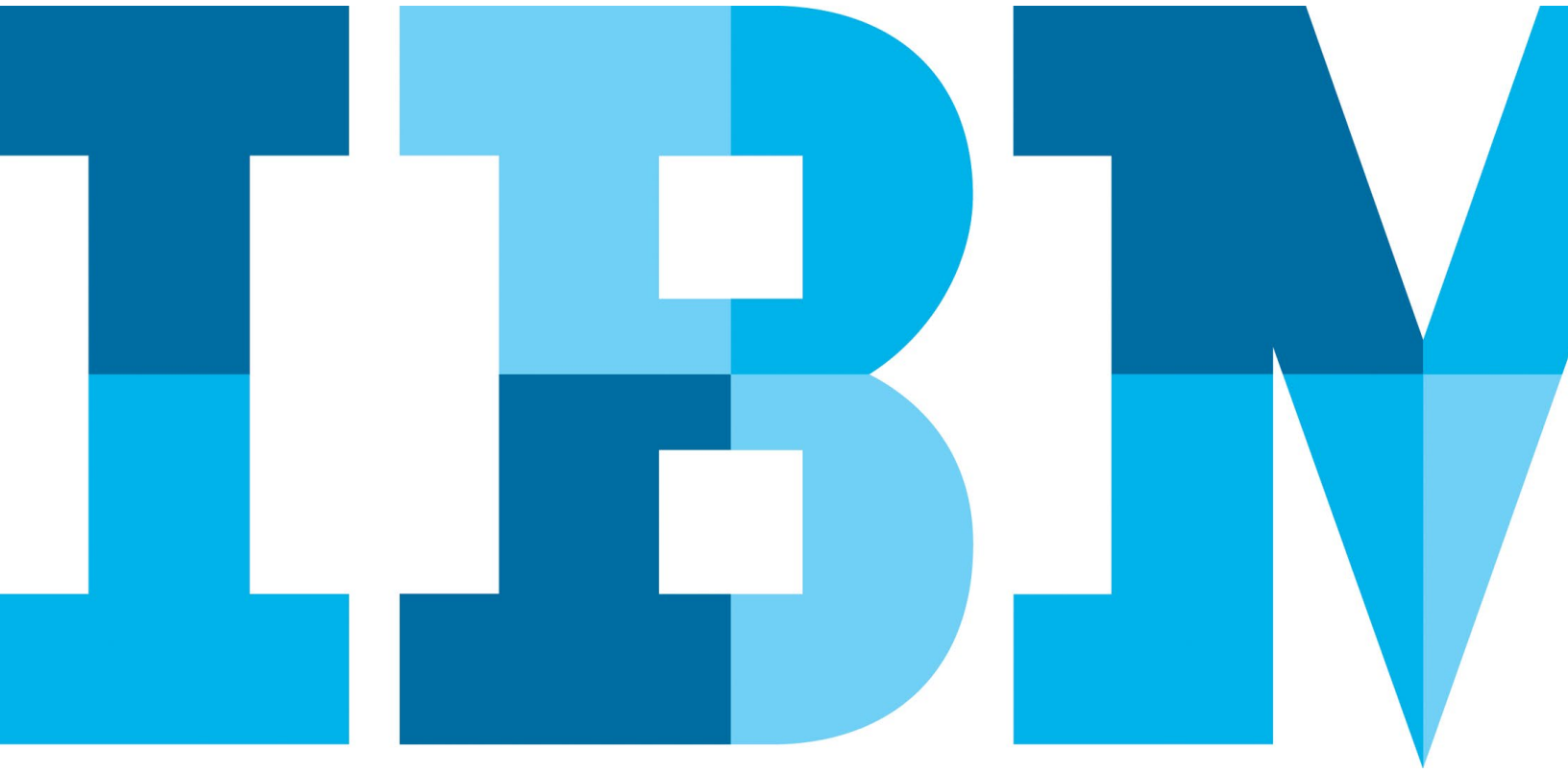
Security
White Paper

February 2018

Uncovering the value of digital identity fraud detection



IBM

Contents

Introduction

If your bank is like most, you've invested heavily in digital services to better connect with customers and pursue new growth opportunities. And as more customers use your online or mobile banking apps to conduct transactions and even apply for loans, you face greater pressure to confirm that the person logging in is who they say they are without arduous authentication requirements.

Digital identity fraud detection has emerged in recent years as an essential component in helping banks more transparently distinguish true customers from potential cybercriminals while pursuing digital initiatives.

But, as with any technology, you'll likely need to present a business case to gain approval for your investment. What factors should you consider in making your business case? Based on extensive discussions with financial institutions IBM has worked with, we've identified three influential factors to consider in the digital age.

Customer experience takes precedence

In the past, business cases for fraud prevention technologies were typically based on savings related to fraud management and compliance costs. While these factors may remain of interest, we believe that understanding the impact on the customer experience and related operational costs takes precedence.

Many institutions have found that transparency is key when it comes to digital security. For both new and existing customers, expectations are high for a seamless process with minimal friction. The more steps users must go through to access services, open new accounts, and conduct transactions, the greater the likelihood that they'll turn to another provider that offers a more convenient experience or to higher-cost channels, including going to a branch or contacting the call center.

As a result, we recommend evaluating the value of digital identity fraud detection based on the following three areas:

- Potential Net Promotor Score (NPS) improvement
- Potential fraud loss reduction
- Potential reduction in operational costs, such as reductions in password reset calls to customer call centers and other manual interactions that result in multiple touchpoints and handle time

Let's take a look at each area.

The effect on Net Promoter Scores

Net Promoter Scores (NPS) have long been used as a major predictive indicator of customers' loyalty to a brand and, thus, their business potential.

NPS is calculated using the following three groups of categorizations for customers:

1. Promoters. People who like the brand, who recommend or "promote" it to a friend, and who will use the brand services given an opportunity.

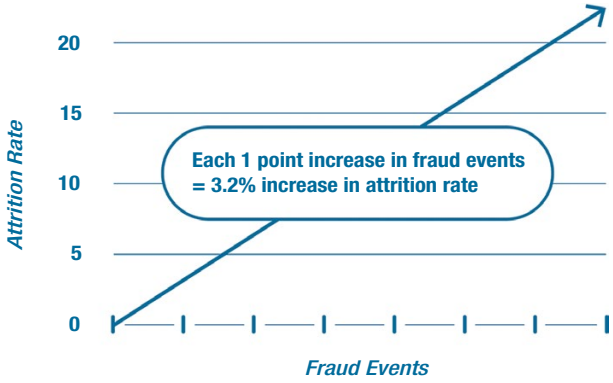
2. Detractors. Individuals who do not like the brand and would deter a friend from using the brand. Detractors will use the brand services only on scarce occasions.

3. Neutrals. These individuals are neither Promoters nor Detractors.

It's not surprising to find customers that move from Detractor to Neutral status, or from Neutral to Promoter status, in NPS based on improvements to the user experience for a brand's services.

As a result, intuitive customer experiences that integrate seamless security can help raise your NPS score. The less friction you can create digitally, the quicker the customer will be able to find or access the products and services they need. This can occur when step-up authentication, such as SMS one-time passwords (OTPs) and knowledge-based questions, are not required, thanks to the ability to seamlessly establish a trusted digital relationship.

On the flip side, the complexity of processes—either too many authentication steps or too many forms to be submitted digitally to verify identities—can be perceived by consumers as burdensome, and may result in lower customer satisfaction and less likelihood for the consumer to recommend your products and services to others.



Source: Security, Fraudulent transactions and Customer Loyalty: A Field Study," Rahul Telang and Sriram Somanchi, Carnegie Mellon University. October 2016. https://www.ftc.gov/system/files/documents/public_comments/2016/10/00062-129181.pdf

The potential reduction in fraud losses

The potential reduction in fraud losses remains a standard measurement in fraud detection business cases. However, what's new is the focus on understanding the cost of fraud losses when it comes not only to online account takeovers, but also to new account fraud and cross-channel fraud.

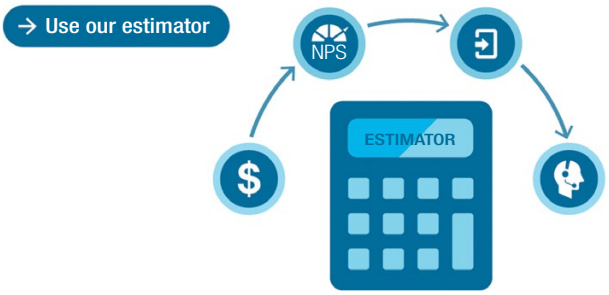
In evaluating digital identity fraud detection solutions, accuracy is an important selection criteria in helping reduce fraud losses. More accurate detection can reduce risks and, thus, help create an environment that enables you to seamlessly welcome customers in, while keeping fraudulent activity out. Additionally, the less time you spend investigating false threats, the more time you have to spend on catching real fraud and avoiding revenue losses.

Research shows that a client who experienced fraud (even when eventually reimbursed) is more likely to leave the brand. According to Professor Rahul Telang of Carnegie Mellon University's Heinz College, each point increase in fraud events increase attrition rate by 3.2 percent.[1] Thus, fraud can hurt your bottom line twice—once with the direct fraud loss, and once with the loss of the client's lifetime value.

Capabilities that can contribute to improved fraud detection include:

- Use of cognitive technology with passive authentication functionality to assess user identities—for both new applicants and existing customers—without burdensome stepped-up authentication layers
- Use of advanced analytics and machine learning to uncover new fraud trends and update fraud prevention controls continually
- Actionable real-time risk assessments and protection against digital account takeovers, new account fraud, and cross-channel fraud

How much can you save with digital identity protection?



The potential operational impact

How many calls has your call center staff received in the last 12 months to reset client passwords? How many cases can you remove from your fraud analysts' queue with improved detection?

Advancements in digital identity fraud detection don't just help you reduce losses, they can also help improve operational efficiency and simplify lifecycle management. Fewer authentication challenges helps reduce password lockouts and lowers the number of password reset calls to your call center. This allows for more effective use of analysts' time that can help deliver savings to your organization's bottom line.

As a result, the potential impact on operational efficiency has become a prominent proof point in many organization's business cases.

How IBM Trusteer can help you improve your business case

When it comes to digital banking, many consumers are seeking greater conveniences and new services that require you to raise the bar for speed and intuitive experiences. 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 so you can deliver the seamless customer experience that powers growth in the digital age.

How can our platform help you reduce your total fraud losses, improve operational efficiencies, and increase brand loyalty?

- Our powerful behavioral biometrics and cross-channel behavioral analytics provide identity-aware authentication, designed to help you more accurately and transparently distinguish true customers from cybercriminals.
- Layering advanced threat intelligence with rich insights into the threat landscape, our solutions deliver real-time fraud detection and protection against digital account takeover, new account fraud, and cross-channel fraud.
- Cognitive technology and advanced analytics help our researchers detect new threats.
- And an agile, cloud-based architecture enables IBM security researchers to rapidly adapt and deploy defenses—behind the scenes—as they uncover new criminal behavior.

Estimate your potential improvements

Every financial institution is different. To help you estimate the potential value you can realize using the IBM Trusteer platform, we've created a digital identity value estimator.[2]

With the estimator, you simply enter four values for your organization:

- Yearly total fraud losses
- NPS effect confidence (low, medium, high or very high)
- Average number of daily account logins
- Number of inbound call center calls

Using an advanced formula based on client engagements around the world, our estimator provides you with insight into:

- How many of your customers can potentially experience a frictionless customer experience, based on more accurate detection
- Your potential reduction in fraud losses
- And what the potential opportunity for cost savings is based on a reduction of call center customer password resets alone

The estimator offers a three-year window into the effect on these three perspectives so you can demonstrate the long-term value when making your business case.

For more information

To learn more about the value of digital identity fraud detection, please contact your IBM representative or IBM Business Partner, or visit the following website: **ibm.com**/security/trusteer

To use our digital identity value estimator to see how much you can save with the IBM Trusteer digital identity platform, visit: digitalidentityvalue.mybluemix.net

[1] "How likely are fraud victims to leave their bank?" American Banker Podcast, February 27, 2017. https://www.americanbanker.com/podcast/how-likely-are-fraud-victims-to-leave-their-bank. To review the full study, "Security, Fraudulent transactions and Customer Loyalty: A Field Study," developed by Rahul Telang and Sriram Somanchi of Carnegie Mellon University, visit: https://www.ftc.gov/system/files/documents/public_comments/2016/10/00062-129181.pdf

[2] The IBM Trusteer Digital Identity Value Estimator estimates potential improvements over three years with use of IBM Trusteer Pinpoint Detect™, IBM Trusteer Rapport®, and IBM Trusteer Mobile SDK.

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
February 2018

WGW03352-USEN-00