Executive Summary

A View of Payments Security: Trends, Gaps and Vulnerabilities

In September 2017, the *Federal Reserve Next Steps in the Payments Improvement Journey* paper called for a study to analyze payments security vulnerabilities. To help inform its next steps to collaborate with the industry to advance secure payments, the Federal Reserve commissioned Boston Consulting Group to assess fraud and associated costs in the U.S. payment system and identify fraud causes and contributing factors. This executive summary highlights key findings of the Boston Consulting Group's review of academic literature, surveys and industry reports on fraud and associated costs. The team also conducted stakeholder interviews to corroborate or help eliminate gaps in the existing research.

Boston Consulting Group Secondary Research Scope

- *Payments fraud* is defined as unauthorized transactions by third parties disguised as authorized users.
- All domestic non-cash payment methods: *credit card*, *debit card*, *ACH*, *wire* and *check*.
- All participants: *issuers* (banks that issue cards), other *banks*, *merchants* (businesses selling goods and services and receiving payments), *corporations* (entities making corporate payments via ACH, check, wire and cards), *government* and *consumers* (who use cards, checks and ACH).

Secondary Research Limitations

- Data gaps across payment methods and stakeholder groups.
- Lack of uniformity in definitions and scope of the various payments fraud studies.
- Divergent survey methodologies used to quantify fraud.
- Inconsistent timing of data in the various studies.
- More recent data (e.g., from 2017 and 2018) were not available at the time of the Boston Consulting Group review.

U.S. Payments Fraud Has Continued to Grow

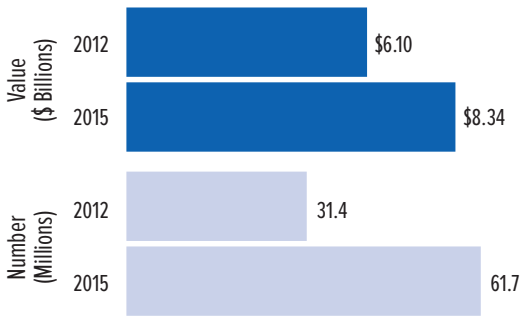
Payments fraud is significant and has grown in absolute terms. The Federal Reserve Payments Study estimated non-cash, non-wire payments fraud was $8.34 billion in 2015, more than one-third larger than $6.10 billion in 2012.[1]

Research reviewed by the Boston Consulting Group confirmed that the overall fraud rate – fraud volume as a percentage of total payments volume – increased for all payment methods combined between 2012 and either 2015 or 2016, depending on the study. Fraud rates vary by payment method and also reflect how fraud mitigation shifts fraudsters to attack other, more vulnerable payment methods or channels. For example, industry reports show a migration from in-person to online (remote) fraud in the United States after the introduction of chip

(continued on back side)

Total Payments Fraud

(Non-Cash, Non-Wire)



1 See the Federal Reserve System report *Changes in U.S. Payments Fraud from 2012 to 2016* published in October 2018.

(continued from front side)

(EMV) cards, mirroring similar shifts in fraud patterns seen in other countries.

Costs to resolve fraud claims and remedy compromised information (*remediation*), as well as to detect and prevent attempted fraud (*mitigation*), could be of a similar magnitude or even greater than fraud losses themselves. A very rough estimate of fraud remediation and mitigation costs based on the Boston Consulting Group's secondary research could be in the range of $7 billion to $15 billion in 2016. In addition, some studies estimated *avoided fraud loss* (known fraud attempts that were prevented through mitigation practices before clearing or settlement) to be significantly greater than reported gross fraud losses – eight times greater for banks and 15 times greater for corporations.

Data Gaps and Inconsistencies

Data gaps and inconsistencies across payment methods and stakeholder groups make it more difficult to assess – and address – payments fraud. Data gaps reflect either the absence of any data points or the lack of concrete, high quality data points that can be used to arrive at a reliable estimation. Three data gaps were uncovered by the Boston Consulting Group secondary research:

- Published payments fraud data lacks distinctions between consumer and business fraud. More details are generally available on types of card fraud than are available for ACH, wire and check fraud.
- Some studies included fraud mitigation and prevention costs only, while other studies included only fraud resolution and remediation costs.
- Some fraud-associated activities are included in broader finance or IT operations, which makes it difficult to determine the portion of costs that are directly related to payments fraud.

U.S. Payment System Vulnerabilities

- **The payments and fraud landscape is shifting as technology evolves.** A sharp increase in payments activity through relatively new channels, such as mobile apps, has created more avenues for fraud. In addition, device proliferation and increased system connectivity offer more endpoints for fraudsters to exploit via sophisticated, large-scale attacks and technology.
- **Uneven resources and capabilities to combat fraud.** Fraudsters exploit the weakest links and highest-return opportunities in the payments ecosystem, including vulnerable endpoints, people, technology and organizations that may lack the fraud-fighting resources and/or experience to effectively prevent and combat fraud.
- **Lack of consistent definitions to measure and track fraud.** Fraudsters are constantly developing alternative types of attacks and searching for new vulnerabilities within the payment system. Despite the speed of change in fraud attacks, timely, reliable and comprehensive fraud data are not shared widely across the industry. This limits the ability of stakeholders to rapidly collaborate to identify fraud patterns, take steps to limit those types of transactions – or simply understand if their loss experience is better, similar or worse than that of others.
- **Individual stakeholder incentives may be misaligned or insufficient to reduce collective fraud losses.** Successfully reducing fraud – not simply deterring fraudsters or deflecting fraudulent acts elsewhere – requires coordinated action by all payments stakeholders, who must balance competing priorities.
- **Reliance on static data that often is compromised.** *Static data* includes Social Security numbers, addresses, account numbers and card expiration dates. These data are used to authenticate transactions, verify identity, and enroll in and access accounts. Given the increasing prevalence of data breaches – and sometimes, oversharing on social media – much of this information is readily available to motivated fraudsters.
- **Inherent weaknesses exist in "people-based" security measures.** People play a critical role in maintaining the sanctity of the payments process, yet consumers and employees can fall prey to fraudsters if they don't understand the risks and how to prevent fraud. Seventy-five percent of all cyber breaches involve human error, estimated the IT Policy Compliance Group.

For more information on how the study will be used to inform the Federal Reserve's next steps to address payments security and vulnerabilities, visit FedPaymentsImprovement.org.