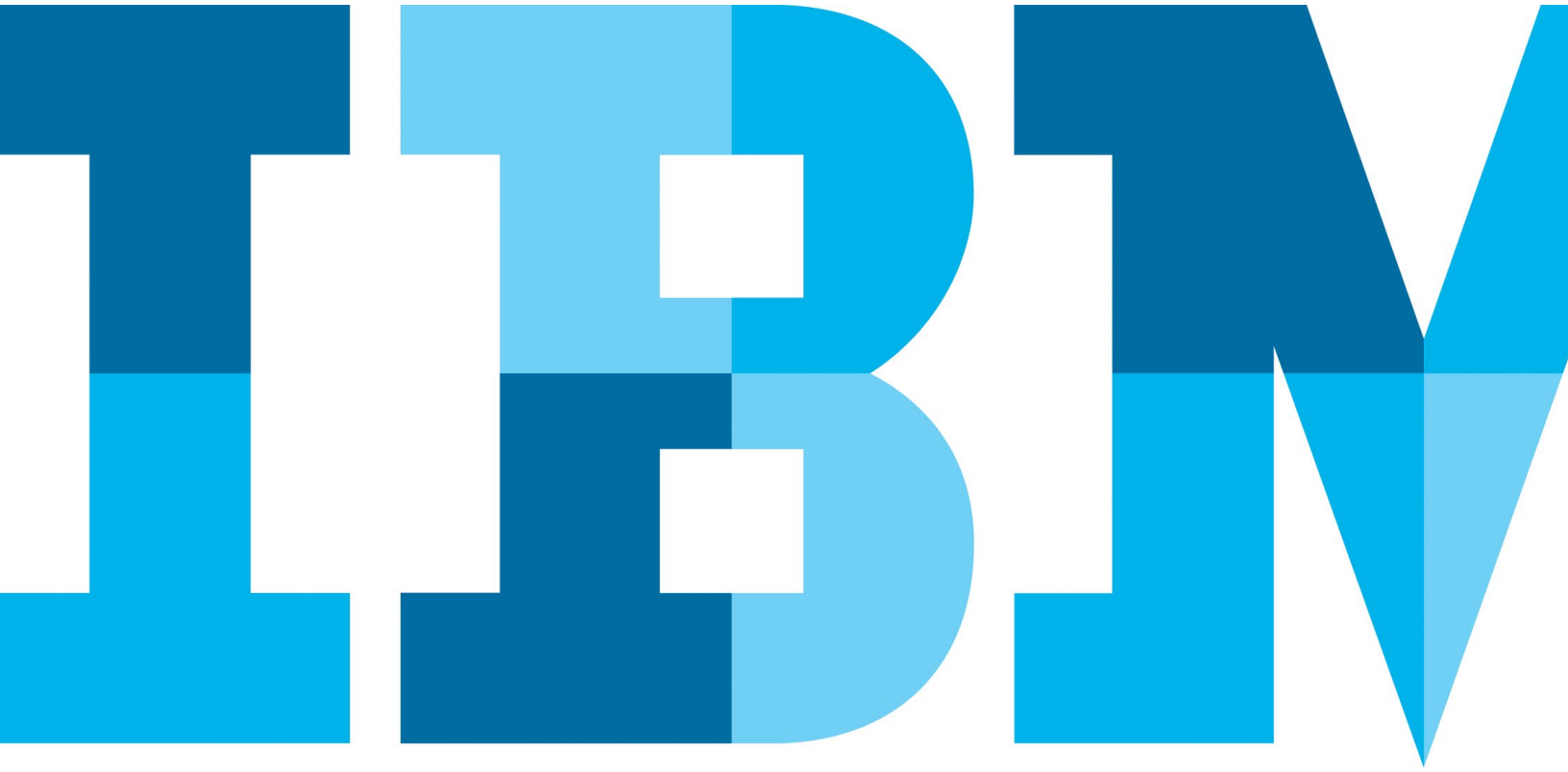
Security
White Paper

October 2017

Transparently detecting new account fraud

IBM Trusteer helps power digital transformations by seamlessly assessing the risk of new digital identities



IBM

Contents

Introduction

The digital transformation in financial services is well underway. New market entrants and traditional financial services companies alike are deploying digital services that enable digital-first consumers to open new accounts and apply for banking, insurance, payment and other financial services—either directly through their digital platform or through third-party application information and payment initiation service providers.

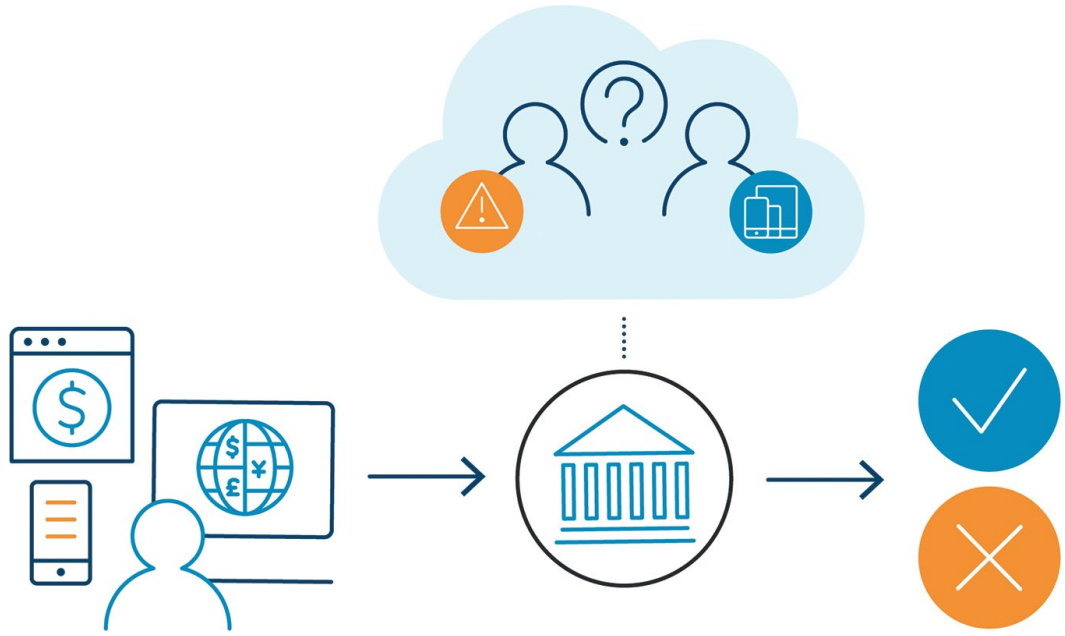
Consumers who have a digital-first appetite expect convenience, speed and security. But developing the kind of experience consumers expect can be challenging. Many factors can contribute to consumer abandonment of new account creation including app and process complexity. For example, lengthy account opening processes with multiple steps (either too many steps for authentication or too many forms to be submitted via a branch or digitally) can be perceived by new customers as onerous. Such processes can affect a customer's digital experience and the new account creation process. Ultimately, these processes may result in a high abandonment rate with consumers either turning to more expensive bank channels, such as the call center, for help or engaging with a competitor instead.

What happens when you need to validate a new customer? Without prior information or customer records, and when the information you may rely on is publicly available, it can be a challenging task to determine whether an account was created by a true user or by a cybercriminal. To help more accurately identify cybercriminals, organizations will need multilayered capabilities that look at the application from as many angles as possible—going beyond publicly available information and traditional sources to examine each user's digital footprints.

This whitepaper outlines the challenges organizations may face in detecting new account fraud and how the IBM® Trusteer® New Account Fraud solution can help organizations transparently assess the risk and predict fraud by assessing that a new account is being opened by an actual customer, and not a cybercriminal intent on defrauding the organization and its customers.

Identifying true customers versus cybercriminals

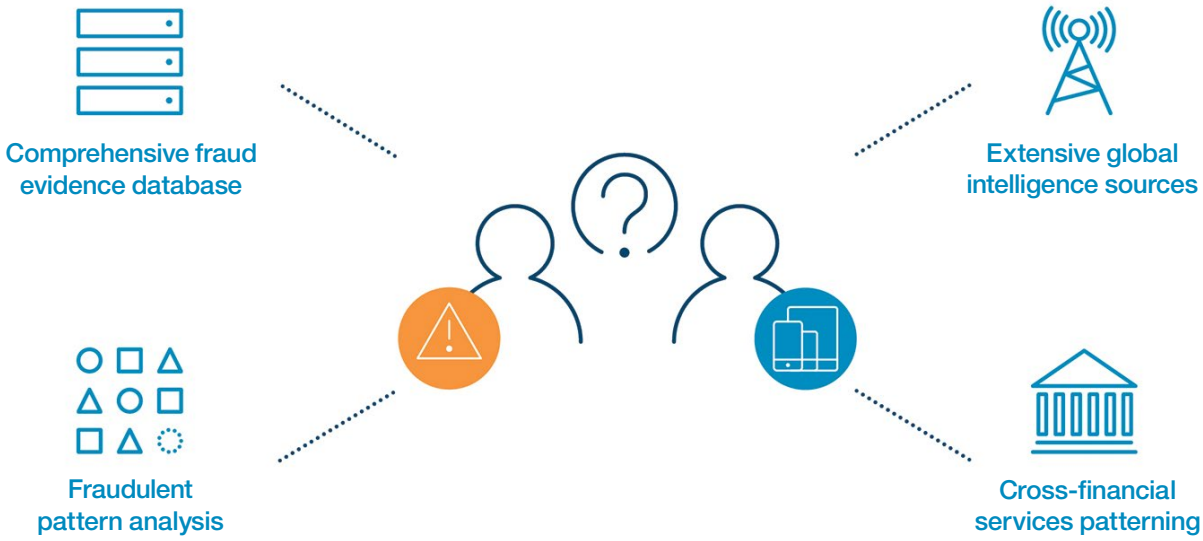
When it comes to verifying digital identities, identifying true customers versus cybercriminals can be a challenge. Cybercriminals have found many ways to create fake identities or use real but stolen identities to open either a brand-new account or a new digital account for an existing customer. They may create synthetic identities from stolen data or add false data to real identities. They may also impersonate existing customers to create new digital accounts on their behalf. Sometimes, they'll spend weeks and, even, months building credit for a fake identity to increase the amount of money they can steal.[1]



The ability to assess risk in real time during new account creation is vital in the new digital era for delivering the kind of customer experiences that will drive business growth.

Additionally, fraudsters have many ways to direct bank communications to themselves using methods such as SIM swap schemes or by porting phone numbers to a different mobile carrier and then registering the number to a new user. By doing so, they can obtain all the communication on behalf of the true user to bypass strong authentication and conduct new account fraud. In these sophisticated attacks, a fraudster, posing as a customer and using information gathered from the victim's social media accounts or background reports, can answer security questions and pass one-time-password (OTP) requests, all on behalf of a true user.

The main challenge across these threats is an organization's ability to assess the new account fraud risk and validate the authenticity of a user early in the account creation process. For both new and existing customers, expectations are high for a seamless process with minimum friction. While security checks are expected, they should be transparent, or at the very least cause minimal irritation. The more steps users must go through, the greater the likelihood that they'll abandon the digital process, and either contact the financial institution on a more expensive channel, such as the call center, or open a new account with a different institution.



The IBM Trusteer New Account Fraud solution can help organizations to understand, detect and predict the risk of fraudulent intent during the new digital account creation process by correlating rich proprietary insights with global intelligence sources.

So how do you spot a true customer from an imposter in the digital world?

The good news is that cybercriminals leave footprints for fraud experts that are markedly different than true customers. If you look closely, cybercriminals' new account applications may look different than true user applications. Small clues, such as the use of a pre-paid SIM card, the use of automated or industrial techniques to fill out digital forms, or even how a user browses the website or mobile app, can signal a pro at work rather than a true user who is just trying to open an account. And even when an application may appear to be legitimate, the ability to correlate one of the data points that was used with fraudulent activity performed on a different organization can detect that fraud is present.

Establishing trust over digital channels using worldwide intelligence

The IBM Trusteer New Account Fraud solution helps banks and financial organizations identify fraudsters' footprints and establish a trusted digital relationship using advanced intelligence and global visibility during new account creation. The IBM Trusteer New Account Fraud solution is integrated with IBM Trusteer Pinpoint™ Detect to allow organizations to transparently assess the risk, enabling a seamless digital account creation experience for customers. Correlating rich proprietary insights with global intelligence sources that provide an additional reputation view, the IBM Trusteer solution can help organizations to understand, detect and predict the risk of fraudulent intent during the new digital account creation process.

IBM Trusteer's advanced intelligence and global visibility span four key areas.

A comprehensive fraud evidence database

IBM Trusteer's automated fraudster detection uses a global criminal evidence database that includes insights into previously identified fraudster evidence and known fraudster evidence such as emails, phone numbers, device elements and mule accounts—all gathered based on security intelligence from hundreds of organizations worldwide.

Additionally, a compromised device can indicate an increased risk for cybercrime. As such, IBM Trusteer solutions incorporate SaaS analytics of device elements that may point to a compromised device. These elements include malware, Remote Access Trojans, jailbroken/rooted devices, SMS stealing apps and any evidence that may indicate that the device being used is not trustworthy.[2] IBM Trusteer solutions also create a device ID, which allows organizations to establish the trust between the device and the account that was just created.[3]

Extensive global intelligence sources

During the new account creation process, the IBM Trusteer New Account Fraud solution incorporates a wide range of intelligence sources to help verify information on the authenticity of the user's digital identity. This includes uncovering risk indicators such as:

- Location information (for example, risk and fraud indications regarding location, risky locations and location mismatches)
- User patterns versus known fraud patterns
- Fraud indications, such as identity elements previously correlated to fraud

These insights when correlated with Trusteer intelligence are used to help differentiate between legitimate and potential cybercriminal activity, early in the account origination process, to help reduce fraudulent activity.

Fraudulent pattern analysis

When it comes to new account opening, either a brand-new account or the opening of a new digital account for an existing user, different patterns emerge when examining the actions of cybercriminals and those of true customers. The IBM Trusteer solution uses machine learning to analyze a multitude of data elements to identify and incorporate these fraudulent patterns as part of the overall risk assessment.[4] The IBM Trusteer New Account Fraud solution, used along with IBM Trusteer Pinpoint Detect, also continually monitors new digital accounts to identify any new activity associated with fraud post-account creation, providing an early warning sign that a young account may be used as a mule account or to conduct fraud.

Some of the analyzed data elements include:

- Insights into the user journey, such as how long users spend on a page, how the form is filled out, how fast users type, and what the journey looks like—whether it matches true user behavior or may raise a suspicion that something may not be right.
- Identity linkages. Is the data being used in new account creation used in a different application and does it match a fraud pattern when looking at worldwide activity?

Cross-financial services patterning

Fraudsters often use the same tactics, or the same stolen or synthetic identity elements, as they open new accounts with different financial service providers. As a result, IBM Trusteer solutions analyze fraudulent patterns across financial service providers worldwide to identify and distinguish true customer patterns from fraudsters. With this global insight, IBM Trusteer can help organizations identify and detect if:

- The identity requesting to open the account has already attempted to open one or more accounts with other protected banks at a velocity and rate similar to known fraudster patterns
- The device, or the same identity elements, is requesting to open multiple accounts on behalf of different users
- The same phone number, email or address is used on multiple applications for different people

Remaining agile with adaptive intelligence

In recent years, identity theft and new account fraud has skyrocketed. Rarely a week goes by without news of another data breach in which cybercriminals make off with stolen data that can be used in creating synthetic identities or impersonating existing customers. IBM Trusteer enlists both advanced technologies and world-class security experts to track daily changes in the cybercrime landscape. The Trusteer security infrastructure continually incorporates new intelligence using the following:

- Machine learning capabilities, including layers of cognitive fraud detection and analytics, to understand, detect, and predict the risk of fraudulent attempts during new digital account creation
- Global, real-time threat intelligence and global insights delivered through the cloud
- Emerging patterns tracked by IBM X-Force®, one of the world's most experienced commercial security research teams

This adaptive intelligence provides a new dimension of insight. It helps organizations to quickly understand, detect and predict the risk of fraudulent attempts, protect against evolving cybercrime tactics, increase the accuracy of assessments and reduce operational costs—all while enabling a seamless digital account creation experience for customers.

Leveraging IBM Trusteer new account intelligence to build your own polices

Banks and other financial institutions often must deal with global and local business requirements, depending on the patterns of use that they encounter and according to each institution's sensitivity to risk. As a result, many fraud teams seek full control over the models they use when evaluating potential risk. The IBM Trusteer Pinpoint Detect policy manager provides organizations with visibility into models, control to adapt models, and flexibility to rapidly apply new countermeasures so they can build new account policies to address internal and external requirements and regulations. The policy manager uses machine learning to synthesize knowledge of current and emerging threats and trends that financial service providers face and provides the ability to customize new policies, simulate rules and adapt risk models automatically, or based on specific intelligence and insight—all without prerequisite knowledge or advanced skills.

Conclusion

What kind of digital experience does your organization want to deliver? If you're like most organizations, your focus is on providing convenience through your digital transformation and delivering the kind of customer experiences that will capture new market share and deliver high Net Promoter Scores (NPS)—a major indicator of customer satisfaction.

But lengthy authentication processes can undermine your efforts.

IBM Trusteer helps organizations transparently differentiate true users from cybercriminals by correlating a full range of risk indicators including the following:

- Known fraudster identification, identified fraudster devices, known fraudster behavior, and a variety of device elements, such as insight into malware, Remote Access Tools, jailbroken/rooted devices, SMS stealing apps and any evidence that may indicate that the device that is being used is not trustworthy
- Global intelligence sources that provide additional reputation insights
- Known new account fraudulent patterns based on the user's journey, location, spoofing indication and identity fraud indication
- Digital identity assessments that detect anomalous footprints and suspicious patterns (or intent)
- Cross-financial services patterning that analyzes fraudulent patterns across financial service providers

By combining these insights with adaptive intelligence and flexible policy management, IBM Trusteer solutions can help provide significant accuracy when it comes to determining the legitimacy of a new user, and, ultimately, help organizations deliver the transparent experience required to fuel the growth of digital services.

Recommended actions are provided in real time along with the detailed reasoning and session details to give your risk team a clear actionable plan. As a result, you can more easily, confidently and seamlessly let new customers in, while keeping fraudulent activity out.

For more information

To learn more about new account fraud, please contact your IBM representative or IBM Business Partner, or visit the following website:
ibm.com/us-en/marketplace/trusteer-new-account-fraud

New Orchard Road
Armonk, NY 10504

Produced in the United States of America
October 2017

Please Recycle

[1] Penny Crosman, "Identity Fraud: Back with a Vengeance, Harder to Stop," American Banker, June 9, 2016. https://www.americanbanker.com/news/identity-fraud-back-with-a-vengeance-harder-to-stop

[2] Capability provided separately with IBM Trusteer Pinpoint Detect and IBM Trusteer Mobile SDK.

[3] Capability provided separately with IBM Trusteer Pinpoint Detect and IBM Trusteer Mobile SDK.

[4] Capability provided by IBM Trusteer Pinpoint Detect.

WGW03333-USEN-00