Highlights

- Assess the risk of new digital identities
- Predict the risk of digital fraud early in the new account creation process
- Transparently detect new account fraud without impacting the customer experience

Seamlessly assess digital identities

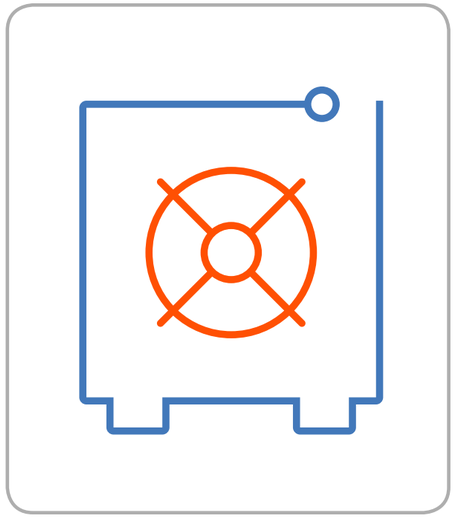
IBM Trusteer helps differentiate legitimate customers from fraudsters during digital account creation

In today's digital world, it can be harder than ever to know who's on the other end of a connection—especially when it comes to verifying new digital identities. The main challenge lies in the financial institution's ability to assess new account fraud risk and whether or not it has the means to validate the user's authenticity early in the account creation process.

But precautions can't hinder the end-user experience. A new account creation process that's long or difficult could mean that customers will choose to do business elsewhere.

What you need is a way to transparently confirm that a new account is being opened by an actual customer—and not a cybercriminal attempting to defraud your organization and customers. This way you can benefit from increased levels of trust all while delivering a banking experience that helps keep customers engaged.

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



▸ Read what one analyst thinks banks must do to take advantage of digital opportunities.

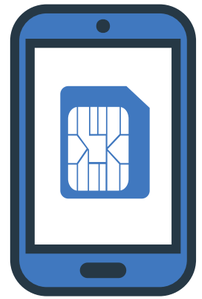
Assessing the risk of fraudulent intent in new digital accounts

To support a streamlined user experience, banks may choose to enable high-risk activities. The goal is to increase satisfaction with the bank's services. But danger lurks in the ability of fraudsters to alter existing user or device information to exploit accounts. Some common scenarios include:

False and synthetic identities: Fraudsters know that when a bank allows prospective customers to easily open accounts, it is opening its doors to virtually anyone, including fraudsters who simply create an account using stolen or synthetic identities. Once created, the new account can be used immediately to conduct fraud. In assessing the risk of new users, financial institutions must be able to identify threats before they cause damage. They need to transparently assess the risk while giving customers a seamless digital account creation experience.

Stolen or spoofed devices: Much as fraudsters can open a new account using a fraudulent identity, they can also access an existing account with a fraudulent device—one that is stolen or modified to impersonate a legitimate device. In opening an account, however, a fraudster leaves a different digital footprint than a legitimate user—and this footprint can be traced using advanced analytics and machine learning technology. Examining multiple sources of data, including the user's device, specific session information and behavioral-biometric patterns, can help detect evidence of malicious intent.

SIM swapping: In this scam, a fraudster contacts a mobile carrier using a stolen identity and falsely reports a stolen or lost device. The carrier then cancels the old SIM card and provides a replacement—which, when inserted into a new device, can be used to receive SMS messages and phone calls, including those sent by the bank, to gain access to banking assets. The challenge is to verify that a request originated from a legitimate customer and not from a fraudster attempting to impersonate a real customer. To do that, organizations need insights into potentially unusual/suspicious activities and requests that indicate potential high-risk activities.



2,658

SIM-swapping reports were filed with the US Federal Trade Commission in January 2016—double the number for the same time in 2015.[1]

Learn more about how IBM Trusteer can seamlessly identify genuine users and detect criminal intent.

1 Carmen Chai, "SIM-swapping scam lets fraudsters drain your accounts," *creditcards.com,* October 25, 2016.

Establishing trust over digital channels using worldwide intelligence

When it comes to financial fraud, both the institution and its customers face significant loss. The cost of a data breach in the financial sector, in fact, is 173 percent the mean cost for all industries.[1] Victims of a SIM-swap scam can not only have their personal accounts drained, but they also can find that fraudsters have applied for and received large bank loans in their name.[2]

Combating such attacks can be a difficult task. For example, banks that use publicly available databases to verify the identity of potential customers they have never encountered before—but who are legitimately attempting to open a digital account—are potentially using resources that are also available to fraudsters. The use of public databases, however, can open the door for fraudsters to pose as real customers. The overarching challenge, therefore, lies in seamlessly establishing trust over the digital channel between banks and potential customers without the banks' already having information or customer records—and seamlessly separating legitimate customer activity from cybercriminal intent early in the new digital account creation process.

To establish this necessary trust, IBM Trusteer solutions help banks and financial institutions identify fraudulent footprints using advanced intelligence and global visibility early in the new digital account creation. IBM Trusteer New Account Fraud correlates rich proprietary insights with global mobile carrier intelligence to create an additional reputation view. The information helps organizations understand, detect and predict the risk of fraudulent intent during new digital account creation. By enabling organizations to transparently assess the risk, IBM Trusteer enables a seamless digital account creation experience for their customers.

The advanced intelligence and global visibility capabilities provided by IBM Trusteer span four key areas:

- A comprehensive fraudster database
- Extensive global mobile carrier intelligence
- Fraudulent pattern analysis
- Cross-financial services patterning

12x

Popularity of Bank of America's mobile banking applications over its branch locations.[3]

Read the IBM white paper to learn how IBM Trusteer powers digital transformation by seamlessly assessing the risk of new identities.

1 "2017 Cost of Data Breach Study: Global Overview," *Ponemon Institute,* July 2017.

2 Miles Brignall, "Sim-swap fraud claims another mobile banking victim," *The Guardian,* UK, April 16, 2016.

3 "How Digital Investments Are Changing the Face of Banking," *The Financial Brand,* July 27, 2016.

Globally identifying patterns of fraudulent activity is key

A comprehensive fraudster database

IBM Trusteer automated fraudster tagging capabilities leverage security intelligence gathered from hundreds of organizations worldwide and compiled into a global criminal database. This resource includes insights into previously identified fraudster devices, known fraudster behavior, email-related information, phone numbers and mule account data.

Financial institutions deploying the IBM Trusteer New Account Fraud solution can use advanced intelligence and global visibility to identify fraudsters' footprints during new account creation—laying the groundwork for a trusted digital relationship with customers.

By correlating this insight with additional attributes, IBM Trusteer can help organizations determine whether:

- The device belongs to a known cybercriminal
- The device is requesting to open multiple accounts on behalf of different users
- The same phone number and address are used on multiple applications for different people

Extensive global mobile carrier intelligence

In order to validate information on device ownership and validate the authenticity of the user's digital identity, IBM Trusteer New Account Fraud incorporates a wide range of mobile carrier intelligence during the new account creation process. This includes uncovering risk indicators such as:

- Location information mismatches (for example, a device that is registered in one country but is being used in another without roaming)
- High-risk locations known for cybercrime activity
- Device and registration inconsistences
- Frequent carrier changes and updates compared to the user's history

To help reduce fraudulent activity, these insights can be used to differentiate between legitimate and potential cybercriminal activity early in the digital account origination process.

USD8 billion

Predicted US losses from new account fraud and account takeover in 2018.[1]

Learn more about detecting new account fraud in this IBM white paper.

1 Kevin Woodard, "The $8 Billion Problem," *Digital Transactions,* February 1, 2016.

Insights into how fraudsters operate are critical to prevention

Fraudulent patterns analysis

In opening either a new account for a new user or new digital account for an existing user, the actions of cybercriminals and legitimate customers follow different patterns. IBM Trusteer solutions use machine learning and advanced analytics to detect and identify fraudulent patterns including:

- Insights into the user journey, such as how long users spend on a page, whether they copy and paste information into the application or type it in, how fast they type, and what errors they make when entering information
- The speed at which the applicant completes the application

Cross-financial services patterning

Fraudsters often use the same tactics again and again as they attempt to open new accounts with different financial institutions. Recognizing this, IBM Trusteer solutions analyze patterns of activity across financial institutions worldwide to identify the patterns of true customers and fraudsters, and to distinguish them from one another.

Using this global insight, IBM Trusteer can help organizations identify and detect whether:

- The identity attempting to open an account has already attempted to open one or more accounts exhibiting known fraudulent patterns with other protected banks
- The device is requesting to open multiple accounts on behalf of different users
- The same phone number and/or address are used on multiple applications

17%

of users guard their accounts with the password “123456.”[1]

Watch the IBM video to see how behavioral biometrics identifies fraudulent patterns to help banks understand how users interact with banking websites.

1 Paul Gillin, “Two-Factor Authentication: A Little Goes a Long Way,” *SecurityIntelligence,* January 30, 2017.

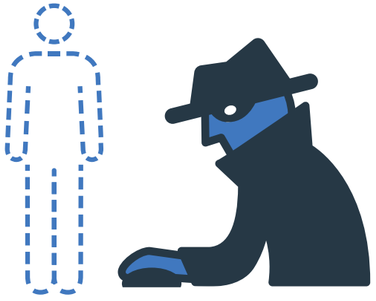
Make “trust but verify” your approach to banking security

As threats become more frequent and sophisticated, new technologies such as behavioral biometrics—which can help identify anomalies in users’ behavior—have the potential to replace passwords and enable organizations to better protect themselves and their customers’ assets.

However, while legitimate users can prove their digital identities, the fraudsters who compromise credentials also can make themselves appear legitimate. Lacking information or customer records, and relying on publicly available information, financial institutions may find it difficult to determine whether an account is being created by a legitimate customer or by a cybercriminal.

The challenge is compounded by the fact that organizations must meet three simultaneous needs—establish basic trust with customers over digital channels, differentiate between legitimate and fraudulent activity, and continually introduce new services and innovative offerings to capture new market share.

IBM Trusteer New Account Fraud addresses the challenges associated with verifying digital identities and separating legitimate customers from cybercriminals. By correlating rich proprietary insights with global mobile carrier intelligence to provide an additional reputation view, the solution can help detect and predict the risk of fraudulent intent throughout the digital journey. This allows organizations to gain the transparency required when assessing fraud risk, while also enabling a seamless digital account creation experience for their customers.



15.4+ million

US consumers were the victims of identity theft in 2016.[1]

Learn how IBM Trusteer can help to seamlessly assess the risk of new digital identities.

1 Bob Sullivan, “Identity theft hit an all-time high in 2016,” *USAToday,* February 6, 2017.

Why IBM?

Rarely a week goes by without news of yet another data breach in which cybercriminals have made off with stolen data. In the UK, for example, a recent report on cyber breaches found that 65 percent of "large UK firms detected a cybersecurity breach or attack in the past year."[1] In the US, malicious hackers hit the financial services sector more often than any other business segment during 2016.[2]

IBM Trusteer fraud protection solutions help protect many of the world's largest and leading financial service providers against digital identity fraud by detecting sophisticated criminal activity. IBM Trusteer solutions help prevent theft right from the start of a transaction using data analytics and security expertise.

IBM Trusteer combines cognitive and advanced intelligence with human expertise to enable more accurate insights into the threat landscape, so banks and financial institutions can spend less time investigating false positives and more time developing the kind of customer experiences that raise their Net Promoter Score.

With IBM Trusteer, banks and financial institutions can let the right customers in and keep fraudulent activity out. As a result, they can deliver the seamless and intuitive customer experiences that power customer-centric growth opportunities promised by digital transformation.

IBM Trusteer enables seamless yet more secure customer experiences by:

- Learning how customers interact with bank applications and websites
- Finding and restricting subtle, unauthorized activity
- Using biometrics to allow users access
- Protecting across digital devices and channels

IBM Trusteer provides significant operational value via simplified lifecycle management using:

- Real-time fraud detection and protection
- Accurate, actionable insights that minimize false positives
- A human team of IBM Trusteer researchers that constantly, proactively adds new layers of protection against emerging threats

Navigating the era of digital banking amidst constant change can be challenging

▸ This video shows how IBM Trusteer uncovers new threats with cognitive fraud detection.

▸ Learn more about IBM Trusteer New Account Fraud on the web.

1 "The cyber threat to UK business: 2016/2017 Report," *National Cyber Security Centre and National Crime Agency,* 2017.

2 "IBM X-Force Threat Intelligence Index 2017," *IBM X-Force®,* March 2017.

For more information

To learn more about IBM Trusteer New Account Fraud and IBM Trusteer Pinpoint Detect, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/us-en/marketplace/trusteer-new-account-fraud

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 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.

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: **ibm.com**/financing

IBM Security
New Orchard Rd
Armonk, NY 10504

Produced in the United States of America
October 2017

WGS03115-USEN-00