Secure Payments Task Force Meeting
Federal Reserve Bank of Richmond, Charlotte Branch
June 8-9, 2017 Meeting Summary

Welcome and Opening Remarks[1]
Gordon Werkema, Federal Reserve Payments Strategy Director, welcomed the Secure Payments Task Force (SPTF) to the meeting. He noted the progress made by the SPTF on its work group efforts since the March SPTF meeting. Todd Aadland, Payments Security Strategy Leader, also spoke to this and provided additional detail on the SPTF process to advance its key deliverables towards publication. Mr. Aadland then introduced new SPTF members and noted that Peter Tapling, Early Warning, and Troy Alvarez, Intel Corp, were elected as the two new Secure Payments Steering Committee (SPSC) members, representing the non-bank provider segment. Lastly, Mr. Aadland provided an overview of the meeting's objectives and agenda.

Web Payments, Verifiable Claims, and Info Sharing Standards at the W3C
Manu Sporny, Digital Bizarre, provided background of some of the work being accomplished by W3C. Mr. Sporny explained that W3C brings companies together, working on different use cases, in order to gain an understanding of the future of the web. Although not mandatory, Mr. Sporny noted that many of their deliverables, which are often in the form of free specifications and standards, are heavily used on the web. Mr. Sporny noted that three W3C work streams may be of interest to the SPTF – web payments, verifiable claims, and information sharing standards. Mr. Sporny believes that the web payments use case is the most useful to the SPTF. This use case aims to make payments easier and more secure on the web, focusing on mobile payments first. The next work stream, verifiable claims, intends to improve the process of Know Your Customer in the digital world. Lastly, to promote information sharing standards, W3C has an Anti-Fraud Blockchain work stream in an incubation phase. This work stream will promote data portability and increase trustworthiness of data sharing. The SPTF was highly engaged and showed interest in examining W3C's work.

Payment Identity Management and Information Sharing Data Sources
Christopher Danvers, American Airlines Federal Credit Union, and Glen Ulrich, U.S. Bank, presented on their individual work groups' work, Payment Identity Management (PIM) and Information Sharing, respectively.

Mr. Danvers updated the SPTF on the progress made on the Payment Use Cases. Since the March SPTF meeting, PIM and Data Protection have incorporated additional SPTF and industry comments. He noted that the industry provided helpful feedback, especially for the ACH use case, and that there was general industry agreement that the Payment Use Cases will be beneficial. In regards to next steps, he explained that the Payment Use Cases are being reviewed by the Law and Regulation Coordination Work Group and their comments will be incorporated before the Decision-Making Framework (DMF) vote scheduled for June/July. Mr. Danvers noted that the Payment Use Cases are on track to be published to the industry in September.

---

[1] John Yanish, Federal Reserve Bank of Minneapolis, reminded those in attendance to participate in a manner consistent with Anti-Trust and other applicable laws.

Mr. Ulrich explained that since the March SPTF meeting, the Information Sharing Work Group has incorporated feedback from both the SPTF and the industry for its Data Sources proposal. The industry feedback confirmed that the Data Sources proposal is beneficial and makes important data information more accessible. Additionally, there was consensus that the proposal is thorough and accurate. Based on the progress of the Information Sharing Work Group, Mr. Ulrich explained that a DMF vote is scheduled for June/July, followed by the publication of the Data Sources in September.

Payment Security Framework
Tammy Hornsby-Fink, Federal Reserve Bank of Richmond, explained that the PIM White Paper and Data Protection Framework have merged into one deliverable, the Payment Security Framework. This was done based on the complementary work being produced by the PIM and Data Protection work groups. The Payment Security Framework is comprised of five components – Stakeholder Perspectives, Payment Security Principles, Baseline Security Practices, Recommended Security Practices, and the Look Forward on Payment Security. [2] Ms. Hornsby-Fink explained that the work groups are seeking feedback on the first four components of the Payment Security Framework, with a specific emphasis on the Baseline and Recommended Security Practices. She updated the SPTF on specific modifications to the components since last reviewed by the SPTF. First, the work groups incorporated SPTF feedback from the March SPTF meeting into the Stakeholder Perspectives, which provided more detailed descriptions for each perspective, additional perspectives, and more clearly differentiated between consumer and business points of view. Second, the SPTF input expanded on the Payment Security Principles to relate more broadly to payment security, as opposed to data protection specifically. Lastly, Ms. Hornsby-Fink explained that the Baseline and Recommended Security Practices are newly drafted by the work groups and relate to each Payment Security Principle, using the NIST framework.

During the break out session, the SPTF members were asked to provide comments on the Payment Security Principles and their supporting attributes, as well as the identified Baseline and Recommended Security Practices. The SPTF focused mainly on providing feedback on the principles and their attributes. For the four Payment Security Principles, across the SPTF segment groups, there was general agreement that each provides a good foundation for the Payment Security Framework and that the supporting attributes reflect its corresponding principle. Of the feedback received, most of the SPTF segment groups noted the need for additional clarity and description for the principles. The SPTF also provided potential additional principles, which mainly focused on technology, security risks, and education. Ms. Hornsby-Fink explained that the work groups plan to create an industry plan, hold a DMF vote in November/December, and publish the framework in the first quarter of 2018.

Communications, Industry Feedback, and Identity and Branding
Gloria Dugan, Federal Reserve Bank of Chicago, provided an overview of the key themes used for industry engagement. Specifically, there is a focus on identifying potential uses for a deliverable and who might utilize it within an organization. To reach different types of users, Ms. Dugan explained that the Design and Delivery Advisory Team are considering various formats for each deliverable – online resource center, print, webinar, etc. The Design and Delivery Advisory Team will be working on an industry communication plan and developing a microsite in July/August, which will launch in September. Based on the increased communications with the industry, the Design and Delivery Advisory Team will

---

[2] Within the Payment Security Principles component of the Payment Security Framework, there are four main principles – data quality, reliability, and integrity are consistently managed; devalue confidential and transactional data; access is monitored and managed; and develop and manage supporting payment security processes.

provide the SPTF with necessary communication tips and continue to promote the SPTF work at industry conferences. Finally, Ms. Dugan unveiled the new branding of the SPTF.

Ransomware Discussion
Brian Peretti, Department of Treasury - OCIP, provided an overview of how the United States Department of Treasury (Treasury) is approaching the issue of ransomware. Due to the fast innovations in technology, dynamic risks are often a result. Of these risks, the Treasury is primarily focused on maintaining the economy and general safety. Mr. Peretti provided an example of an international ransomware attack, which required much support from the Treasury to monitor the domestic financial sector. In order to mitigate these attacks, Mr. Peretti explained the importance of the SPTF to continue educating and recommending baseline practices and plans, in order to reduce industry risk. Based on the discussions held, the SPTF was in agreement that safe and complex barriers are pertinent in security systems to promote protection. Finally, Mr. Peretti reminded the SPTF that the Treasury is not a regulator, which would typically review security baselines; however, he mentioned that the Treasury does communicate with regulators in order to have a better idea of the landscape and the amount of risk being taken on.

Standard Fraud Reporting Requirements
Ed O'Neill, Federal Reserve Bank of Chicago, reviewed the Standard Fraud Reporting Requirements, noting that the purpose is to create a structure that aligns current fraud metrics with future ones, by payment type. Since the March SPTF meeting, the Information Sharing Work Group has incorporated much of the feedback and particularly focused on developing the outlined Fraud Reporting Channels, Fraud Reporting Categories, and definitions within those sections. Mr. O'Neill noted that the Information Sharing Work Group is soliciting additional feedback from the SPTF.

The SPTF assembled into two groups, card payment and non-card payment, to review the Standard Fraud Reporting Requirements and determine whether the Fraud Reporting Channels, Fraud Reporting Categories, and definitions are accurate and factually correct. Of the input provided by both groups, the majority focused on the need to be more accurate and include additional detail for each payment type. Mr. O'Neill explained that once this input is incorporated by the work group, the work group will aim to receive industry feedback in the fall of 2017, hold a DMF vote in November/December, and publish the Standard Fraud Reporting Requirements in the first quarter of 2018.

Federal Reserve Engagement in Payment System Security
Mr. Aadland explained that later in 2017, the Federal Reserve System will be better positioned to communicate its next steps with the SPTF. He explained that the Federal Reserve System is using an analysis of industry progress and discussions with industry participants to guide the next steps. Based on the discussions held, there was support for the Federal Reserve System to continue in some capacity, such as to continue to lead the industry dialogue, assist in the industry adoption process of secure payments enhancements, and, based on industry trust in the Federal Reserve System, support the standardization of fraud reporting and sharing. Mr. Aadland then asked SPTF members to communicate specific challenges that they as still facing within the payments industry. The SPTF noted industry challenges, such as the lack of information sharing trustworthiness, regulation, and pressures to be current on various industry innovations. It was noted that many of these challenges are reinforced by the environment, finances, and lack of collaboration.

Closing Remarks

Mr. Aadland thanked the SPTF members for their participation at this meeting and their ongoing commitment to the Task Force. He quickly reviewed the opportunities for SPTF members to attend upcoming drop in calls aimed at reviewing the DMF process, since there are many planned votes this summer. He then reviewed the remaining meeting dates for 2017.