinCEN should have sought the perspective of privacy advocates in the drafting of the proposed rule. During the formulation of the proposed regulations, FinCEN sought the opinions of a wide variety of stakeholders, including financial institutions,²³ various law enforcement agencies,²⁴ and other foreign financial intelligence units,²⁵ yet the documents provided to EFF do not show the agency talked with any of the many privacy rights organizations in the United States or abroad.

While financial institutions likely value their customers’ privacy, other competing interests, such as cost, can complicate that concern, making financial institutions inadequate advocates for the privacy rights of American citizens. For example, FinCEN based its decision to lower the reporting threshold for financial institutions, in part, on financial institutions’ potential exposure to liability under the Right to Financial Privacy Act (“RFPA”).²⁶ Congress passed the RFPA in order to provide statutory protection for American citizens’ privacy interest

²³ See, e.g., Cross-Border Electronic Transmittals of Funds Survey, 71 Fed. Reg. 14289 (March 21, 2006) (“[FinCEN] requests comments on a survey that seeks input from trade groups representing members of the U.S. financial services industry.”).

²⁴ See, e.g., Financial Crimes Enforcement Network, Implications and Benefits of Cross-Border Funds Transmittal Reporting, 6-38 (January 2009).

²⁵ See, e.g., *id.* at 30-1 (“FinCEN contacted representatives from multiple international [financial intelligence units] to identify their current use of cross-border funds transmittal data.”).

²⁶ Right to Financial Privacy Act, 12 U.S.C. § 3401 *et seq.*

in their sensitive banking and financial information.²⁷ The Act imposes liability on financial institutions that disclose their customer’s private information without authorization;²⁸ the statute also provides an exception for disclosures required by the government.²⁹ Rather than propose a rule requiring disclosure at and above the \$3,000 level — a level that, according to law enforcement agencies, would provide a “sufficient basis for meaningful data analysis” — FinCEN proposed, after consultation with financial institutions, that *all* CBEFTs be reported. As the agency states, this rule avoids “subjecting [financial] institution[s] to liability” for any reports inadvertently made on transactions below the \$3,000 threshold.³⁰

The logic of FinCEN’s decision — to require reporting of *more* sensitive information to the government rather than subject financial institutions to potential liability for violating the law — runs contrary to Congress’ purpose in passing the RFPA in the first instance and demonstrates the inadequacy of financial institutions as advocates for citizen privacy interests. While financial institutions may, at times, value their customers’ privacy interest in financial information, that interest is not absolute and may be outweighed by the financial institution’s own interests.

Law enforcement officials are no exception to this rule, either: officials may legitimately value the privacy interests of citizens, but the pressure to collect and analyze more data can be overwhelming, especially when that pressure comes from elected officials. Without the perspective of dedicated privacy advocates, the proposed regulations will inevitably compromise

²⁷ The RFPA was passed in direct response to the Supreme Court’s decision in *United States v. Miller*, 425 U.S. 435 (1976), which held that no reasonable expectation of privacy — and, thus, no Fourth Amendment protection — attached to financial information disclosed to a bank.

²⁸ 12 U.S.C. § 3417.

²⁹ 12 U.S.C. § 3402.

³⁰ See Cross-Border Electronic Transmittal of Funds, 75 Fed. Reg. 60377, 60385 (proposed September 27, 2010).

the privacy interests of American citizens. Thus, EFF strongly urges FinCEN to reconsider the proposed rules with the active participation of privacy advocates.

FinCEN Has Not Demonstrated that Adequate Technical and Data-Security Systems are in Place

Along with the absence of input from privacy advocates, the absence of documentation demonstrating rigorous analysis of the technical and data security requirements for the proposed rules similarly threatens to compromise the privacy interests of American citizens. The IRTPA mandates that “[n]o regulations . . . be prescribed” before FinCEN certifies to Congress that the agency “has the technological systems in place to effectively and efficiently receive, keep, exploit, protect the security of, and disseminate information from reports of cross-border electronic transmittals of funds.”³¹ While the statute does not mandate that certification occur prior to the notice of proposed rulemaking, any thorough assessment of the proposed rule necessarily must include an assessment of the technical security precautions undertaken by FinCEN. Through our FOIA request, EFF specifically sought information related to the data-security and technical assessments the agency had performed;³² however, the agency’s response was limited to the generic assessments that had already been made public. The agency did not provide any information demonstrating that adequate systems have been designed or are in place to securely transmit, store, access, and analyze 7.5 billion individual CBEFT reports.³³ In the absence of Congressional certification or other supporting documentation demonstrating robust data-security reviews, it is impossible to provide fully-informed and comprehensive comments on the propriety of the proposed regulations.

³¹ 31 U.S.C. § 5318(n)(5)(b).

³² See Section II, *supra*.

³³ FinCEN estimates it will receive 750 million reports annually. Cross-Border Electronic Transmittal of Funds, 75 Fed. Reg. 60377, 60388 (proposed September 27, 2010). The agency has stated it intends to “maintain five years of CBFT data online and readily available, with another five years of archival data stored electronically.” See Financial Crimes Enforcement Network, Implications and Benefits of Cross-Border Funds Transmittal Reporting, 32 (January 2009).

Given the serious privacy implications of the proposed regulations, EFF respectfully requests that FinCEN revisit the proposed regulations by soliciting the opinions of privacy experts and advocates and by performing, and publishing, analysis of the technical requirements necessary for the proposed regulations.

IV. Conclusion

When combating money laundering and terrorism financing, it is vital that our government's response strike a considered balance between the legitimate law enforcement need for information and the privacy interests of American citizens. These regulations, as proposed, do not strike that balance. FinCEN has not justified the need for such vast quantities of sensitive information and has failed to adequately assess the serious, concomitant privacy implications of the proposed regulations. In light of these considerations, EFF respectfully requests FinCEN to thoroughly reconsider the need and privacy impact of the proposed rules.

Respectfully Submitted,

Mark Rumold
Open Government Legal Fellow
Electronic Frontier Foundation

Jennifer Lynch
Staff Attorney
Electronic Frontier Foundation