Detecting digital identity fraud with IBM Trusteer
Contents

2 Introduction
2 Welcoming customers in while keeping fraudsters out
3 A seamless customer experience
4 Intelligence infused with cognitive technology and advanced analytics
5 Simplified lifecycle management
5 Conclusion
6 For more information

Introduction
The digital transformation is changing how customers interact with banks. Many key consumers, like millennials and high-net-worth clients, are seeking greater conveniences and new digital services—everything from the ability to apply for loans on smartphones to same day payments. To help meet customer demands, banks need to offer a seamless user experience across all devices—smartphones, PCs and tablets.

As you work to deliver digital services, you need to know that the “customer” logging in to your online or mobile banking app is who they say they are. However, you may face significant challenges in doing so. Cybercriminals are continually introducing new and increasingly sophisticated financial malware along with convincing social engineering tactics to impersonate banking customers.

Often, banks view the challenge as a balancing act, in which greater innovation can come with some sacrifice to security.

Instead security can be an enabler to the digital transformation—helping banks welcome customers in and keep fraudulent activity out so they can pursue new growth opportunities, improve the customer experience, and build customer loyalty.

In this whitepaper, you’ll learn how IBM® Trusteer® is offering digital identity fraud detection to help banks:

- Accelerate their digital banking transformation
- Detect sophisticated criminal activity at the outset of transactions
- Reduce security-related operational costs through simplified management

Welcoming customers in while keeping fraudsters out
Do you know if the “customer” logging in to your digital banking system is who they say they are?

It’s a challenging question, and banks often use numerous security layers—some transparent to the customer, some not—to answer it. But many banks, and their customers, have found the answers aren’t always right.

Sometimes legitimate transactions are held pending out-of-band verification from the customer, while fraudulent transactions conducted by cybercriminals using remote access tools can slip by unnoticed.
The cost of not getting it right can be high.

Incorrectly holding transactions can create serious customer satisfaction issues and erode brand loyalty. Conversely, missed fraud can have significant ramifications both in terms of fraud losses and brand reputation. A 2016 Ponemon Study, sponsored by IBM, found that financial institutions had a “higher than average rate of lost business and customers” from data breaches than other organizations.¹

IBM Trusteer is bringing together digital identity fraud detection capabilities, adaptive intelligence and cloud-based services to help financial institutions:

- More accurately assess user identities and anomalies
- Continually adapt protections
- Reduce operational costs

A seamless customer experience

If you think about it, not much has changed when it comes to customer expectations. In the past, customers expected easy, fast and convenient services at their local branch.

Long teller lines and the need to show multiple IDs were considered an imposition and could impact customer satisfaction and loyalty greatly.

Today, digital banking faces the same expectations. Onerous login processes with multiple authentication requirements and challenge questions can often be perceived as cumbersome as long lines, and customers can quickly become frustrated.

A seamless experience is one important key to the success of any digital banking initiative. In fact, the Information Security Media Group (ISMG), found that 99 percent of the 150 financial institutions it surveyed viewed preserving a seamless customer experience as a priority, with 63 percent saying it was a “top” priority.²

IBM Trusteer solutions are designed to transparently uncover relationships between customers and their digital identities, sessions and devices, and behaviors and transactions so you can more quickly and more accurately separate legitimate customers from the cybercriminals.

Using behavioral biometrics to build models based on patterns of mouse movements, IBM Trusteer can deliver identity-based authentication from login through the entire application flow.
With the ability to continuously and transparently learn user behavior across hundreds of millions of sessions, the platform can identify in real time either inconsistent user behavior or known fraudster behavior and provide an alert so action can be taken.

In addition, the platform uses cross-channel analytics on a wide-range of behavioral indicators, such as device use, geo-location, session length and transaction norms, to uncover inconsistencies in near-real time.

All of this occurs transparently, “under the covers,” so that you can identify and deny unauthorized activity across all devices and channels without adding burdensome authentication layers that can impede customer access and impact the customer experience. As a result, you can better focus on growing your business—across digital channels and geographies—and improving your net promoter score (NPS).

Using IBM® Trusteer® solutions, a financial service organization realized:

- 90% reduction in fraud costs
- 50% decrease in auditing and compliance preparation time
- 204% return on investment

Source: 2016 Forrester Total Economic Impact Study, Commissioned by IBM.

Intelligence infused with cognitive technology and advanced analytics

If you’re like most bank executives, you are likely excited by the chance to transform the way customers interact with your bank.

But while you’re working to transform digital banking, cybercriminals are transforming malware and social engineering attacks to better impersonate your customers.

The IBM Trusteer team brings together a decade of fraud expertise combined with advanced analytics and patented machine learning to help detect and prioritize new fraud patterns so you can focus on growing your business instead of monitoring the changing landscape.

For example, Trusteer security experts use an adaptive intelligence system that leverages advanced analytics and patented machine learning capabilities to analyze the millions of digital banking sessions that flow daily to its threat network.

The platform also uses advanced analytics and patented machine learning to analyze unstructured website data—including links, images, forms, text, scripts, DOM (document object model) data, URLs and more—to detect new phishing sites. The system can rapidly cull through millions of sessions at a speed and scale not previously possible to identify and alert IBM security researchers of web injections.
This information is combined with data from a variety of sources including:

- Intelligence gathered from millions of client endpoints worldwide
- World-renowned insights from IBM X-Force® Research
- A historical fraud behavioral index
- Real-time user behavior gathered through behavioral biometrics

The result: We’re able to identify and help you prioritize emerging threats and changes in the security landscape as they occur so you’re prepared.

**Simplified lifecycle management**

Your focus is on transforming your customers’ experience. It’s why an important element of our solution is helping you simplify management and reduce the operational hassles that all too often come with technology solutions.

Our advanced fraud detection capabilities provide actionable insights that can help your staff easily see which transactions to allow, which ones to restrict/request step-up authentication, and which ones require further investigation, and why. With fewer false positives to sift through, your team can spend less time chasing false alarms, and more time on innovation.

Comprehensive reporting and risk assessments are available to help you accelerate your risk and compliance modeling.

In fact, a 2016 Forrester Total Economic Impact study, commissioned by IBM, found that a financial services organization realized a 90 percent reduction in fraud costs, a 50 percent decrease in auditing and compliance preparation time, and a 204 percent return on investment (ROI) using Trusteer solutions.³

Finally, our cloud-based platform provides an agile architecture so that as IBM security researchers uncover new criminal behavior, they can rapidly adapt and deploy defenses—behind the scenes.

**Conclusion**

Many consumers are seeking greater conveniences and new services when it comes to digital banking that require you to raise the bar for speed and intuitive experiences.

However, to deliver exceptional digital services, you need the ability to seamlessly welcome customers in, while keeping fraudsters out.

The solution is no longer about finding the right balance between security and convenience. It’s about using security as an enabler to help you accelerate your digital transformation.

The digital identity fraud detection platform from IBM Trusteer is designed to help you more quickly, transparently and accurately confirm that the “customer” logging in to your digital banking system is who they say they are.

Using powerful behavioral biometrics and cross-channel behavioral analytics, the Trusteer platform provides identity-aware authentication to help you separate your customers from cybercriminals, and help you reduce false positives.

Intelligence infused with layers of cognitive technology and advanced analytics detects new malware and phishing attacks at a speed and scale like never before. As a result, you can focus on growing your business instead of monitoring the changing landscape.

And the platform’s cloud-based architecture and comprehensive reporting help reduce the time and cost associated with managing fraud protection and deploying new defenses.
For more information
To learn more about detecting digital identity fraud with IBM Trusteer, contact your IBM representative or IBM Business Partner, or visit the following website: ibm.com/security/trusteer

© Copyright IBM Corporation 2017
IBM Security Group
Route 100
Somers, NY 10589

Produced in the United States of America
June 2017

IBM, the IBM logo, ibm.com, Trusteer, and X-Force are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at ibm.com/legal/copytrade.shtml

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. It is the user’s responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.


Please Recycle

WGW03301-USEN-00