Journey

The Trusted Identity Platform

Linchpin of the Networked Era: Trusted Identity

Unlocking Growth

April , 2020 | Mark Bakies, VP of Product Management

Linchpin of the Networked Era: Trusted Identity

The interconnectedness and openness made possible by the Internet and broader digital ecosystem has delivered unparalleled value to society. We have entered an era of hyper-connectivity where digital services blend invisibly with people's daily lives. This paradigm shift has fundamentally changed how we shop, vote, make financial and health decisions, and communicate with friends and family. Almost every area of modern life has been impacted by these technologies, taking us into the Fourth Industrial Revolution, also known as the "Networked Era."

Most unfortunately, for all of the rapid-fire innovations in the online world, it remains next to impossible to be certain that a person truly is who they claim to be. This directly leads to significant risk and/or or a weakened ability to reap the full benefits of the Networked Era.

Security is a *fundamental requirement* in the Networked Era, and one of the most critical elements of security is ***trusted identity***. As more economies and societies transition from the physical world to the digital world, it has become quite clear that existing methods for identity verification and authentication, identity credential handling, data security, and consumer privacy in the online world are inadequate. And these inadequacies are preventing an entire ecosystem of services from being delivered.

Trusted identities are, therefore, the precondition to unlocking the next big growth wave in the Networked Era. The bottom line is that trusted online digital identities (who you are, what you are permissioned to do, and your reputation) will define how we are going to engage and transact in the Networked Era.

Identify Yourself

Verizon states that current methods of digital identity verification and authentication are so weak that identity itself is now the most dominant attack vector used by the bad guys[1]. Verizon data enumerates the fact that 81% of all breaches feed off of lost, stolen or weak identity credentials. RSA reports similar findings in that compromised identities represent the single biggest attack vector for advanced attackers[2].

The Challenges for Business

Protecting this new attack surface, which has grown *significantly* as more people are working from home during the Covid-19 pandemic, is difficult. At the moment, businesses actually have no choice but to trust all identities unless there is conclusive proof that the identity has been compromised. Yet the current reliance on traditional authentication methods, including credit scoring and address verification, rarely functions in a cross-border e-commerce world. Now that credit and debit cards have EMV chips that make them more secure in *physical* environments, *virtual* enterprise Contact Centers have become a favorite target for fraudsters, especially the voice channel because it's so eminently hackable. This is one of the core challenges for information security professionals because their models *are not designed to address identity as an attack surface*. Yet, the business opportunity gained by moving more and more of their business online makes digital transformation a strategic objective of almost every large business.

As organizations scramble to keep up with consumer demand for always-on, frictionless online experiences, fraudsters have capitalized on the gaps and loopholes in fraud defenses. Using identity as the primary attack vector, they manage to bypass traditional security defenses by mimicking trusted user behavior. This widely-known fraud strategy has resulted in an exponential rise in cybercrime.

In a perfect world, each end of any online interaction would be anchored by trusted identities. This creates confidence in transactions and interactions by knowing -- beyond a shadow of a doubt -- that people and businesses **are exactly who they claim to be**. People, businesses, and devices would digitally interact with one another, seamlessly, with minimal friction and with confidence. It would be a world in which trust is easily established and people confidently gain access to the information and/or services and/or experiences they desire. Fraud will become a thing of the past.

Do You Know the Cost of Fraud?

The effects of chronic data breaches in the digital world have now taken hold. Our failure to keep the bad guys out is reflected in the fact that the global financial cost of fraud is $5.127 trillion annually [3]. LexisNexis™ reports that the impact of fraud on U.S. merchants as a percentage of revenues has moved upwards to 1.80%[4]. LexisNexis also points out that for every dollar lost to fraud, it costs businesses another $3+ to cover the costs associated with the labor to investigate the crime,

repair the damage, enhance security, fines, legal fees, and external recovery expenses.

It is also well known that customers care deeply, and are very concerned, about security. In today's world data breaches are well-publicized and severely damaging to customer trust. A Cisco report stated that 22% of breached organizations in 2016 lost customers--40% of them lost more than a fifth of their customer base[5].

Post-Perimeter IT Landscape

Due to mobile computing, cloud apps, and the expansion of telecommuting, de-perimeterization of IT security is now a fait accompli. This has created both new challenges for CSOs and new opportunities for attackers. The leading threats emerging from the post-perimeter IT landscape are at the root of identity becoming the go-to attack vector. Instead of targeting hardened networks and application infrastructures, an ever-increasing number of attackers (both outsiders and insiders) are exploiting identities to gain "legitimate" access to sensitive systems and data.

Additional proof that the current identity models are broken and in crisis: Verizon noted that organized criminal groups were behind 39% of breaches; nation-state or state-affiliated groups were involved in 23% of breaches; and, on average, 56% of breaches took several months or longer to discover[6]. The same report concluded that 69% of breaches were perpetrated by outsiders; 34% were internal actors; and 71% were financially motivated. These recent data breaches have shown that sensitive personal information is widely available and static identity assessment methods (such as context-based authentication) are no longer effective in verifying a person's true identity.

Trust Drives Use

A Frost & Sullivan report states "consumer trust in online services drives usage patterns: when a data breach is reported, 48% stop using that service." They go on to say "while the trend across all consumers shows an increase in online spending over the past 12 months, those businesses exhibiting the highest levels of digital trust increased their net spending online significantly more compared to those with the lowest."

In other words, higher digital trust directly translates into higher revenue.

Ever wonder why businesses don't do more to fight fraud? They can, but if their methods create too much friction then customers will take their business elsewhere. An IDology© research study found that 66% of businesses identify 'balancing fraud prevention and customer friction' as their number one challenge. [7] Likewise, Payments Journal reports that "balancing Consumer Friction with fraud prevention" is the biggest challenge in fighting fraud for 72 percent of fintech and payments businesses. In the same report, 58 percent of fintech businesses also reported that identity verification is one of the biggest fraud prevention challenges within their industry, the highest number across all industries[8]." New forms of fraud such as synthetic identity fraud, mobile fraud, and account takeovers will only drive these numbers higher.

It is not only the fraudsters creating these huge problems but insider attacks as well. Whether wittingly or not, insiders are a significant source of fraud in the enterprise. In a Frost & Sullivan whitepaper, they report 53% of survey respondents said they had experienced an insider attack in the last 12 months and 20% reported 6 or more attacks in 12 months.[9]

Contact Centers on the Front Lines of Fraud

Since the implementation of EMV chips in credit and debit cards, Contact Centers in particular have come under frequent attack by fraudsters.

- A PinDrop study found that, on average, the cost of fraud occurring in Contact Centers amounts to 58 cents per call, when amortized across every call handled within the contact center[10].
- IDology also reported that fraud had decreased in only 9% of Contact Centers, while 53% said it stayed the same, and 38% admitted that fraud had increased[11].
- Worse, in a TrustID survey, they found 69% of Contact Centers are still using Knowledge-Based Authentication (KBA) to authenticate callers and, yet, only 10% of respondents felt very confident in KBA's ability to authenticate callers accurately[12].

KBA as an authentication technology has several other undesirable attributes as well, including: 1) lengthens agent average handle time, 2) degrades the customer experience, and 3) gives a false sense of security.

Given the ineffectiveness of KBA technologies, IDology set out and asked Contact Centers the following question:

“What do you think will be trending in identity verification in the next few years?”

The answer: The utilization of mobile device attributes for verification took the lead (44%), followed by artificial intelligence (42%), machine learning (41%), and submitting identity documents via mobile (40%)[10].

Ideally, we should be able to reconcile security with innovation and ease of use. And while these threats absolutely are real, the response must be balanced. The Internet is one of the most powerful engines for social change and economic prosperity. We need to preserve those qualities while making it more resilient against attack and misuse.

What Does the Path Forward Look Like?

What are the tools and technologies that will allow us to make legitimate customer and business interactions and transactions safer? Can it be done using a solution that improves the customer experience and increases the security of the transaction, while being transparent to the user at all times? If we can answer these questions, through building solutions, then trust in digital transactions and interactions will emerge as the new paradigm.

We’ve been thinking about these challenges and opportunities for the past two years, and have come up with a ground-breaking solution that solves this problem for security, privacy and customer experience simultaneously. Journey is in stealth mode, but will broadly announce its solution in mid-2020.

At Journey, we believe a trusted digital identity is the most important innovation needed in the online world. Making a verifiable digital online identity the root of that trust is the key to unlocking the next wave of growth in the Networked Era. We recognize that a trusted identity is first and foremost a security problem. Privacy is the other critical element in creating trusted identities; therefore, all of our products and platforms fully adhere to the principle of privacy-by-design. Only by first solving security and privacy problems will it be possible to create trusted digital identities for the online world.

No Need for Compromise

The Journey solution addresses the conflicting requirements of privacy and accountability. We provide strong authentication without friction by adding an engineered security platform that is imperceptible to the end user. Most importantly, our solution helps to prevent fraud because fraudulent behavior becomes easier to detect, given the fact that bad actors behave differently than a trusted user.

Fraudsters must go to great lengths and invest huge amounts of effort to mask their devices, their locations, and their true identities, often using stolen credentials in order to fit into the profile of the genuine customer. While it is, indeed, possible to “fake” one’s identity reputation and behavior are much more difficult to imitate.

The Platform

Our Trusted Identity Platform is not a single breakthrough but, rather, encompasses and supports a wide range of elements. We fully understand that trustworthy, solid peer-to-peer relationships among people, organizations, and the Internet of Things is what will revolutionize digital interactions.

We believe that the following elements are critical and must be considered by every organization in order to establish and protect trust anchors:

- cryptographic identities
- zero-trust networks
- zero-knowledge service providers
- multiple-factor authentication
- risk-based step-up authentication
- behavioral and physical biometrics
- new security and privacy models to comply with the changing regulatory environment

Our approach is modular and flexible and can accommodate these vectors and more, depending upon the needs of each business.

A New Security Model, Rooted in Identity

Trusted Identity is first and foremost a security challenge. One of the most important elements of our security model is to eliminate the exchange of identity

credentials. Instead, we allow the customer to provide proof of ownership of their credentials. Our privacy model ensures that consumer data privacy compliance and consent requirements demanded by even the most stringent privacy regulations can be not only met, but exceeded, in both letter and spirit, while improving customer experience rather than sacrificing it. Privacy can – and will – have a major comeback.

Digital identity is about establishing full confidence and trust at both end points of the interaction. Each party needs to be confident that the party at the other end is who they say they are. And both require trust in the system that mediates that interaction. Imagine a world where a person's identity and the devices operating on their behalf can be verified immediately, safely, and securely, across multiple touchpoints and in both the digital and the physical world; where access is gained without passwords and data is exchanged only with consent and privacy. This is the future we are creating at Journey.

This newly found confidence in both consumers and business will bring about the next growth wave of digital and networked services. Fraud will be all but eliminated. Consumer data privacy compliance will become simple because sharing identity credentials will be replaced by proof-of-ownership of the appropriate identity credentials. These interactions will transform payment and commerce from a location-centric, in-person model to a global, not-present, digital model. This newfound trust will spark exciting innovations in both new and existing industries. It's hard to imagine the types of user experiences that a trusted digital identity makes possible.

Journey has taken a fresh look at this problem, identifying the core pieces that make up an entire *identity* and the security needed to protect that identity, all the while acknowledging the basic inherent need for privacy. It is our mission to restore trust to the digital world by making identity the root of that trust.

Getting to a world where there is trust that people are who they say they are is a journey worth taking. See you there!

References

[1]Verizon, “2017 Data Breach Investigations Report”, July 2017, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

[2]MINIMIZING THE IDENTITY ATTACK VECTOR WITH CONTINUOUS AUTHENTICATION, RSA, https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/White_Paper_Minimizing_the_Identity%20Attack_Vector_with_Continuous_Authentication.pdf

[3]The Financial Cost of Fraud, 2019, Gee and Button, Crowe Ireland with University of Portsmouth, http://www.crowe.ie/wp-content/uploads/2019/08/The-Financial-Cost-of-Fraud-2019.pdf

[4]The True Cost of Fraud Study, 2018, LexisNexis, https://risk.lexisnexis.com/insights-resources/research/2018-true-cost-of-fraud-study-for-the-retail-sector

[5]“Cybersecurity Report: Chief Security Officers Reveal True Cost of Breaches And The Actions That Organizations Are Taking,”, 2017, Cisco Systems

[6]Verizon Data Breach Report, 2019, https://enterprise.verizon.com/products/security/verizon-risk-report/?cmp=paid_search:google&gclid=Cj0KCQjwuNbsBRC-ARIsAAzITucdvfSbvYIkMWiN0mY9KrZHoINB9ZGm09mtHeumknIXshOcs6xnizUaArOfEALw_wcB

[7]“Sixth Annual Fraud Report”, IDology, Inc., 2018 https://ww2.idology.com/sixth-annual-fraud-report

[8]Source: Fraud Report, Payments Journal, January 2, 2019 https://www.paymentsjournal.com/security-and-consumer-friction-fraud/

[9] Frost & Sullivan “The Global State of Online Trust” https://docs.broadcom.com/doc/the-global-state-of-online-digital-trust

[10] PINDROP study 2017 Call Center Fraud Report: https://www.pindrop.com/wp-content/uploads/2017/04/Fraud-Report-Global-4-24-17-FINAL.pdf

[11]“Sixth Annual Fraud Report”, IDology, Inc., 2018 https://ww2.idology.com/sixth-annual-fraud-report

[12] “State of Call Center Authentication”, 2018, TrustID

[]“Insider Threat – 2018 Report”, Cybersecurity Insiders, Crowd Research Partners, December, 2017, https://crowdresearchpartners.com/portfolio/insider-threat-report/