In Pursuit of a Better Payment System

Secure Payments Task Force

Secure Payments Task Force

November 1 - 2, 2017

Federal Reserve Bank of Richmond, Charlotte Office

Charlotte, NC

Anti-Trust Compliance Statement

Task Force Participants are expected to ensure that their participation and communications at Task Force meetings do not violate antitrust laws.

This means that no activity or discussion at our meetings or other related functions may be engaged in for the purpose of bringing about any understanding or agreement among participants to do any of the following: (a) raise, stabilize, or set future prices; (b) regulate future production levels among individual participants; (c) allocate geographic markets or customers; (d) encourage boycotts or seek to exclude specific participants; or (e) aid in creating improper monopolies.

In addition, participants should avoid discussing or revealing any individual participant's competitively sensitive information, including any participant's prices, discounts, costs, capacity, inventory, sales, future business plans, or bids for contracts.

Any questions regarding the meaning or applicability of this statement, as well as any concerns regarding activities or discussions at Task Force meetings, should be promptly brought to the attention of counsel for the Federal Reserve Bank, present at the meeting.

Opening Remarks

Todd Aadland

Meeting Objectives

- Outline progress and activities to support advancing the phase one task force deliverables
- Exchange information from industry experts on payments security initiatives
- Engage in discussion to align on next steps for phase two task force deliverables
- Highlight the evolution of the Secure Payments initiative

Agenda – Day 1

Time (ET)	Topics	Speakers
1:00 -1:15 p.m.	Opening Remarks	Todd Aadland
1:15 - 1:30 p.m.	Welcome	Dave Sapenaro and Esther George (recorded remarks)
1:30 - 1:45 p.m.	Information Sharing Data Sources DMF Vote Results	Todd Aadland, Peter Tapling and Glen Ulrich
1:45 - 2:00 p.m.	SPTF Website Launch Preview and Communication Plan	Meagan Musgrave, Amma Guerrier and Gloria Dugan
2:00 - 2:45 p.m.	Payment Lifecycles and Security Profiles (formerly the Payment Use Cases) Panel	Christopher Danvers, Reed Luhtanen, Suzanne Martindale and Peter Tapling Moderator – Todd Aadland
2:45 - 3:00 p.m.	BREAK – Transition to breakout sessions	
3:00 - 4:30 p.m.	Payment Lifecycles and Security Profiles – Segment Breakout	Steering Committee and Breakout Facilitators
4:30 - 4:45 p.m.	BREAK – Transition to plenary	
4:45 - 5:45 p.m.	Understanding NIST Cybersecurity Framework Panel	Ryan McNaughton, Patrick Quentmeyer, Charles Wallen Moderator - Tammy Hornsby-Fink
5:45 - 6:00 p.m.	Day 1 Wrap Up	Todd Aadland
6:00 - 7:30 p.m.	*RECEPTION*	

Agenda – Day 2

Time (ET)	Topics	Speakers
8:00 - 8:15 a.m.	Opening Remarks	Todd Aadland
8:15 - 9:00 a.m.	Payment Lifecycles and Security Profiles Segment Breakouts – Read Out	
9:00 - 9:15 a.m.	Payment Security Framework Overview	Tammy Hornsby-Fink
9:15 - 10:15 a.m.	Payment Security Framework - Table Discussions	Table Facilitators
10:15 - 10:30 a.m.	*BREAK*	
10:30 - 11:30 a.m.	Standard Fraud Reporting Panel	Andrew Churchill, Manish Nathwani and Seth Ruden Moderator - Ed O'Neill
11:30 - 11:45 a.m.	Standard Fraud Reporting Overview	Ed O'Neill
11:45 - 12:45 p.m.	*LUNCH*	
12:45 - 1:45 p.m.	Standard Fraud Reporting – Segment Breakouts	Breakout Facilitators
1:45 - 2:00 p.m.	*BREAK – Transition to plenary*	
2:00 - 2:30 p.m.	Standard Fraud Reporting Segment Breakouts – Read Out	
2:30 - 2:45 p.m.	Next Steps	Dave Sapenaro
2:45 - 3:00 p.m.	Closing Comments	Todd Aadland

Welcome

Esther George and Dave Sapenaro

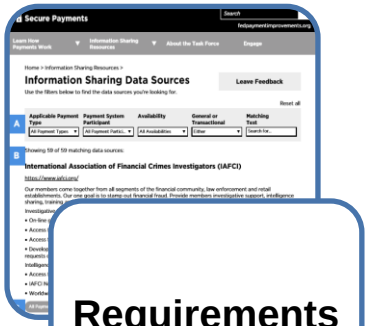
Information Sharing Data Sources DMF Vote Results

Todd Aadland, Peter Tapling and Glen Ulrich

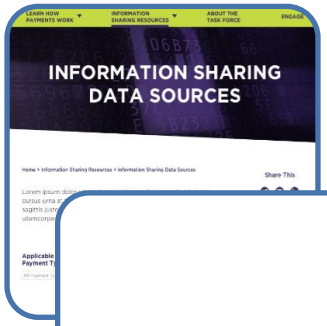
Task Force Microsite

Meagan Musgrave

Microsite Development and Design Process



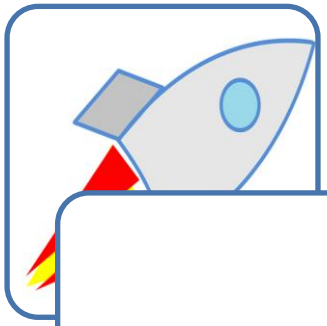
Requirements and Wireframes



Design

In Progress

Production and Testing



Launch!

Design and Delivery Advisory Team

Thank you!

Angi Farren, UMACHA

Amma Guerrier, Xenith Bank

Ryan McNaughton, North American Banking Company

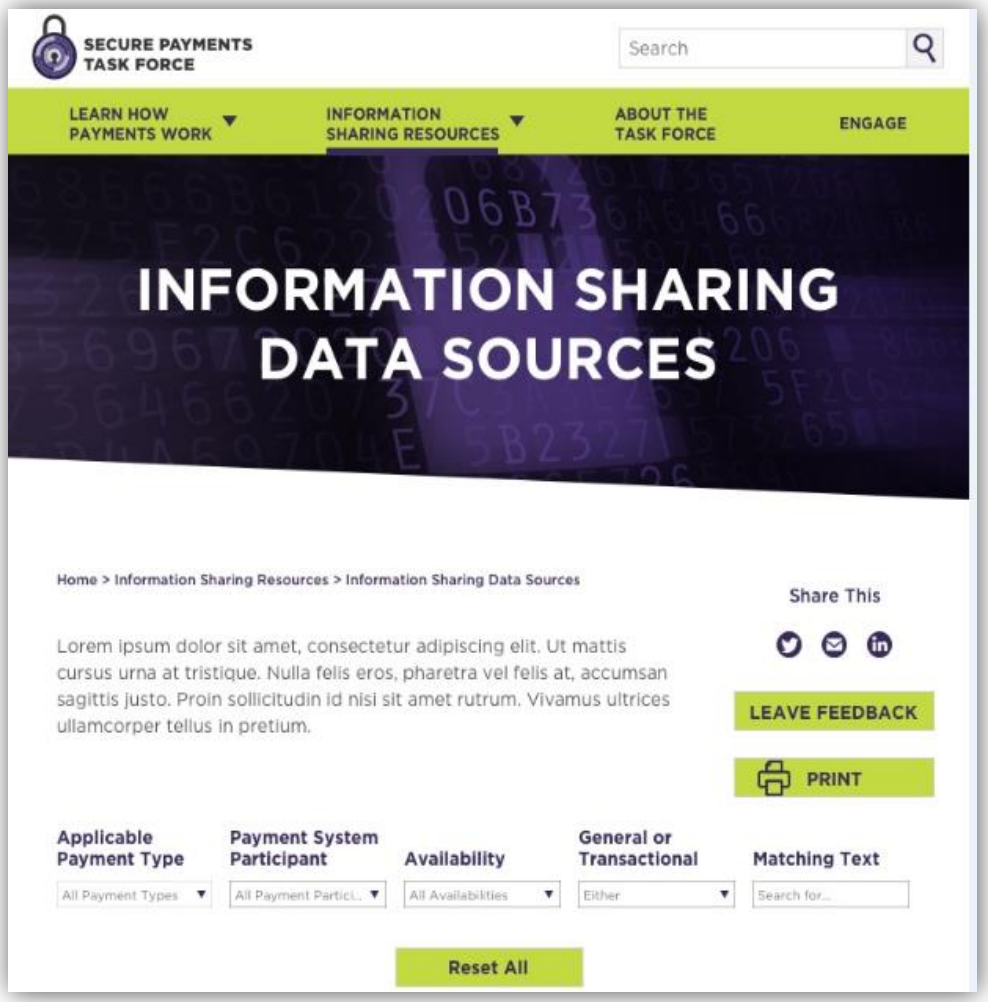
Bryan Penny, Nordstrom

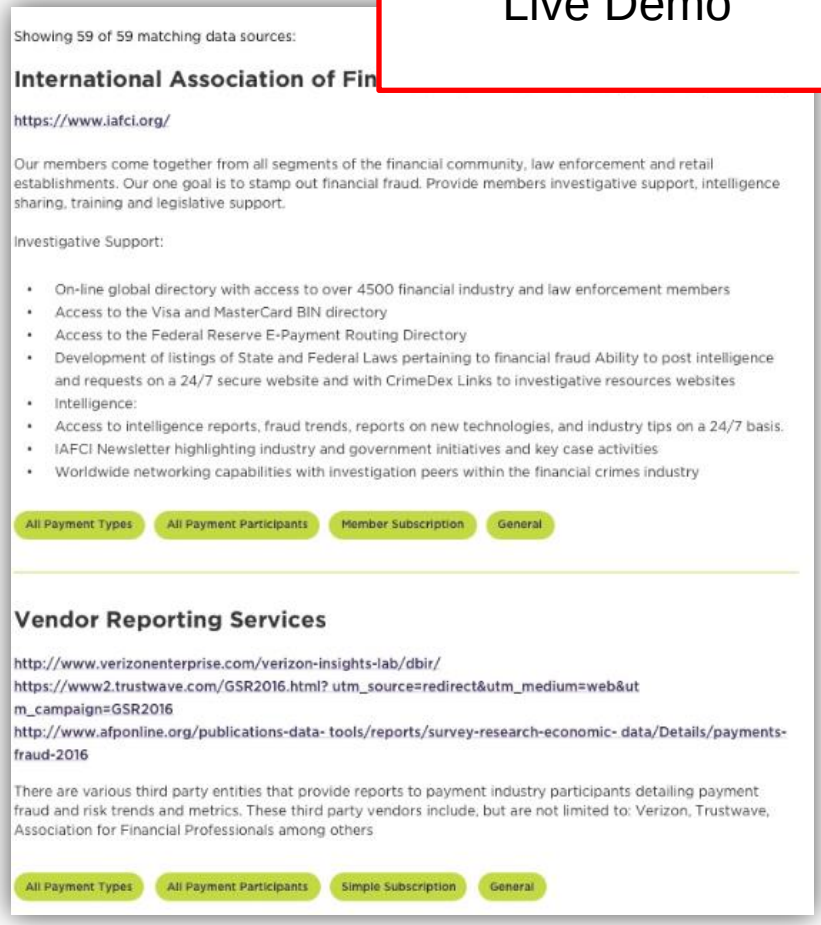
Dave Tatge, R4 Technologies

Gilbert Verdian, VocaLink

Amy Zirkle, Electronic Transactions Association

Information Sharing Data Sources





Live Demo

Microsite Development – Next Steps

Final Testing

Publish on November 17!

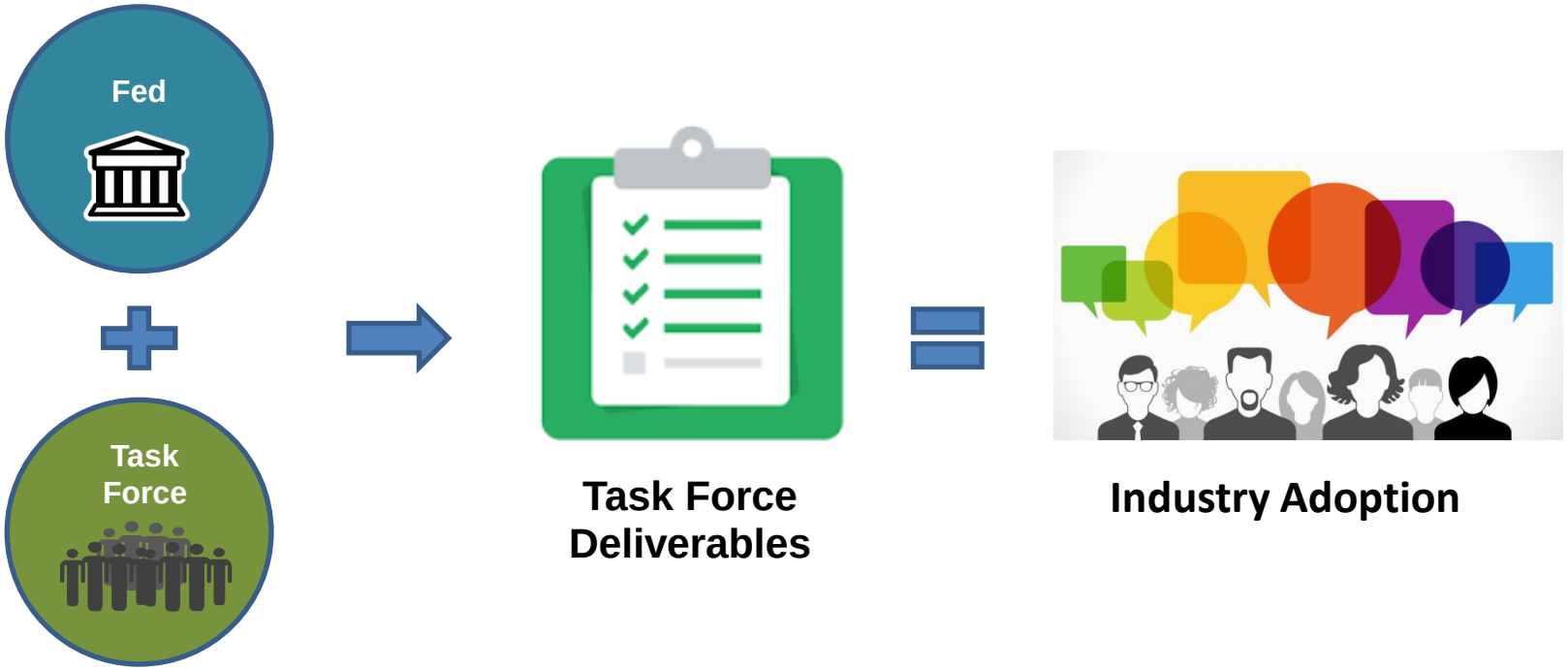
Raise awareness and socialize data sources

Communication Plan

Amma Guerrier, Gloria Dugan

Industry Adoption of Task Force Deliverables

Task Force and Fed partnering to engage industry stakeholders



SPTF and Fed Partnering to Promote SPTF Microsite

Launch Communications

SPTF Support

- Communications tool kit
  - Elevator pitch
  - Email/Blog template
  - FAQs
- Social media postings
  - Steering Committee video testimonials
- Email communications to staff/customers/members

Federal Reserve Support

- Direct email communications
- Task Force microsite
- Newsletter/blogs
- Social media content
- Web content
  - FedPaymentsImprovement.org
  - FRBservices.org

SECURE PAYMENTS TASK FORCE

Communication Plan Timeline

2017 - 2018

October	November	December	2018
	SPTF In-person Meeting 11/1-11/2	**Steering Committee Meeting 12/6-12/7**	

SPTF Deliverables and Microsite

DMF Vote Validation

Microsite Development

Demo

Nov 1-2
Preview microsite with the Task Force

Nov 17
Launch microsite and communications

Task Force Communication Efforts

Nov 16
Distribute the Task Force communication toolkit

Fed Communication Efforts

Payment Lifecycles and Security Profiles Panel

Christopher Danvers, Reed Luhtanen, Suzanne Martindale and Peter Tapling
Moderator – Todd Aadland

Payment Lifecycles and Security Profiles

Segment Breakout

Understanding NIST Cybersecurity Framework Panel

Ryan McNaughton – NABC, Patrick Quentmeyer – Treasury and
Charles Wallen – Spectrum
Moderator - Tammy Hornsby-Fink

Day 1 Wrap Up

Todd Aadland

In Pursuit of a Better Payment System

Secure Payments Task Force

Secure Payments Task Force

November 2, 2017

Federal Reserve Bank of Richmond, Charlotte Office

Charlotte, NC

Day 2 Opening Remarks

Todd Aadland

Agenda – Day 2

Time (ET)	Topics	Speakers
8:00 - 8:15 a.m.	Opening Remarks	Todd Aadland
8:15 - 9:00 a.m.	Payment Lifecycles and Security Profiles Segment Breakouts – Read Out	
9:00 - 9:15 a.m.	Payment Security Framework Overview	Tammy Hornsby-Fink
9:15 - 10:15 a.m.	Payment Security Framework - Table Discussions	Table Facilitators
10:15 - 10:30 a.m.	*BREAK*	
10:30 - 11:30 a.m.	Standard Fraud Reporting Panel	Andrew Churchill, Manish Nathwani and Seth Ruden Moderator - Ed O'Neill
11:30 - 11:45 a.m.	Standard Fraud Reporting Overview	Ed O'Neill
11:45 - 12:45 p.m.	*LUNCH*	
12:45 - 1:45 p.m.	Standard Fraud Reporting – Segment Breakouts	Breakout Facilitators
1:45 - 2:00 p.m.	*BREAK – Transition to plenary*	
2:00 - 2:30 p.m.	Standard Fraud Reporting Segment Breakouts – Read Out	
2:30 - 2:45 p.m.	Next Steps	Dave Sapenaro
2:45 – 3:00 p.m.	Closing Comments	Todd Aadland

Payment Lifecycles and Security Profiles

Report Out

Payment Security Framework Overview

Tammy Hornsby-Fink

Payment Security Framework

Overview

Component	Objective
Stakeholder Perspectives	• Provides valuable insights for users of the framework when determining specific actions to take for their respective organizations
Payment Security Principles	• Foundational elements to frame recommendations
Baseline Security Practices	• Outline minimum security practices
Recommended Security Practices	• Provide additional recommendations based on risk landscape/appetite
Look Forward on Payment Security	• Outline suggested actions to be taken by industry • Outline planned actions of the SPTF • Plan for keeping framework current as payment landscape continues to evolve

Payment Security Framework

Stakeholder Perspectives

- Since June Task Force Meeting
  - Segment drop-in calls to refine Stakeholder Perspectives
  - Reviewed and updated Stakeholder Perspectives based on task force feedback
  - Separated industry standards/rules organizations perspective from regulator perspective
  - Obtained feedback on updated perspectives via task force survey

Payment Security Framework

Current Stakeholder Perspectives

- Biz Users
- Consumers
- Financial Institutions (FIs)
- Industry Standards/Rules Organizations
- Integrators, VARs, Fintechs
- Merchants
- Processors
- Regulators

Payment Security Framework

Stakeholder Perspectives Task Force Survey Results

Segment Representation				
Segment	**Survey #**	**Survey %**	**SPTF #**	**SPTF %**
Business End Users	3	5%	7	3%
Government End Users	0	0%	1	1%
Consumer Interest Organizations	1	2%	2	1%
Large FIs	5	9%	16	8%
Medium FIs	7	12%	19	9%
Small FIs	7	12%	19	9%
Non-Bank Providers	20	35%	68	34%
Other Stakeholders	14	25%	70	35%

Participation in the Stakeholder Perspectives survey was consistent with the composition of the Task Force

Payment Security Framework

Stakeholder Perspectives Survey Results: Highlights

- Value to the Industry
  - Strongly Agree/Agree: 84% (48 participants)
  - Neutral: 12% (7 participants)
  - Disagree: 4% (2 participants)
- Organizations Would Reference the Perspective
  - Financial Institutions (FIs): 70%
  - Biz Users: 51%
  - Consumers: 51%
  - Merchants: 51%
  - Processors: 51%
  - Industry Standards / Rules Organizations: 44%
  - Integrators, VARs, Fintechs: 46%
  - Regulators: 42%
- Comments and suggestions for modifications will be provided to work groups for review and actioning

Payment Security Framework

NIST Cybersecurity Framework Declaration Proposal

- Received a Task Force Declaration Proposal requesting the task force to declare the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) as a recommended cyber-risk management approach for the U.S. payments ecosystem
- Declaration Rationale
  - NIST CSF is a voluntary risk-based approach to managing cybersecurity developed by both public and private organizations
  - NIST CSF has gained broad adoption and significant support from organizations and regulators both in the United States as well as internationally

Payment Security Framework

NIST Cybersecurity Framework Declaration Proposal

- Potential Valuable Outcomes
  - A common collaborative approach to managing cybersecurity risk across industry segments and payment types
  - Strengthen the security of the payments ecosystem to protect data, provide predictable availability and ensure privacy
  - Enhance cybersecurity risk management processes to minimize the potential for the compromise of sensitive payment data thus resulting in a reduction of payments fraud

Payment Security Framework

NIST Cybersecurity Framework Declaration Proposal

Reviewed the Declaration Proposal with work group chairs and the Steering Committee

- Agreed the Declaration Proposal request is in scope for the Data Protection and Payment Identity Management Work Group efforts
  - Payment Security Principles
  - Baseline and Recommended Security Practices
- Referred to the joint work group to determine potential impact of the Declaration Proposal and proposed next steps to be shared with the Steering Committee and task force chair

Payment Security Framework

NIST Cybersecurity Framework Declaration Proposal

Reviewed the Declaration Proposal with the joint work group

- Majority of the work group (87%) agreed the proposal is in scope for the work group's efforts
- Work group discussed the Cybersecurity Framework as a potential security framework for task force endorsement
- Seeking input from the task force to help inform next steps

NIST Cybersecurity Framework Declaration Proposal

Table Discussion

- Reflect on the NIST Cybersecurity Framework Declaration Proposal when considering the following:
  - Has your organization utilized or referenced the NIST Cybersecurity Framework?
  - What are your opinions on the value of the NIST Cybersecurity Framework to your organization?
  - What are your opinions on the value of the NIST Cybersecurity Framework to the payments industry?
  - What are your views on the task force endorsing the NIST Cybersecurity Framework versus continuing to develop our own?

Payment Security Framework

Table Discussions

Standard Fraud Reporting Panel

Andrew Churchill – Midas Alliance, Manish Nathwani – Shazam and Seth Ruden – ACI

Moderator – Ed O'Neill

Standard Fraud Reporting Overview

Ed O'Neill

Standard Fraud Reporting Proposal

Overview

- Background
  - Identify opportunities to standardize the fraud reporting types, categories and definitions by payment type
    - Common taxonomy for the industry to leverage when reporting, communicating and benchmarking fraud data by payment type
  - Evaluate the identification/creation of a channel to capture, analyze and report fraud data by payment type
- Progress since June Task Force meeting
  - Updated the fraud reporting types, categories and definitions for each payment type based on feedback from the task force
  - Conducted initial meeting with the credit card networks as a potential aggregation point

Standard Fraud Reporting Proposal

Overview

Component	Objective
Fraud Reporting Types	• Describe the environment where a fraudulent transaction can originate
Fraud Reporting Categories	• Identify the types of fraud that could occur within a specific fraud type or within a specific payment type (where a fraud type has not been defined)
Fraud Reporting Category Definitions	• Identify the definitions of each Fraud Reporting Category

Aggregation Points	• The organizations that need to be engaged to:
	  • Agree upon the definition and data mappings for each Fraud Reporting Category within each Fraud Reporting Type
	  • Provide the data to the curator
	  • Agree upon the fraud metrics and reports to be published by the curator
	  • Serve as a custodian, along with the payments industry, to help maintain and vet additions/modifications to the fraud metrics/reports

Curator	• The organization responsible for:
	  • Working with the Aggregation Points to develop the technical specification to collect the fraud data
	  • Collect the data from the aggregation points, consolidating the data and publishing the agreed upon reports/metrics
	  • Work with the custodians of the data (Aggregation Points and payments industry) to maintain the fraud metrics/reports

Standard Fraud Reporting Proposal

Work Group Discussions

- Industry problem being solved for
  - "Less of a problem but more of a need" to provide consistent, actionable information on fraud across payment types
  - Discussed the need for more of a consistent "enterprise view" of fraud (i.e. across all payment types)
  - Some larger organizations expressed they have the information they need today to benchmark and discuss fraud rates with their peer groups (i.e. Nilson, Auriemma, ABA)
  - Other organizations expressed a need to drive more consistency in the categorization and definition of fraud across payment types to better benchmark performance and track progress of risk mitigation activities
  - Discussed how some payment types (e.g. card payments) have fraud categories and definitions today whereas others are not as defined

Standard Fraud Reporting Proposal

Work Group Discussions

- Uses of standard fraud reporting
  - Some large organizations indicated they have access to the information they need to understand and manage risks
  - Non-Bank Providers would use this information to be better informed on fraud rates by payment type and channel which would help them further educate their customers
  - Small and medium organizations would use this information to help educate their organizations and any correspondents on fraud trends and further inform their risk decisions
  - For payment types where standard definitions of fraud types and categories are not readily available (i.e. Wire or ACH), this information would create a common taxonomy for organizations to track and manage fraud risks

Standard Fraud Reporting Proposal

Segment Breakout Discussion

Reflect on the current proposal from the work group from two points of view for each payment type

- Standardizing fraud reporting types, categories and definitions
  - Describe how your organization/segment would use and benefit from standardized fraud categories, types and definitions?
  - Do the fraud types and categories outlined in the current proposal capture the appropriate level of information? If no, please provide your rationale and proposed alternative
  - What operational impact would this have on your organization/segment?

- Centralizing the collection and reporting of fraud data by payment type (leveraging the industry-established fraud reporting types, categories and definitions)
  - What would the value be to the industry of centralizing the collection and reporting of fraud data by payment type?

Standard Fraud Reporting

Segment Breakouts

Standard Fraud Reporting

Read Out

Next Steps

Dave Sapenaro

Closing Comments

Todd Aadland