Security
Thought Leadership White Paper

July 2016

Faster payments: Help detect and prevent fraud while speeding up financial processing times in the US

IBM Security Trusteer Pinpoint Detect helps provide detection and prevention in real time to meet shorter processing windows

Introduction

In today's fast-paced world, the expectation often is that everything happens instantaneously. Consider banking, where customers typically expect immediate action on payment transactions and funds transfers from their accounts. In many countries including the UK, Singapore, Nigeria, Poland, Mexico and Sweden, near-instantaneous banking is indeed possible. But it is not possible in the US, where payments are still cleared in the traditional way—once a day, usually overnight—resulting in delays of one or two business days for transferring funds.

Making payments and funds transfers happen in a more immediate timeframe, however, has a great business value both for the customers who use the service and for the financial institutions that provide the service. It has been observed that in the countries where this has been enacted, the usage of transfers has surged thanks to multiple new use cases.[1] Faster transfers have had a significant impact, for example, on business-to-business payments by allowing companies to better predict their cash flow and to earn additional interest on funds they hold for additional business days after transfer. This additional interest can be significant when large sums are involved. Businesses paying out part-time workers can also settle payroll payments faster and more easily. Other examples occur in personal banking, where immediate transfer can help ensure that bill payments are not missed, or in the banking customer's direct account-to-account transfers (P2P) used for settling personal debts.

The National Automated Clearing House Association (NACHA) is the trustee and rule-maker for the United States Automated Clearing House (ACH) network, connecting all financial intuitions and constituting the backbone for the electronic movement of money and data in the US. NACHA is responsible for managing the network's development, administration and governance. NACHA is funded by the financial institutions it governs and directs.

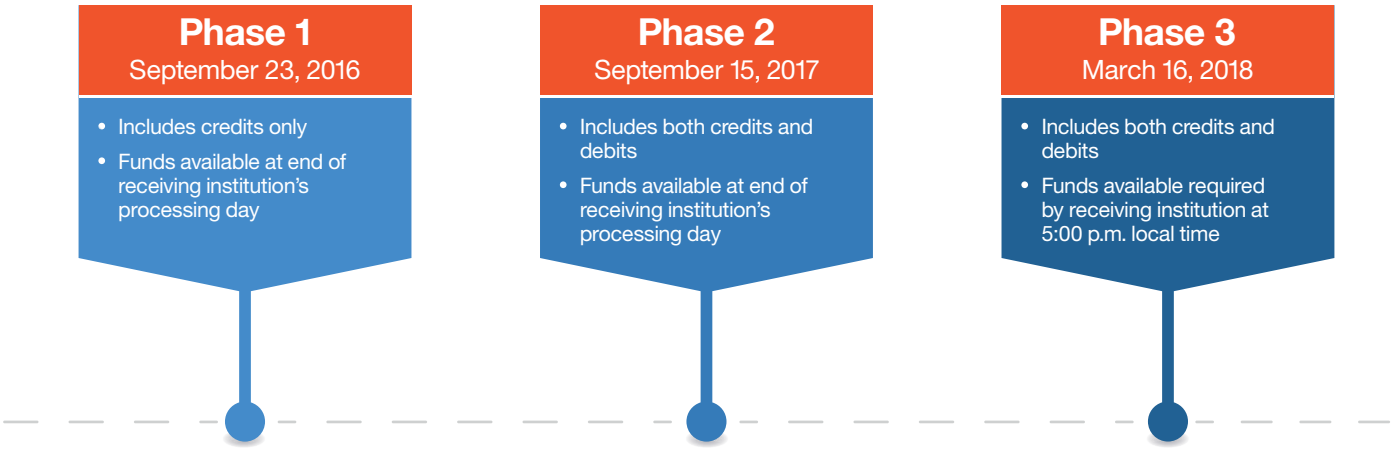
The evolving standards for faster financial processing

Acknowledging the needs of both the financial institution and the customer, as well as expectations for and the business value of faster payments settlement, NACHA recently issued a directive for improving clearing processes known as the Faster Payment Imperative.[2] The directive is a result of a multi-year project to achieve agreement among the various stockholders involved on changes and processes. According to the NACHA directive, two new clearing windows will be established per day for originating financial institutions (ODFI) to submit transactions to receiving financial institutions (RDFI). These new clearing windows will be added to the nighttime clearing window to create a total of three cycles per day. The new windows will be:

- Morning submission deadline at 10:30 a.m. ET, with settlement occurring at 1:00 p.m.
- Afternoon submission deadline at 2:45 p.m. ET, with settlement occurring at 5:00 p.m.

The current directive excludes international transactions and transactions larger than USD25,000. It includes three implementation phases starting September 23, 2016 and completing March 16, 2018.

Three-phase implementation for NACHA Faster Payments Imperative



What are the implications of online fraud?

Not being the first country to implement faster payments allows US financial institutions to learn from others' experience about the potential effect on financial fraud that new standards create.

For example, the UK, which moved to a fast 15 seconds clearing time in 2008, found that the change virtually provided cybercriminals with a faster getaway vehicle. Financial institutions in the UK experienced an increase of 132 percent in online-banking fraud losses over the two years preceding implementation of the new standards (from GBP22.6 million to GBP52.5 million).[3] It was not until 2010 that the UK started getting online fraud under better control through the use of advanced real-time agile protection technologies.

The challenges for the financial industry in the UK in fighting online fraud were a result not only of the move to real-time processing but also of the magnitude of the change in the time required to detect and react to fraud. Shortening the time span required for processing funds from hours to seconds was a major factor in enabling fraud. As is the case in the US, many UK financial institutions were employing legacy backlog off-line procession solutions based on periodic transactions anomalies assessment, which are ineffective in the new world of rapid processing. Slow-acting security solutions were a problem for the UK because cybercriminals were fast to react to the processing systems changes. Within virtually no time, the criminals developed extremely innovative and effective techniques to commit fraud. This effect established a new era in cyber fraud including polymorphic fraud, which accelerated ever-changing threats—presenting new attacks and campaigns on a daily basis in a range of evolving forms including malware, remote-access Trojans (RATs) and account take-over.

Another major challenge was that many of the fraud detection and prevention solutions used in the UK were not sufficiently accurate. This resulted in a huge overload of work for back-end fraud teams, who were required to manually process the many false positive cases that these solutions returned. The new regulations allowed delaying only a limited number of transactions for further evaluation. This led to security teams lowering the sensitivity of their detection software to reduce the rate of alerts —which in turn allowed more fraud cases to slip by and a spike in online fraud.[4, 5]

This ability to commit the fraud and immediately cash out created a new era in online fraud—and called for a new paradigm in protection.

In this new era, what can be done to prevent online fraud?

Forced by the realities of this new era, financial institutions today are equipped with solutions that detect and alert on fraudulent transactions in real time as they are submitted—for the ability to enforce real-time prevention measures. But achieving high accuracy detection with minimal, manageable, alert rates is not trivial. Achieving that balance requires extensive understanding of cybercrime operation methodologies, as well as good data collection and analytics facilities. Factoring of multiple risk indicators, for example, can result in greater accuracy, which increases as more indicators are considered. Strategies such as observing transactions of anomalies alone or device fingerprinting alone would achieve a moderate detection rate—but with a too-high alert rate. The combination of these strategies will improve results but would still yield an alert rate that is too intensive to handle, keeping the fraud investigation team swamped with too many alerts and causing them to miss a considerable amount of fraud.

IBM® Security Trusteer® Pinpoint™ Detect offers a fundamentally different approach that can help financial organizations detect fraud while assisting in reducing false positives and the alert rate. The IBM approach to fraud detection is based on three core principles—visibility, a global threat intelligence network and agility by design.

Visibility

At the heart of Trusteer Pinpoint Detect is an engine that correlates a wide range of critical fraud indicators—including phishing attacks, malware infections, compromised credentials and advanced evasion methods—with enhanced device, geolocation and transactional modeling to help more accurately detect fraudulent activities.

Global threat intelligence network

In fighting fraud, the breadth, depth and speed of intelligence gathering are critical. The IBM global threat intelligence network analyzes threat intelligence from 270 million end-user endpoints as well as behavioral profiles, which are used to create dynamic digital models. The network is continuously processing security intelligence. Armed with this intelligence, Trusteer threat analysts, leveraging cutting-edge analytics technologies, research and investigate industry- as well as organization-specific threats. They can then adapt defenses with automatic updates without additional effort of the financial organization. Trusteer Pinpoint Detect leverages this unique intelligence, which includes a multitude of session attributes data and fraud indicators, to help more accurately identify fraud in immense data sets.

Agility by design

Time is a crucial element in cybercrime prevention, and Trusteer Pinpoint Detect has an agile architecture that enables a highly flexible and fast response process. Using cloud-based technologies, IBM can help rapidly detect, analyze, build and deploy countermeasures for new and emerging threats. Financial institutions can also receive application-aware defenses specifically tailored to their needs and the threats they face. This capability can help further increase detection accuracy, and is designed to help reduce operational costs.

Conclusion

The results of the UK implementation of faster payments and its online banking fraud implications present a distinct call to action to adapt legacy fraud detection tools and processes toward the upcoming new era. Trusteer Pinpoint Detect uses evidence-based indicators of fraud to offer a next-generation approach that helps address the challenges of traditional risk engines. By uniting the traditional risk score approach with an actionable indication that takes into account fraud data and deep knowledge of current strategies used by fraudsters, the Trusteer Pinpoint Detect service can provide a real-time, highly accurate and evidence-based answer, rather than the statistical answer other solutions use, on whether a transaction is fraudulent or not.

By combining Trusteer Pinpoint Detect with other Trusteer fraud prevention solutions, financial institutions can gain a comprehensive fraud prevention platform that delivers broad visibility across the threat landscape. Trusteer solutions provide real-time intelligence that dynamically adapts and automatically updates protection, without customer interaction.

For more information

To learn more about Trusteer Pinpoint Detect software, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/software/products/en/category/advanced-fraud-protection

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
July 2016

Please Recycle

[1] Claire Greene, Marc Rysman, Scott Schuh and Oz Shy, "Costs and Benefits of Building Faster Payment Systems: The U.K. Experience and Implications for the United States," *Federal Reserve Bank of Boston*, February 24, 2015. http://www.bankofcanada.ca/wp-content/uploads/2015/12/costs-benefits-building-faster-payment-systems.pdf

[2] "Same Day ACH: Moving Payments Faster," *NACHA*, April 9, 2016. https://resourcecenter.nacha.org/?q=node/47

[3] Tim Dalgleish, "Will Real-Time Online Banking Payments Increase Fraud by $25 million in Australia? (Part I)," *LinkedIn*, January 21, 2016. https://www.linkedin.com/pulse/real-time-online-banking-payments-increase-fraud-25-part-dalgleish

[4] Mary Ann Miller, "Faster payments means faster fraud," *Fintech Business*, December 07, 2015. http://www.fintechbusiness.com/blogs/89-faster-payments-means-faster-fraud

[5] Bailey Reutzel, "Lessons from the U.K.'s Colossal Payments Overhaul," *American Banker*, March 30, 2015. http://www.americanbanker.com/news/bank-technology/lessons-from-the-uks-colossal-payments-overhaul-1073417-1.html?zkPrintable=1&nopagination=1

WGW03237-USEN-00