

Fraud Measurement Improvement

An ACH and Wire Discussion

In late 2018, a diverse group of 300 industry stakeholders came together at the FedPayments Improvement Community Forum to engage in inclusive dialogue focused on improving the U.S. payment system. Through general sessions and topic-specific workshops, Forum attendees provided their candid feedback about the latest payment modernization efforts.

This highly interactive workshop session offered diverse industry perspectives and in-depth dialogue on the specific need for improved ACH and wire fraud measurement and the Federal Reserve's plan to form a work group to develop recommended ACH and wire fraud definitions.

Highlights From the Panel Discussion

Inconsistent payments fraud definitions are a barrier to effective industry communication and collaboration on fraud mitigation and remediation. A review of secondary research on payments fraud found widely varying survey methods and definitions, as well as little detail about ACH and wire fraud compared with card fraud.

Jim Cunha described that better, more-timely data about where ACH and wire fraud is occurring starts with creating a playbook of consistent fraud definitions.

This is one of the Federal Reserve's four priorities for near-term action to advance payments security, as announced earlier at the Forum by [Ken Montgomery](#), the Federal Reserve's Payments Security Strategy Leader. These priorities are based on research,

input from the [Secure Payments Task Force](#) and ongoing payments industry discussions.

The Federal Reserve intends to [form and lead an industry work group](#) to align and normalize ACH and wire fraud definitions in collaboration with the payments industry, and create a roadmap to encourage broad industry acceptance and use of these definitions.

The desired outcome of this work group is not a mandate or regulation, Cunha emphasized, but rather to strengthen and support timely information sharing and understanding of fraud trends involving ACH and wire payments.

Cunha added that the Federal Reserve does not intend to duplicate or redirect any ongoing

Introduction

Jim Cunha
Senior Vice President
Federal Reserve Bank of Boston

Moderator

Andrés Rapela
Assistant Vice President
Federal Reserve Bank of Boston

industry efforts in this area, but to build on existing work and collaborate as appropriate.

To fulfill its objectives, the ACH and wire fraud definitions work group is expected to operate for nine to 12 months and be composed of 20 to 30 industry and Federal Reserve members with specific expertise.

The work group will be diverse and representative of various

payments stakeholder segments, and will include those with expertise in payments fraud research, institutional fraud governance, fraud operations, ACH and wire operations, fraud systems technology, operational risk management and risk intelligence and analytics.

Tabletop Takeaways

Participants in the tabletop discussion were asked to:

- Validate the scope of the ACH and wire fraud definitions work group.
- Discuss where they see opportunities and challenges in the proposed ACH and wire fraud definitions objectives and work effort.
- List their respective organizations' primary source of timely information on the state of ACH and/or wire fraud.

Attendees were in alignment on the value of this proposed effort. Currently, inconsistent, inaccessible or untimely fraud data makes fraud detection and mitigation a more difficult and less effective task for industry participants. Broadly accepted and consistent ACH and wire fraud definitions would be useful in facilitating efficient and

effective fraud reporting, analytics, fraud resolution and trend analysis.

Scope of fraud data should be holistic and inclusive.

Attendees generally agreed that ACH and wire fraud definitions should include as much information as possible, while ensuring the data is still consumable and interpretable.

For example, the data should include both attempted (unsuccessful) and successful fraud, as well as the various types of fraud (e.g. first, third, induced, etc.). Any data that is generated by the payment initiation is valuable to understanding the exploit.

A divide developed about whether or not to include check fraud definitions in the scope of the proposed work group.

Some attendees pointed out that check fraud is less of a concern because check use has declined and check fraud information is "plentiful." Other attendees said check fraud trends are still relevant to their organizations and with the evolution of this payment type, there can be movement into the ACH space.

There was general agreement that all fraud matters and each payment method requires study in

order to get a full picture of payments fraud.

While helpful, current fraud data sources are difficult to synthesize with one another due to the different taxonomy used in the sources.

When asked how their organizations obtain timely information on payments fraud, attendees said they use internal tracking, third-party vendors, industry associations and media reports. The [American Bankers Association](#), [Association of Financial Professionals](#), [EPCOR](#), [FS-ISAC](#), and [RSA](#) conferences were among the fraud information sources repeatedly mentioned.

Despite the reliability of these resources, attendees highlighted the differences in scope or fraud taxonomy among them, which makes it difficult to reconcile and understand the whole picture.

Attendees also noted that differences in taxonomy impede their ability to gather timely information to quickly mitigate and/or react to fraudulent trends and activities.