Know the real me: Building a circle of digital identity trust

How truly knowing your customers can lead to stronger relationships and greater security

IBM

Contents

01 Know your customers

02 Consider your challenges

03 Understand your opportunities

04 Determine what you want

05 Learn the solution

06 Transform your knowledge into action

Get started >

View the online version

“As a fashion forward designer, I search for unique fabrics. As a committed conservationist, I insist they be eco-friendly.”

You know your customers

You have always cared deeply about them.

You worked hard to introduce the digital services and tools they demanded to interact with you easily—whenever they wanted, wherever they were. You put extraordinary effort into providing them with the security and assurance they needed to trust you unquestioningly regardless of the channel they used.

So when your customers complained that your current authentication methods were frustrating and that strict security measures were hindering their digital experiences, you listened. And you realized they were right. Now, it's time to do something about it.

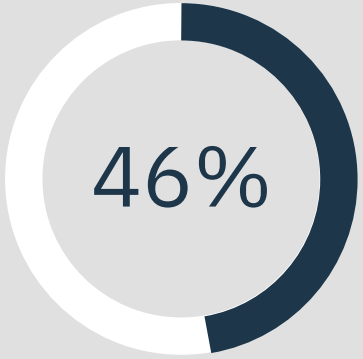
It's time to let your customers know that you know what they want, understand how they feel, and are dedicating yourself to making the relationship work. Not just for you. But for them.

The high cost of mistrust

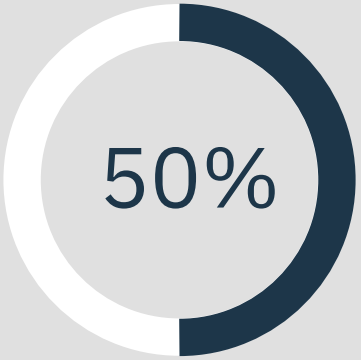
Sometimes when our goal is to protect, an abundance of caution can conflict with convenience. Security can impede satisfaction. Your customers want assurance that strong security is in place, but they don't want to think that they're the ones under scrutiny. They need to believe that as much as they trust you, you trust them in return. They want to know that you actually know who they are.

It's when customers feel that they're being treated like the criminals you're trying to circumvent that the relationship begins to corrode. Out of sheer frustration, they might shift to more costly channels, such as call centers or customer service desks. Even worse, they might abandon you all together, potentially resulting in diminished digital growth and sales opportunities, and financial loss. As their attitudes and behaviors continue to deteriorate, customer loyalty can suffer, and ultimately your bottom line can be affected.

You're both in agreement: there's room for improvement



In a recent study conducted by Javelin, 46 percent believe their fraud processes may inconvenience legitimate applicants for new accounts[1]



Only 50 percent of consumers believe that mobile banking is secure[1]


“As a busy entrepreneur, I haven’t a moment to waste. As Olivia’s daddy, I’ve got time to read Clifford the Big Red Dog *five times in a row.”*

Consider your challenges

In a recent Javelin poll, it was revealed that cross account takeover tripled from 2014 to 2017.[1] Much of this growth can be attributed to fraudsters who compromise email or mobile phone accounts, and then use one-time passwords as step-up authentication for high risk events.

As financial institutions struggle to prevent this misuse of accounts from occurring, they create authentication systems that impede their actual customers. Currently, 1 in 5 authentication attempts fail.[1] And, 13 percent of financial organizations surveyed reported a failure rate of over 40 percent.[1] That's substantially higher than the average failure rate of 22.8 percent across all businesses surveyed.[1]

Compare this to the entrenched consumer expectations established by leaders like Amazon. Click one button and whatever it is you desire will arrive on your doorstep tomorrow.

Which will you choose: protection or connection?

If you're like many of the participants in the Javelin study, you're grappling with an organizational dilemma. What do you do? Increase security measures to ward off the legion of fraudsters who become more and more sophisticated each day? Or offer your customers a hassle-free experience that solidifies your relationship?

The answer is: you do both.

Currently, 1 in 5 authentication attempts fail.[1] And, 13 percent of financial organizations report a failure rate of over 40 percent.[1] That's substantially higher than the average failure rate of 22.8 percent across all businesses.[1]

How do you establish digital identity trust throughout the customer journey while protecting their accounts?

Customer desires

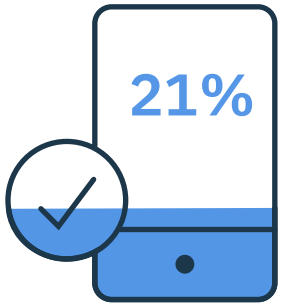
- Reduce risk inherent in digital channels
- Ensure customers perceive a secure environment

Industry needs

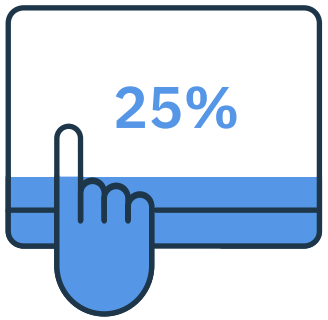
- Provide new, user-friendly digital capabilities
- Invest in digital identity trust
- Remain competitive
- Grow the business

According to the Javelin study, organizations in the financial services industry know it's time to...

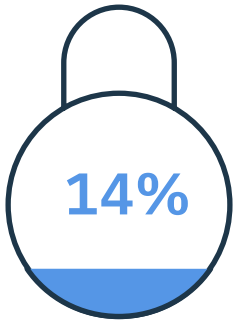
Reduce the friction of authentication of existing customers [2]



Improve the digital/ user experience [2]



Bolster the security of existing customer accounts [2]



Understand your opportunities

You might believe that you need to choose between two possible outcomes: protecting the security of your customer data, or providing a frictionless user experience. You've got some great news coming.

Innovations in technology, like AI, machine learning and behavioral biometrics, now make it possible for you to help safeguard customers from fraud and still provide the ease of use that can help you grow your digital business. You can finally address the demands of your CSO and CFO while supporting your CMO's efforts.

With the proper approach you can take steps to:

Improve the user experience

- Create a seamless customer experience across the digital lifecycle
- Maintain relationships with existing customers
- Attract new customers to digital channels
- Increase adoption and retention of new digital offerings
- Reduce digital abandonment

Protect your customers and your brand

- Provide security assurance without hampering the user experience
- Protect against attacks of a growing legion of sophisticated fraudsters
- Keep pace with evolving techniques for fraud

Improve the bottom line

- Increase digital sales and grow the business
- Diminish the use of more costly channels such as call centers
- Mitigate risk and fraud loss


“As a grandfather, I want to give him the moon. As an astrophysicist, I hope to explain the stars.”

Determine what you want

Before you determine how you'll take advantage of the many opportunities that lie ahead, you'll want to assess your own organization's needs. Define the current conflict between your authentication and verification processes and the complexity encountered by your users. Your goal is security and simplicity.

If your organization is like most others, you've already realized that this is an area for concern. A 2018 Javelin study revealed that only 52 percent of financial services organizations surveyed are confident that their fraud mitigation processes are effectively identifying fraudulent applicants.[2]

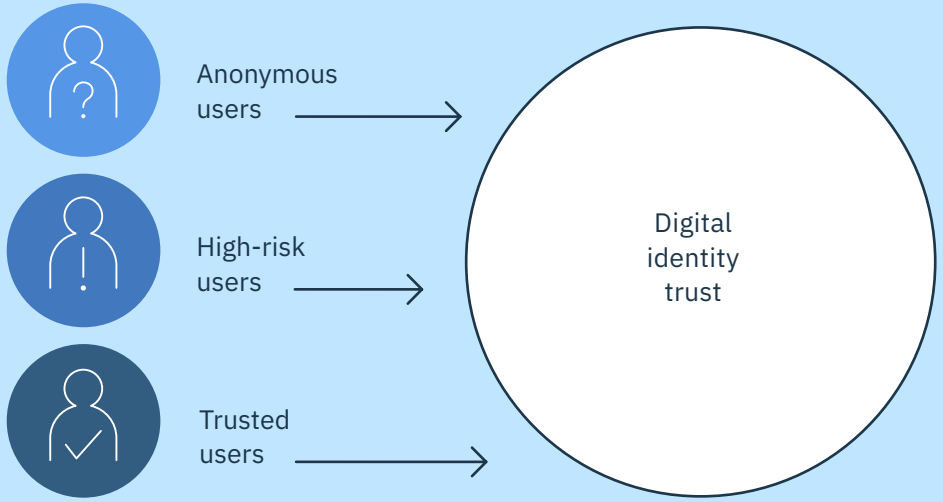
Based on the results of the Javelin study, there appears to be little doubt that digital identity trust is a pressing organizational priority. But how, exactly, do you achieve it?

How do you...

- Provide solutions that meet your specific organization's needs?
- Ensure the solutions you onboard fit existing processes and solutions?
- Manage all the complexities and evolving landscapes?
- Achieve stakeholder buy-in?
- Select the solutions that will take you into the future?

The answer is that you need to establish a circle of digital identity trust.

Establish a circle of digital identity trust



Who do you let into your circle of digital trust? And how?

Determine what you want

Knowing who to trust

A circle of digital identity trust can help transform new and anonymous users into trusted, loyal customers. It helps you offer those people who want the convenience of mobile access anytime, anywhere will enjoy a frictionless experience as they build and earn your trust.

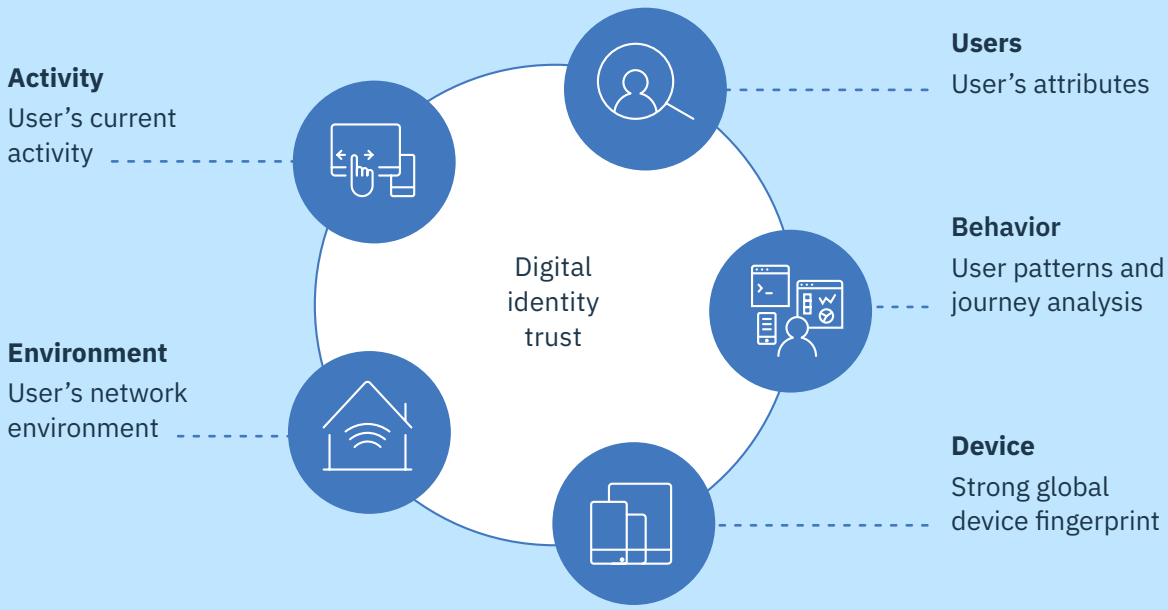
There are 3 steps to establishing this circle of digital identity trust:

1. Establish trust: New accounts/ anonymous users
2. Sustain trust: Trusted/existing users
3. Confirm trust: High-risk users

Building trust requires learning and ultimately knowing about the user, their device, specific activity, their technical environment, as well as their patterns of behavior.

With the advent of new technologies and analytics, this level of knowledge is now possible.

Digital trust begins with context



"Laying a strong foundation in robust fraud management strategy can free up resources to focus on other aspects of building relationships with customers."

—Javelin
Preserving Trust in Digital Financial Services: The role of identity and authentication [1]

"It's about the customer. It's about security. It's about the future."

—ISMG
2018 Digital Trust Survey [2]

"Technology investment need not mean greater complexity. Smart investments, in fact, can make the entire process far easier for the customer – and more secure for the enterprise."

—ISMG
2018 Digital Trust Survey [2]

"...users demand streamlined experiences, in which fraud mitigation tools do not interfere with the tasks they are performing."

—Javelin
Trust in Digital Financial Services: The role of identity and authentication [1]

Learn the solution

IBM Trusteer helps organizations seamlessly establish digital identity trust across the omnichannel customer journey. Through cloud-based intelligence, backed by AI and machine learning, Trusteer provides a holistic platform designed to help you welcome new and existing customers, while keeping bad actors out. Organizations are enabled with the ability to establish a trusted, frictionless digital relationship quickly and transparently.

IBM Trusteer offers a complete platform to help you achieve the following goals:

- Meet customer expectations through a seamless user experience
- Customer satisfaction to help promote greater retention
- Secure engagement
- Reduced fraud losses
- Lower operational costs
- Achieve operational efficiencies
- Enjoy continued business growth

Remove authentication roadblocks with the Trusteer Pinpoint platform

Now you can provide secure customer interactions without compromising a seamless digital experience. The IBM Trusteer Pinpoint platform includes customer-friendly services that provide a frictionless journey throughout the customer lifecycle: IBM Trusteer Pinpoint Assure, IBM Trusteer Pinpoint Detect and IBM Trusteer Pinpoint Verify.

3 steps to establishing a circle of digital identity trust

1. Establish trust: New accounts/ anonymous users — **Pinpoint Assure**

2. Sustain trust: Trusted/existing users — **Pinpoint Detect**

3. Confirm trust: High-risk users — **Pinpoint Verify**

3 steps to establishing a circle of digital identity trust

Pinpoint Assure

This advanced security tool uses an extensive fraud evidence database to assess the risk of new and unknown digital identities. It uses rich proprietary insights, mobile carrier intelligence, advanced analytics and machine learning to detect and predict the risk of fraudulent intent at digital account creation, while still providing a positive, seamless experience for your customers.

Pinpoint Detect

IBM Trusteer Pinpoint Detect is a cloud-based solution that helps protect your digital channels against account takeover or fraudulent transactions. It can also help detect end user devices infected with high risk malware. It enables you to assess omnichannel fraud with risk detection, scoring, and step-up authentication to help verify higher risk users – without disrupting the experience of true users.

Pinpoint Verify

Combined with Pinpoint Detect and Pinpoint Verify, this service completes your end-to-end digital identity trust solution.

Working with Pinpoint Detect, it allows organizations to build strong, two factor step up authentication for users who show unusual activity or who engage in higher risk actions or transactions.

Combined with Pinpoint Assure, it allows you to create strong, two factor step up authentication for high risk new users during the account registration process. Identifying which users are high-risk can help you reduce the risk of abandonment due to widespread user frustration caused by a complicated authentication process.

Confidence in security increases customer engagement

There are tangible benefits when customers perceive security in digital channels. Financial institutions that report their customers believe in the security of their digital channels see significantly higher monthly usage of their online portals and mobile applications: 52 percent versus 44 percent for online and 43 percent versus 38 percent for mobile.[2] This translates into a number of benefits for the financial institution, including lower costs when users shift from using branches or call centers to using online and mobile banking and increased opportunities for engagement.

Why should you choose IBM Trusteer for your digital identity trust goals?

The IBM Trusteer platform offers continuous digital identity assurance and context-based authentication, regardless of what industry you're in:

- **AI and machine learning infused with security intelligence service**
- **Scalable, agile could platform powered by a global network of risk expertise**
- **End-to-end strategy for building digital identity trust across the omnichannel journey**

Digital identity trust lifecycle powered by AI and machine learning

Trusteer Digital Identity Trust Platform

Intelligence Cloud
Agile and scalable cloud platform

Global Identity Trust Consortium
Correlates among known patterns, devices, and behaviors

Trusteer Pinpoint Platform

Establish	Sustain	Confirm NEW!
Pinpoint Assure Assess risk of new and unknown digital identities	**Pinpoint Detect** Dynamic behavioral risk assessment of known digital identities	**Pinpoint Verify** Increase trust level with flexible, strong authentication

Rapport
Detect & remediate malware & protect against phishing attacks

Mobile
Exposes mobile risk to allow account compromise mitigation

INTEGRATION

IBM Safer Payments
Omnichannel fraud protection

Most importantly, the IBM Trusteer platform is backed by a team of experts who are passionate about your success. They'll collaborate with you, and with other members of your organization, to create an end-to-end solution that supports your initiative with:

- One product
- One joint roadmap
- One contract to sign
- One solution that meets FFIEC, 2FA and PSD2 standards

500+

organizations rely on IBM Trusteer

1B+

user sessions monthly

Recognized

fraud and risk analytics vendor


“As a mother, I prepare each meal with love. As a chemist, I bake fluffy cakes with $NaHCO_3$.”

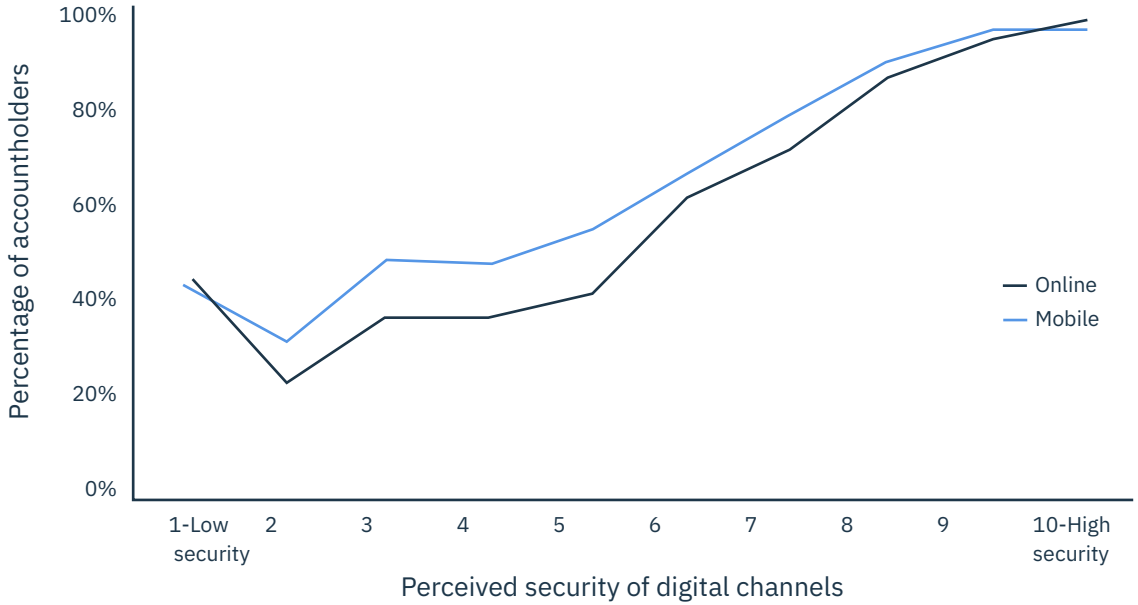
Transform your knowledge into action

Most organizations are already aware of the need to improve their security processes. Yet for many financial service companies, there is still work to be done, as 4 of 10 don't believe customers have full confidence in the security of their digital channels.[2]

This is because they're reminded of their vulnerability every day when they read headlines that yet another organization has been hacked by sophisticated fraudsters. Executives worry that they, too, may fall prey to a breach and suffer the swift reaction of consumers who fear their accounts are vulnerable.

But even as organizations plan to make this important expenditure, they're wary of the problems they may face. Customers recoil when confronted by procedures that may slow them down, or make them feel like they're the criminals. And then there may be an issue with implementation: complexity of technologies, stakeholders and silos, and cost.

In banking, trust and digital security correlate



Source: Javelin Strategy & Research, 2018[1]
Trust among primary financial institution customers (US) by perceived digital security

Transform your knowledge into action

IBM Trusteer has created a comprehensive solution designed to help organizations meet their goals of establishing digital identity and building trust while providing the true customer with an end-to-end journey that is seamless but secure.

For over a century, IBM has provided innovative, reliable solutions that help organizations improve their operations and establish better customer relationships. We've been at the forefront of digital change, developing AI, machine learning, blockchain, cloud and other transformational technologies. We're proud to offer IBM Trusteer as a digital identity trust solution.

If you want to transform knowledge into action—so you can offer your customers a positive, seamless experience—you'll want to learn more about IBM Trusteer.

Try the IBM Trusteer interactive experience

Visit the Pinpoint Verify Marketplace page

IBM Trusteer can help you address key issues identified in the Javelin study[1]

- Align identity and authentication experiences throughout the customer journey
- Minimize reliance on PII (personal identifiable information) at account opening
- Use well-informed risk-based authentication to judiciously apply step-up authentication
- Move away from one-time passwords
- Embrace biometrics for login and step-up authentication

“As a military leader, I demand victory. As a weekend soccer coach, I teach that having fun is more important than winning.”

Sources:

[1] *Preserving Trust in Digital Financial Services: The role of identity and authentication*, Javelin Strategy & Research, 2018

[2] *2018 Digital Identity Trust Survey: How do you establish and maintain identity trust across all channels?*, ISMG, 2018

IBM Global Services
1 New Orchard Road
Armonk, New York 10504-1722

Produced in the United States of America
October 2018

66020366USEN-00

View the online version