WesPay

Washington Update

Payments News from our Nation's Capital

March 2014

$25 per Issue • $200 Annual Subscription

Authors:
Craig Saperstein - craig.saperstein@pillsburylaw.com
Deborah Thoren-Peden - deborah.thorenpeden@pillsburylaw.com
Pillsbury Winthrop Shaw Pittman LLP

Contents

Obama Administration Cybersecurity Framework Published

In February, the National Institute of Standards and Technology ("NIST") published Version 1.0 of the Framework for Improving Critical Infrastructure Cybersecurity ("Framework"), developed to assist organizations in critical infrastructure sectors, including the financial services sector, in managing cyber threats. The Framework is very similar to the Preliminary Cybersecurity Framework ("Preliminary Framework") issued by NIST last October and discussed in a previous edition of this newsletter. Like the Preliminary Framework, the final Framework is voluntary in nature and largely relies on existing standards and best practices developed by both industry and government. However, in a departure from the Preliminary Framework, the new Framework scraps the Preliminary Framework's detailed, prescriptive appendix focusing on privacy protection and instead features a more concise, less prescriptive privacy discussion. In addition, the Framework is accompanied by a new "Roadmap" that identifies current challenges to the American cybersecurity infrastructure.

Refresher on Obama Administration Cybersecurity Initiative

In February 2013, President Obama signed an Executive Order and issued a Presidential Policy Directive ("PPD") to enhance cybersecurity for "critical infrastructure," which refers to the systems and assets (whether virtual or physical) that are so vital that their incapacity or destruction would have a debilitating impact on security, public health, or the economy. The PPD identifies the financial services industry as one of 16 critical infrastructure sectors upon which federal cybersecurity policy should focus. In turn, the President's Executive Order directed NIST, by February 2014, to develop a voluntary, technology neutral Cybersecurity Framework, including voluntary standards and industry best practices, to reduce risks to critical infrastructure operators and owners.

In the wake of the Executive Order, NIST began to gather information from government agencies and critical infrastructure sector stakeholders to develop a Preliminary Framework. The Preliminary Framework, published in October 2013, contained three major components: (1) the Framework Core, which is a set of cybersecurity activities that are common across critical infrastructure industry sectors and that consists of the key functions for an organization's cybersecurity strategy; (2) the Framework Profile, which calls upon an organization to identify gaps that need to be addressed as it transitions from the current state of its cybersecurity plan ("Current Profile") to its enhanced "Target Profile"; and (3) Framework Implementation Tiers, which describe how an organization progresses from an informal, reactive approach to cybersecurity to an "agile and risk-informed" approach. An overview of each of these components can be found in the December 2013 edition of this newsletter. NIST requested public comment on the format and clarity of the Preliminary Framework, as well as on the ability and desirability of a wide array of entities to cost effectively implement it.

Framework Hews Close to Preliminary Framework

Building off the Preliminary Framework and the public comments it received in response, NIST released Version 1.0 of the Cybersecurity Framework in February, consistent with its deadline under the President's Executive Order. Beyond removing several minor elements of the Preliminary Framework and adding a discussion of activities related to identifying cybersecurity risks and recovering from cyber attacks, the body of the Framework is largely similar to that of Preliminary Framework.

However, in a departure from the Preliminary Framework, which prescribed a variety of specific practices for entities to undertake with respect to privacy protection and civil liberties in a detailed appendix, the Framework instead provides a short "general set of considerations and processes" that may be of assistance in ensuring that privacy is protected in the midst of an entity's cybersecurity activities. These recommendations include ensuring

that an organization's cybersecurity risk assessment and responses consider privacy implications, its and its service providers' processes promote compliance with cybersecurity rules, and its workforce is adequately trained regarding the entity's cybersecurity policies. Beyond these general practices, the privacy methodology calls on an organization to take steps to identify and address the privacy implications of its access control measures, to conduct privacy reviews of key cybersecurity practices, and to assess and address the circumstances and the extent to which personal information is shared outside the organization as part of cybersecurity information sharing activities. NIST will hold a workshop focused on the advancement of privacy engineering as a foundation for identifying technical standards that could be used to mitigate cybersecurity events' impact on privacy in the coming months.

As a supplement to the Framework, NIST released the Roadmap for Improving Critical Infrastructure Cybersecurity, which discusses challenges to combatting cybersecurity and the agency's forthcoming activities, in conjunction with industry stakeholders, to further develop cybersecurity standards. In the Roadmap, NIST intimates that it may be appropriate to transfer responsibility for further evolution of the Framework to a non-governmental organization. However, before such a transfer occurs, NIST plans to receive informal input from stakeholders on the Framework until it issues a formal notice of revision to the Framework, likely later this year. NIST will also hold public workshops to consider improvements that should be addressed in future iterations of the constantly evolving Framework. These areas will include:

- **Authentication:** The Institute notes that it will continue to support the development of better online authentication technologies so that individuals can augment passwords (which it describes as "something you know") with authentication methods focused on "something you have," or "something you are," such as a token or biometric.
- **Automated Sharing of Indicator Information:** NIST will work with public and private partners to promote adoption of automated sharing of indicator information, which, it contends, will allow organizations to more easily detect and respond to cybersecurity events.
- **Conformity Assessment:** To improve an organization's understanding of how its products, services, or systems meet requirements for managing cybersecurity risk, NIST will work with partners to ensure that existing conformity assessment programs are leveraged.
- **Cybersecurity Workforce:** NIST will promote its current and future cybersecurity workforce training initiatives and aim to extend its activities across all critical infrastructure sectors. The agency will also support training and education, as well as research opportunities to enhance such training and education.
- **Data Analytics:** NIST will work to measure some of the fundamental scientific elements of big data and will participate in standard-setting activities focused on advancing data analysis.
- **Cybersecurity Standards for Federal Agencies:** NIST will spearhead an effort to identify areas of alignment between the Framework and existing federal agency policies related to cybersecurity risk management practices.
- **International Collaboration:** NIST will work with foreign governments, as well as international standard-setting bodies, to explain the Framework and align it with other approaches where possible. It will also encourage businesses to engage in international standard-setting activities.
- **Supply Chain Risk Management:** NIST will encourage industry engagement to promote the mapping of existing supply chain risk management standards and to identify challenges to supply chain risk management, so that supply chain participants that "design produce, source and deliver products or services" are accounted for in cybersecurity risk assessment and mitigation strategies.

Will the Framework Make a Difference?

Although the Obama Administration has publicized the development of the Framework as an impactful accomplishment, members of the Administration still publicly concede that, without proper incentives, many organizations may hesitate to adopt the best practices articulated in the Framework or to assist in propelling forward the activities outlined in the Roadmap. The Obama Administration has acknowledged that legislation or regulations may be necessary to authorize such incentives. We will report on further developments related to the Administration's implementation of the Framework and on the continuing debate in Congress on cybersecurity issues in future editions of this newsletter.

CFPB Proposes Supervision for Larger Participants in International Money Transfer Market

On January 31, 2014, the Consumer Financial Protection Bureau ("CFPB") proposed that large money transfer businesses that conduct at least one million international money transfers annually should be subject to the Bureau's supervisory authority. The impact of the proposed rule, if adopted, is that such businesses – like other "larger participants" in certain non-bank financial markets – would be subject to examinations and information requests, just like those that large depository institutions must incur.

Background on CFPB Larger Participant Authority and Remittance Standards

The CFPB asserts, under the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank"), that it is authorized to supervise – that is, to conduct on-site and off-site examinations of and request documents from – large depository institutions, as well as certain larger participants in non-bank financial markets, to assess financial institutions' compliance with federal law and to detect and assess risks to both consumers to consumer financial markets. Although the Bureau notes that examinations vary by market and by entity, generally the Bureau will start the supervision process by meeting with a supervised entity's management, requesting records, and reviewing the entity's compliance management system. Thereafter, the examiners will set forth the scope of an on-site examination and then coordinate with the supervised entity to set up on-site and off-site discussions regarding the entity's policies and procedures and further review of documents and records. At the end of an examination, the CFPB may issue confidential examination reports, supervisory letters, and compliance ratings for the supervised entity.

Specific to nonbank financial markets, Dodd-Frank gives the Bureau explicit authority to supervise larger participants in the payday loan, mortgage origination and servicing, and private education loan markets. However, Dodd-Frank also gives the CFPB discretion to develop rules governing supervision of larger participants in other nonbank financial markets. In an initial notice issued in 2011, CFPB suggested that it was considering extending its nonbank supervision program to larger participants in the debt collection, consumer reporting, consumer credit, money transmitting, check cashing, prepaid card, student loan servicing, and debt relief services markets. Since then, the Bureau has implemented thresholds for supervision – typically based on a company's annual receipts – of "larger participants" in the debt collection, consumer reporting, and student loan servicing markets, but has not yet done so in the other markets. Late last year, the CFPB reiterated in its semiannual regulatory agenda that it will propose regulations to extend the scope of its supervision to larger participants in other nonbank financial markets.

In tandem with its development of a policy for supervision of large nonbank financial institutions, the Bureau continues to implement substantive rules related to consumer products or services. As reported previously in this newsletter, one such rulemaking related to new requirements for financial

institutions and money services businesses ("MSBs") that facilitate funds transfers, including wire transfers, ACH transactions and other international payments, from U.S. consumers to foreign recipients. The so-called "remittance rules," which entered into effect in October 2013, impose extensive new disclosure requirements, as well as significant consumer protections, for international remittance transfers of more than $15. The regulations generally require a remittance transfer provider that facilitates at least 100 transfers per year to disclose the actual amount of currency to be received prior to the initiation of the transfer, as well as after initiation of the transfer, in the form of a receipt, as well as other requirements. Given that the remittance rules are now in place, some industry observers have expected that the CFPB would likely develop standards to ensure that larger participants in the international money transfer market are complying with such rules, just as depository institutions must do. The CFPB has already published examination procedures for remittance transfers provided by both bank and nonbank remittance transfer providers, released last October; the Bureau has stated that such procedures would apply to larger participants in the nonbank international money transfer market once regulations defining the CFPB's larger participant authority for that market are finalized.

Proposed Rules Sets 1 Million Transfer Threshold for Money Transmitter Supervision

In late January, the CFPB issued a Notice of Proposed Rulemaking to define larger participants in the market for international money transfers, which the Bureau characterizes as electronic transfers of funds sent by nonbanks from consumers in the United States to persons or entities abroad, regardless of whether the consumer sending the funds holds an account with the nonbank provider. In the proposal, the Bureau suggests that a provider's "aggregate annual international money transfers" should be the criterion to measure whether a company is a larger participant and therefore will be subject to supervision. The agency suggests this factor is the most useful metric because it reflects the number of interactions a company has with consumers and, according to Bureau research, many money transfer providers already assemble such data for internal business purposes since many providers are compensated on a per-transfer basis. The measure would include international money transfers in which an agent – such as a grocery store or convenience store – acts on a transfer provider's behalf. However, it would not include transfers in which another company provided the transfers and the supervised nonbank financial institution performed activities as an agent on behalf of that other company, unless the nonbank was acting as an agent on behalf of an affiliated company.

Under the proposed rule, a nonbank participant would be considered a larger participant if it has at least one million aggregate annual international money transfers. Such as threshold, the CFPB estimates, would subject approximately 25 international money transfer providers – which, collectively, provided about 140 million transfers in 2012, with a total volume of approximately $40 billion – to supervision. According to the CFPB, the 1 million transfer threshold would capture approximately 90 percent of the nonbank market for such services and would consist of both companies that send money to a variety of countries around the world, as well as companies that focus on transfers to specific regions or countries.

CFPB Requests Comment on Proposed Rule

Through April 4, 2014, the CFPB will be accepting comment on its proposal to apply its supervision authority to nonbank international money transfers providers that provide at least 1 million aggregate transfers per year. In particular, the Bureau requested comment on the following issues:

- Should the CFPB clarify, modify, or substitute the definitions for key terms contained in the rule, such as "international money transfer," "international money transfer provider," or "aggregate annual international money transfers?"

- In determining whether a nonbank participant in the international money transfer market is a "larger participant" worthy of supervision, should the Bureau retain its proposed measure of aggregate annual international money transfers, or should it use a different metric, such as annual receipts or annual transmitted dollar volume?
- Should the CFPB consider a lower or higher threshold than 1 million aggregate annual transfers, such as 500,000 on the lower end or 3 million on the higher end? According to the Bureau, a threshold of 500,000 would subject three additional companies to supervision that collectively comprise approximately 1.5 percent of the market for international money transfers. In contrast, if the CFPB were to raise the threshold to 3 million aggregate annual transfers, only about 10 participants, covering approximately 75 percent of the market, would be supervised.
- Should the Bureau establish different threshold for larger participants based on the region that is the destination for the money transfer? Although the CFPB asserts that it is considering this region-based alternative, the notice cautions that such an approach could be difficult to administer, given that it is not aware of any data sources to support it and that transfer volumes could shift based on market forces and political events.

Comments on these issues, and any others raised by the proposed rule, can be submitted to the CFPB at http://www.regulations.gov, identified by the Docket Number CFPB-2014-0003. The CFPB expects that a final rule arising from its proposal would be effective no earlier than 60 days after such a final rule is published, though the Bureau gave no indication as to how soon it will move forward with a final rule after comments are received. We will continue to monitor this rulemaking and report on any developments in future editions of this newsletter.

About the Authors: ***Craig Saperstein*** *is an attorney in the Public Policy practice of Pillsbury Winthrop Shaw Pittman LLP in Washington, D.C. In this capacity, he provides legal analysis for clients on legislative and regulatory developments and lobbies congressional and Executive Branch officials on behalf of companies in the payments industry.* ***Deborah Thoren-Peden*** *is a partner and member of the Financial Institutions Team at Pillsbury Winthrop Shaw Pittman LLP. She provides advice to financial institutions, bank and non-bank, and financial services companies.*

www.wespay.org
300 Montgomery St, Suite 400
San Francisco CA 94104
(415) 433-1230