TRANSFORMING THE BANKING EXPERIENCE WITH TRUSTED IDENTITIES

Entrust Datacard™

+1-888-690-2424 | entrust.com

Table of contents

Challenges Facing Financial Institutions

"Consumers now interact with banks 15-20 times per month, up 3-4 times in the pre-digital era."
– NETFINANCE

Financial Institutions need to start rethinking how they interact with their consumers. Today's FIs face a breadth of consumer demands, competitive threats and security and fraud risks. While it's easy for financial institutions to overlook consumers' user experiences in favor of security, the fact is that consumers are seeking richer, more gratifying digital banking experiences, and they will go to the competitor that offers simplicity as well as security.

"An average company hears from less than 5% of its unhappy customers."
– RUBY NEWELL-LEGNERT

Acquiring and retaining consumers in a fiercely competitive marketplace flooded with waves of non-traditional players — requires a consumer-centric digital strategy. The key enabler for an effective digital strategy is trusted identity. With a single trusted identity, consumers can move freely between banking channels and access online services, mobile apps and bring efficiency to ATM, self-service, and in-branch experiences.

Digital banking is nothing new — online banking has been around since the late 1980s, and even mobile banking is more than 15 years old. The real frontier is interconnecting these digital channels with the modern branch location to create a seamless omni-channel consumer experience — empowering both retail and commercial banking customers with the choice of transacting whenever and wherever it is most convenient.

Disruptors in the Digital Marketplace

Clearly, the advent of online and mobile commerce has transformed how we interact with our banks. Rather than visiting a branch or ATM to deposit a check, pay a bill, or transfer money to friends or family, our mobile phones have become a virtual ATM in our hands. Rather than visiting retail stores across town, we browse from the convenience of our tablets experiencing unprecedented choice, convenience and price advantages.

In our increasingly interconnected world, consumer expectations for seamless, anywhere anytime services continue to drive rapid innovation. Instead of leveraging a convenient consumer experience as an accessory to a product or service, forward-thinking businesses like Uber and Airbnb are winning on that convenient experience alone. These leaders are creating consumer experiences that fully deliver on instant connections, convenient anywhere anytime services and the ability to move seamlessly from digital transactions into a real-world experiences using the one device that everyone knows and loves.

As observed by The Financial Brand, this "Uberization" of industries has brought us to an intriguing point:

- The world's biggest taxi company (Uber) owns no vehicles.
- The world's largest lodging provider (Airbnb) owns no real estate.
- The world's largest retailer (Alibaba) has no inventory.
- The world's most popular media company (Facebook) creates no content.

These disruptors have effectively cut out the middleman, building success on an exceptional consumer experience that instantly puts a wealth of goods and services at consumer fingertips.

A Growing Threat for Financial Institutions

What does this mean for financial institutions? According to Goldman Sachs analysts, non-traditional digital banking "startups" are already jeopardizing around $4.7 trillion of the financial services industry's business. Today's financial consumers care less and less about the end products — high-return deposit accounts or low-rate loans — and more and more about the simplicity, convenience and empowerment of the omni-channel consumer experience.

While most in the financial industry is aware of the importance of moving toward this omni-channel experience, this has traditionally been seen as a strategy for adding value to existing financial products and services. The threat of "Uberization" changes this from an added-value strategy to an essential priority of survival. A 2015 survey of millennial financial consumers found that two out of three feel that bank's digital services are somewhat or not at all seamless. Financial institutions must beat these start-ups at their own game, getting ahead of the innovation curve by instantly connecting consumers with mobile-optimized services, enabling anytime-anywhere transactions and delivering the convenience of a truly friction-free experience as they move between the mobile, online and in-branch worlds.

Identity: The Foundation of the Omni-Channel Experience

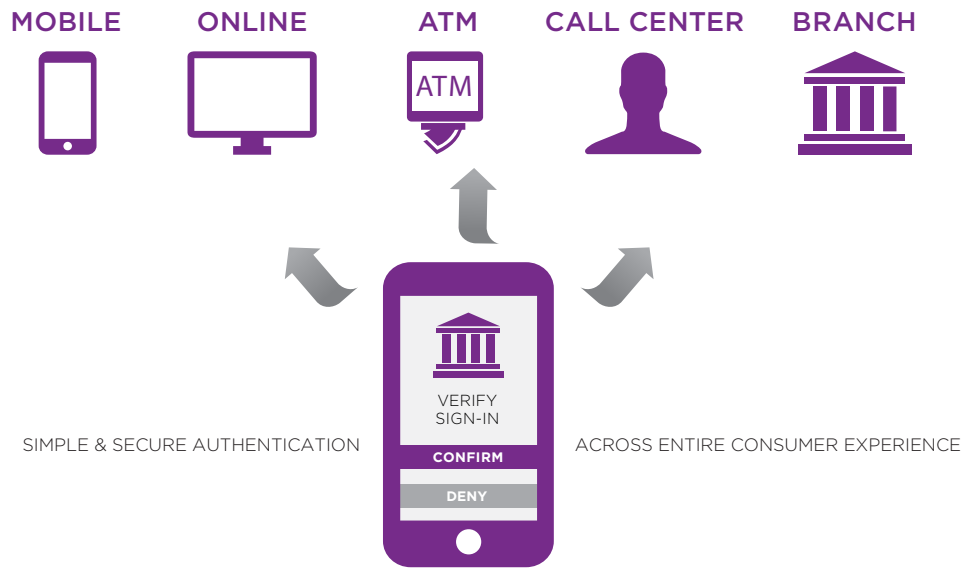
Mobile banking is more than 15 years old. The real frontier for today's financial institutions is interconnecting digital channels with the modern branch location to create a seamless omni-channel consumer experience — empowering both retail and commercial banking customers with the choice of transacting through whichever channel is most convenient. The core of this challenge: authenticating identity. Financial institutions must work toward a single powerful credential that gives consumers seamless access to multiple channels (online, mobile, POS, ATM, etc.) and acts as a multi-functional tool for accessing information, verifying transactions, signing or approving contracts and more.

Omni Channel Use Cases

Your customers want to move freely between channels, including online, mobile and in-branch experiences. Our authentication solutions give them this freedom and allow them to access it all with a single trusted identity - no usernames, no passwords, and no hassle.

Mobile Banking Access. The mobile banking experience is similar to accessing a standard mobile app - only more secure. Customers simply sign on using a PIN or biometric. In the background, a strong digital identity and adaptive authentication verify both user and device identity.

Omni Channel Access



Online Banking Access. Eliminating passwords for online banking access, creates a more enjoyable user experience as well as mitigating significant security vulnerabilities. With our authentication solutions, a push notification is sent to the customer's phone to authenticate their identity, which enables them to log into their account-clean, simple and secure.

Full Omni-Channel Access. Mobile banking is more than 15 years old. The real frontier is interconnecting these digital channels with the modern branch location to create a seamless omni-channel customer experience - empowering both retail and commercial banking customers with the choice of transacting through whichever channel is most convenient. The core of this challenge: authenticating identity. Financial institutions must work toward a single powerful credential that gives customers seamless access to multiple channels (online, mobile, POS, ATM, etc.) and acts as a multi-functional tool for accessing information, verifying transactions, signing or approving contracts and more.

As your digital strategy evolves, customers will be able to use their mobile identities to access ATMs, self-service kiosks and even to authenticate call center and in-branch interactions, in both branches or other remote locations.

Traditional Credentials Cannot Keep Up

In a world of accelerating connectivity, where consumers expect to move from online to mobile channels and interchange between multiple connected devices (laptops, tablets, smartphones and more), both the security and convenience of each digital interaction hinges on fast and effective authentication of the identity of both the connected device and the user behind that device. Traditional credentials simply cannot keep up:

- **Usernames:** Poorly concealed; easily guessed
- **Passwords:** Simple passwords are easy to guess, but even the most complex passwords can be cracked with today's sophisticated techniques and tools
- **Secret Questions:** Hard for legitimate users to remember and easy for criminals to research online
- **Payment Card Numbers:** Magnetic stripe numbers can be skimmed; chip card numbers can still be stolen and used online
- **CVVs:** Numbers are static and can be easily obtained, making them a poor security measure for card-not-present fraud
- **One-Time Passcodes:** Complicate the user log-in experience, add the burden of carrying hardware tokens and are susceptible to advanced malware attacks

In essence, consumers are attracted to convenience — but retained with security. A recent survey of financial consumers found that 68 percent said they would switch financial institutions to obtain more convenient digital channels. But they will just as quickly jettison a convenient experience when it proves unreliable and insecure, as that same study found that that 73 percent of consumers said they would likely switch their financial institution following a breach of their personal or financial information.

As financial institutions work to deliver this upfront convenience and back-end security, traditional credentials are failing on both accounts. For customers, managing countless credentials of varying types across devices, channels and providers is far from seamless — and often a downright hassle. This lack of convenience undercuts the core value of the omni-channel experience, defeating seamlessness before the experience has even begun. Difficult identity authentication leads to abandoned transactions and fewer interactions — and as loyalty and stickiness fades, consumers defect to competitors in search of a better experience.

In addition to the threat of lost consumer loyalty, the hassle of managing multiple credentials leads many consumers into "workaround" behaviors that seriously compromise the security of a financial institution. From using common passwords and patterns to sharing tokens, these "workarounds" open the door for identity theft, data breaches and other cybercrime. With cybercrime growing in frequency and sophistication — and with the shift to EMV payment cards pushing more fraudsters to digital channels — financial institutions are hesitant to expose themselves to additional risks of rolling out new, more convenient digital offerings. They know that, in the event of a breach, the loss of consumer trust will negate any gained consumer convenience.

A Powerful Solution Emerging

With consumer lifestyles increasingly centered on mobile devices, forward-thinking financial institutions are now seeing the vast potential of a relatively obvious identity solution: If mobile transactions are the growing core of the consumer's omni-channel experience, why not make the mobile device the core of a powerful identity solution?

Transforming the Customer Experience with Mobile Identities

Mobile identity is rapidly emerging as an effective solution for empowering the friction-free experience consumers desire, paving the way for new digital services to be introduced while providing the necessary security to combat sophisticated cyber threats in today's complex digital ecosystems. The following pages consist of the key benefits of a mobile identity solution.

The Convenience of Mobile Identity

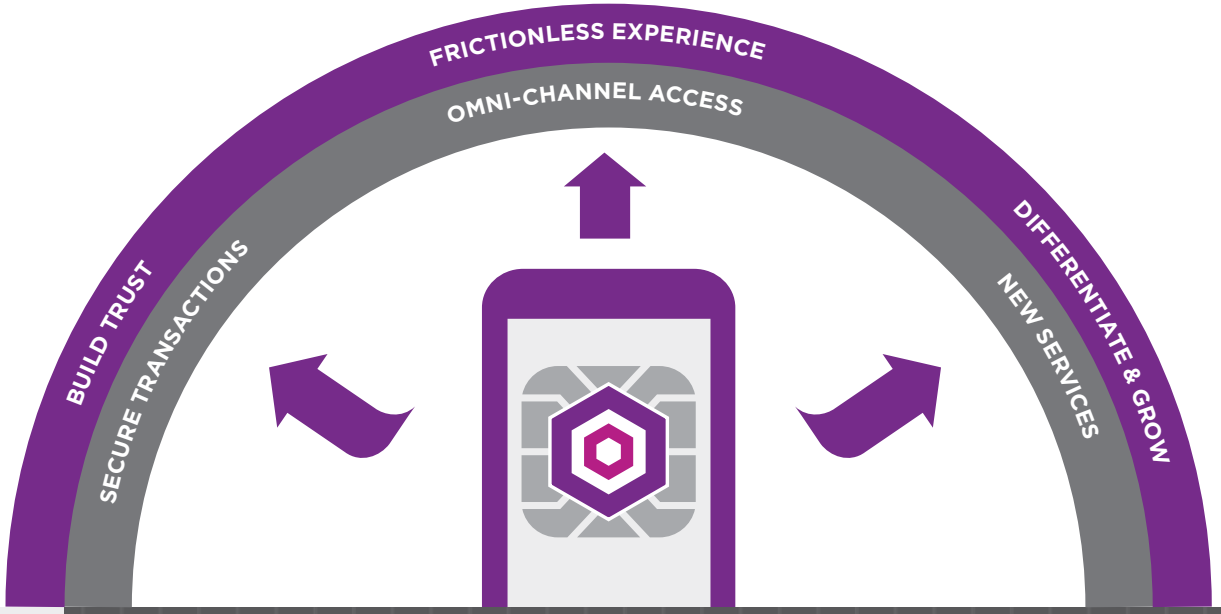
Consumers love their smartphones. They carry them everywhere. Embedding a trusted identity within this already popular device puts an identity authentication solution conveniently at consumers' fingertips, eliminating the need to tote additional credentials or tokens along with them. And, because consumers increasingly conduct essential transactions via mobile channels, a trusted mobile identity enables them to access all of their digital channels and conduct digital transactions with a single, intuitive credential — enabling a truly seamless experience.

Envisioning the Seamless Experience of Mobile Identity

Seeing the full potential of mobile identity requires envisioning how trusted identities act as the foundation of consumer experience transformation.

Implementing trusted identity provides a range of benefits including frictionless access to services, building trust through simple to use transaction security and differentiating from competitors to delight customer and grow market share.

One Identity — Many benefits



Trusted Identities Start with Your Mobile Banking Application

Where and how the trusted identity resides is important. At Entrust we believe banks and other consumer facing organization want to augment the value and use of their own mobile application and not introduce a new (identity application) that may be less desirable for the customer (2 apps to manage).

Banks can embed trusted identities into their mobile application using a SDK. The SDKs provide access to the full suite of IdG Mobile features and can be used for a number of use cases.With identity built right into the mobile banking application – security / access can become virtually transparent to the use as this identity can be used in the background without the need for users to enter OTP codes or remember passwords and challenge questions and answers (KBA – knowledge based authentication).

Embed Trusted Identity Directly Into Your App

Accessing Mobile Banking

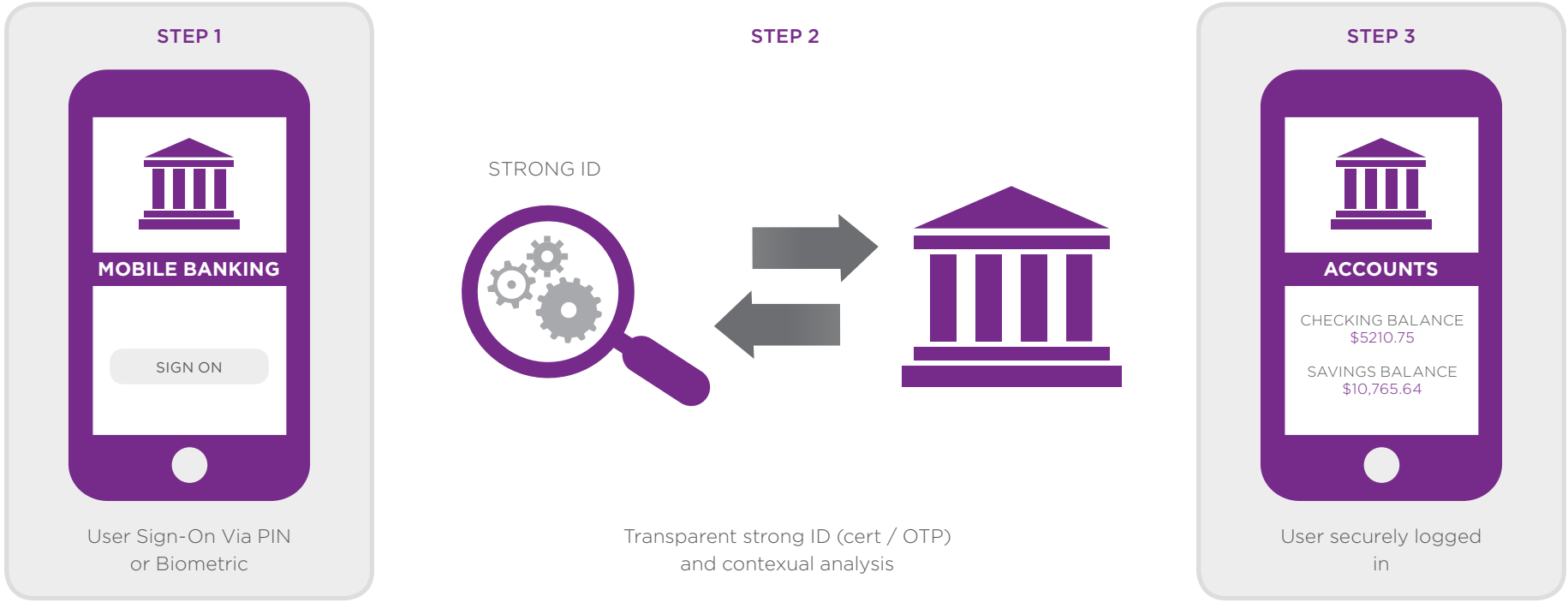
The customer selects their mobile banking application icon on the mobile phone. The app should be protected with biometric access like TouchID or PIN so that IF the customer ever loses their phone – someone cant pick it up and log in.

Once the application is opened, the sign on begins automatically.

Behind the scenes (transparent to the user) the trusted user identity on the phone is validated by the authentication server back at the bank. As well, best in class authentication solutions can do a number of other transparent security checks such as assessing the mobile device fingerprint, the geo-location and even a fraud "risk score" from third party fraud engine. All this happens in micro-seconds.

The user in logged into mobile banking and all they did was open the application with a fingerprint check. No passwords – no hardware tokens – no challenge questions...

Mobile Banking Access

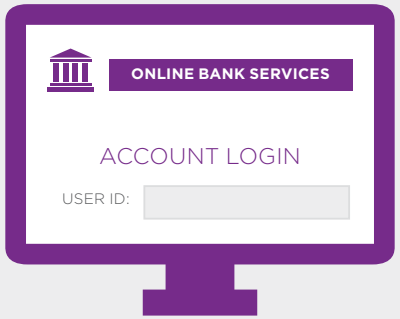


Accessing Online Banking

With mobile identity, a customer no longer must recall and input a complex username and password to access web applications like online banking. Instead, a user is sent a push notification directly to their secure mobile device to authenticate the web session. The customer simply confirms with a click — no password required — that they are, in fact, initiating a web session.

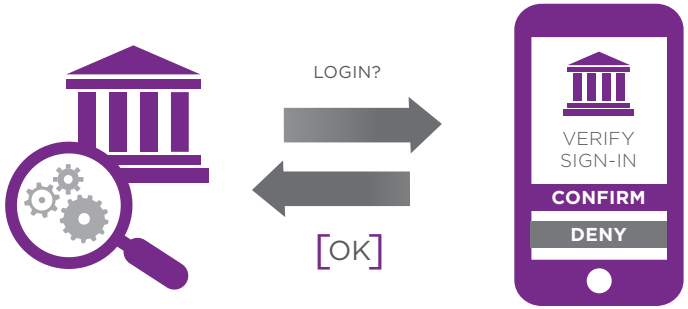
Online Banking Access

STEP 1



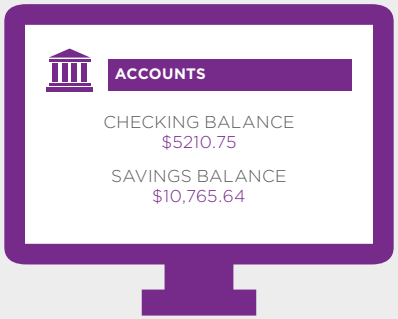
User signs in — no password

STEP 2



Push notification sent to user's phone

STEP 3

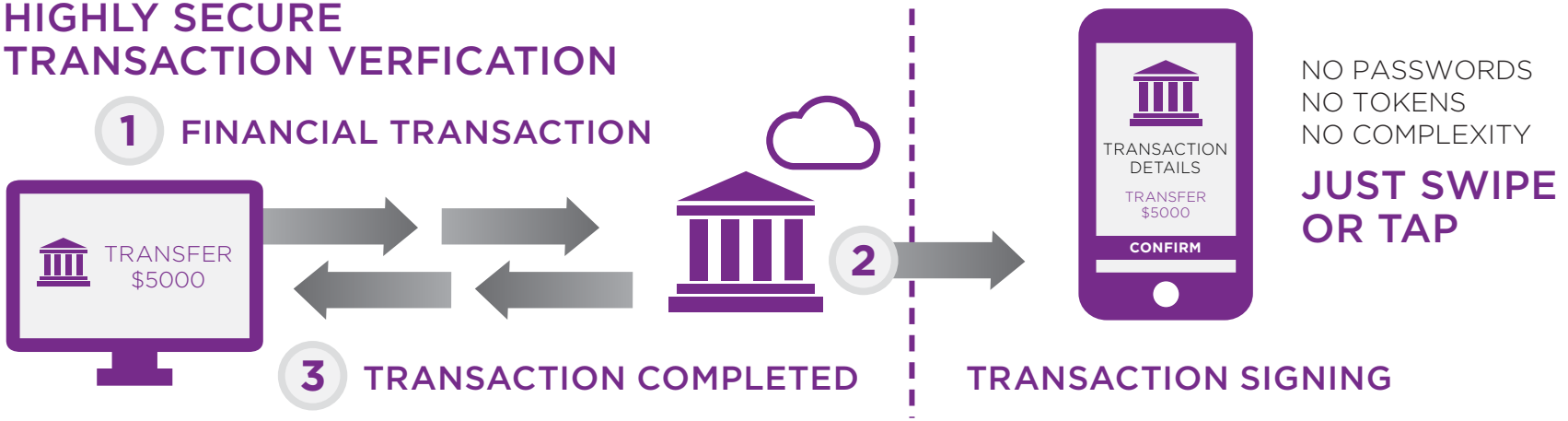


User securely logged in

Making Online Transactions

When making an online transfer, how can a customer be sure the system is not infected with malware ready to intercept the transaction? With a mobile security solution, a push notification can be sent directly to the secure mobile device, enabling the customer to verify the transaction details. Customers receive instant confirmation if a transaction is successful — and can immediately flag fraudulent transactions.

Defeating Account Takeovers / Man In The Browser Attacks



In certain situations, customers may not have an active data connection to receive push notification on their mobile phones. Transaction verification using the mobile QR code reader provides the same level of transaction security and only involves a few more keystrokes to enter an OTP on the online channel to complete the transaction.

Transaction Verification When No Data Connection Exists

On-the-Go Transaction Signing

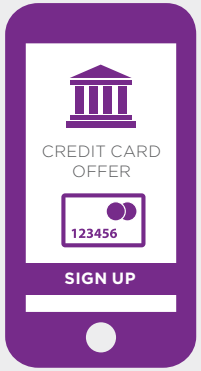
Many consumer transactions require formal, signed approval — from credit card and loan applications to contracts and special offers. A truly seamless experience must include digital signing capabilities for on-the-go, anytime-anywhere approval — but traditional digital signing is difficult to deploy and even harder for customers to use. A mobile identity platform can leverage the built-in biometrics capabilities of a mobile device to allow fast, easy and secure digital signing. The customer receives a notification when a transaction requires a digital signature, and authenticates the digital signature by scanning a fingerprint. This not only enhances the customer experience — it speeds day-to-day business operations and improves internal productivity for financial institutions.

Mobile Digital Signatures

STEP 1

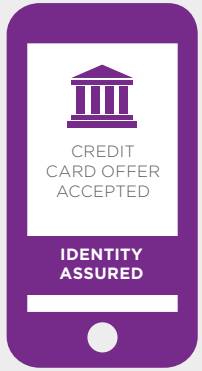
Present customer with credit offers, new products, etc.

STEP 2



Offer pushed to mobile device for customer review

STEP 3



Customer accepts and transaction becomes legally binding

Shopping Online

When shopping online, maintaining a secure transaction while ensuring a seamless, user-friendly experience is difficult. With mobile identity, when an online retailer verifies a customer's sufficient funds with a financial institution, it can also request the consumer to approve the transaction through a push notification to the secure mobile device. With a simple tap on a mobile device, the customer, the financial institution and the retailer gain instant transaction verification.

This type of verification also enables customers to customize guidelines as to which type of transactions they want to receive in real time — those over a specific dollar amount, from specific vendors (eBay, Amazon, etc.) or even originating from a foreign location. This allows the customer to create the perfect balance of added peace of mind without creating added hassle while providing the financial institution with lower risk of fraudulent activity.

In some situations, online transactions requiring verification cannot be verified via push notifications due to the absence of a data connection. In these cases, a QR code can be generated on the online banking screen and scanned by the mobile identity application. Transaction details are then presented to the user for review and approval.

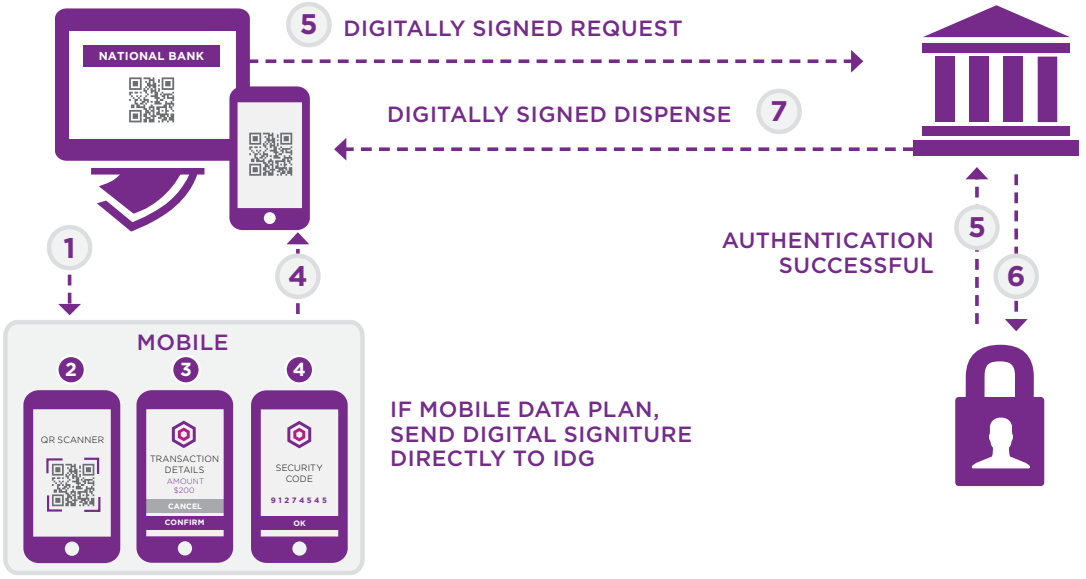
Defeating Card Not Present (CNP) Fraud

At the ATM or Point-of-Sale — Without Network Access

When a customer uses an ATM or point-of-sale (POS) terminal in a store, mobile identity can add an extra layer of security, verifying the transaction in real time even without network access.

1. The ATM or POS terminal displays a unique, transaction-specific QR code on-screen or on a printed receipt.
2. The customer scans the QR code with the secure mobile device.
3. The customer reviews the transaction information and confirms via mobile PIN or TouchID.
4. The mobile device displays an 8-character digital signature for the transaction.
5. The customer enters the unique digital signature into the ATM or POS terminal.
6. The ATM/POS confirms that the digital signature matches the transaction — and officially approves the transaction.

ATM or Point of Sale QR Code — Mobile No Data Connection



Augmenting a Trusted Mobile Identity with Layered Security

While a trusted mobile identity provide a truly powerful approach to secure access and transactions, the number of attack vectors continue to grow. The best solution implementation will include a layered security approach providing a number of transparent methods to assess and mitigate against risks. The key – is to keep all security transparent and IF you need to engage the cosumer – make sure all the need to do to assure identity is a quick touch, tap or swipe.

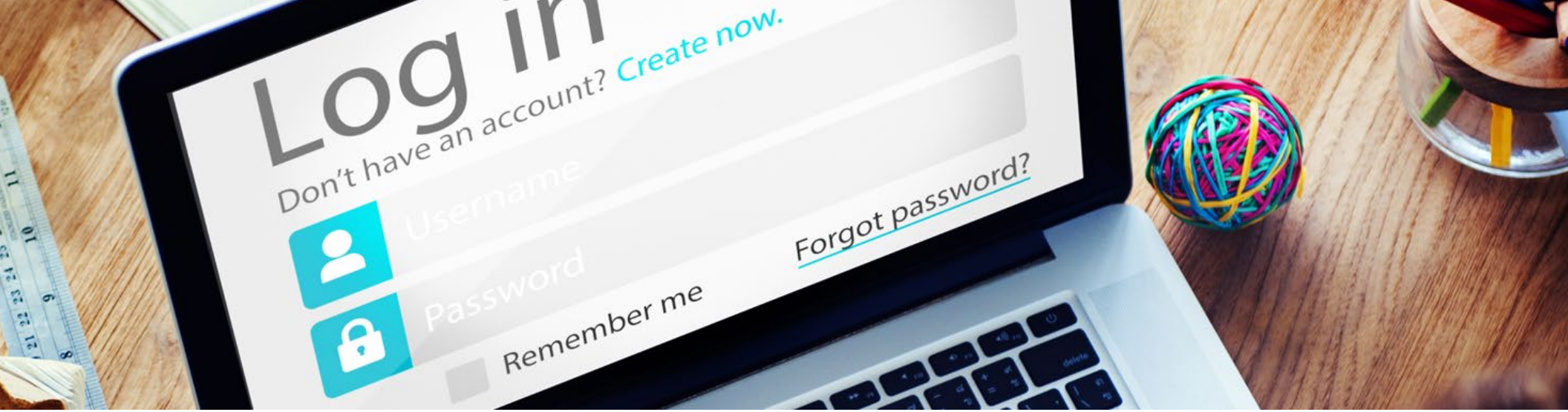
The Transparent Layers of Strong Identity

RISK VECTORS

Jail broken phones
Lost/stolen phones
Rogue applications
Breached credentials
Impersonating devices
Banking trojans/malware
CNP fraud

Security Layers

Operating System		Jailbreak detection Sandboxing Malware Detection Trusted execution environment (TEE)
Device		Device fingerprinting Geo-location Device ID Protected application access
Channel		Mutual SSL authentication
User		Adaptive authentication Embedded digital ID Push authentication
Transaction		Push transaction signing Transation signing tokens



Mobile Identity: Anchoring Your Disruptive Innovation

The diverse and powerful use cases described illuminate the big-picture value of a mobile identity platform. A trusted mobile identity can become the anchor point for an entire strategy for captivating consumers with truly seamless omni-channel convenience. You can provide your customers with a single, trusted identity credential that is already embedded in their daily lives. This single identity empowers the consumer to conduct all their critical interactions — from online and mobile to ATM and in-store POS, all the way to call-center inquiries. That same identity unlocks valuable new potential for the consumer, from enhancing transaction security to allowing simplified digital signing, person-to-person payments and even physical access to a branch. Looking to the future, your mobile identity platform offers the agility to become the single trusted identity credential for a vast range of third-party transactions — third-party retailers, social networks, healthcare and even government services. This crucial adaptability serves to make your trusted mobile identity even more essential to your consumers' everyday lives, reinforcing loyalty to build and sustain relationships. In essence, the mobile identity is the anchor point for a financial institution's own disruptive innovation, putting you at the forefront of the "Uberization" of the industry.

Leveraging Mobile Identity to Drive Innovation

Financial institutions are facing increasingly complex and interconnected ecosystems of mobile devices, online channels and in-branch interactions — compounded by cyber threats that grow in sophistication and frequency daily. The inherent features of today's mobile devices — from GPS location to biometrics capabilities — make a mobile identity platform an attractive solution for enhancing network security, identity authentication and transaction verification. These security capabilities give financial institutions the tools they need to mitigate the risk of costly breaches, as well as the equally devastating loss of consumer trust that follows a breach.

At the same time, mobile identity is a natural solution for conquering the threat of "Uberization," providing financial institutions with a potent platform for driving innovation, defining and meeting new customer needs, and delivering simplified, intuitive, seamless customer experiences. Following the lead of disruptive leaders like Airbnb and Facebook, financial institutions can leverage a mobile identity solution to put innovative offerings directly into consumers' hands, turning the mobile devices that consumers love into a powerful tool that instantly connects them with information and services, enables their anytime-anywhere transactions, and delivers a friction-free transition as they move between the digital realm to the real world.

About Mike Byrnes

Mike Byrnes has more than 20 years' experience in product management and technology marketing with a focus on internet security and business communication systems. Mike drives product marketing for the Entrust IdentityGuard authentication platform with a significant focus on mobile solutions.

In addition to mobile, his background covers identity and access management, fraud detection, malware protection, and email encryption solutions. Mike serves as vertical market prime for Entrust financial services segment, working with large banks across the globe to roll out solutions to their consumer- and corporate-banking client base.

About Entrust Datacard

Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide.

For more information about Entrust products and services, call **888-690-2424**, email **entrust@entrust.com** or visit **www.entrust.com**.

Headquarters
Entrust Datacard
1187 Park Place
Shakopee, MN 55379
USA

Twitter Facebook Youtube LinkedIn Google+ RSS

Entrust Datacard™

30124-2-0116