MOBILE AUTHENTICATION

Establishing Secure Commerce Without Friction

ca technologies

Mobile Commerce Is Booming

OVER 1.7 BILLION CONSUMERS WILL HAVE SMARTPHONES **BY 2018**[1]

ONLINE TRANSACTIONS WERE CONDUCTED ON SMARTPHONES DURING **Q4 2014**[2]

[1] Statista, www.statista.com
[2] Joshua Stanphill, Teamwork Retail, 2015

Yet, Barriers to Wide-Scale Adoption of Mobile Commerce Remain

And everyone has their own agenda ...

Consumers seek reliability and security

Nobody wants to be "that guy" holding up the line because the technology doesn't work—or worse yet, "that girl" who got her identity stolen. And, isn't it a risky commitment putting all your sensitive information on a device that can be lost or stolen?

Merchants and service providers are looking for convenience and cost-savings

Is mobile technology something customers want? Will it make transactions more or less convenient? They also worry about liability for security issues as well as the initial cost and inconvenience of set up.

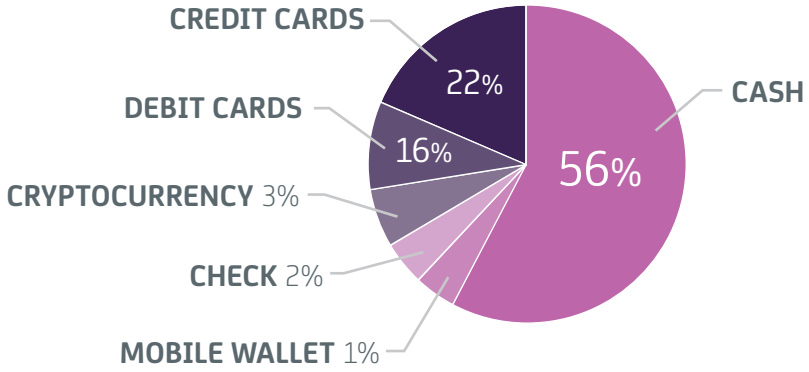
Phone manufactures are looking for competitive advantage and a new stream of revenue

Which standards and technologies will offer users the best experience without sacrificing the security of their information? Oh, and they need to understand how this is going to make them more money.

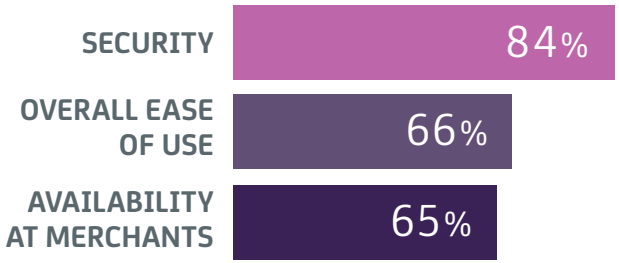
Consumers Are Especially Worried About Security

In a time where stories cyber attacks and security breaches pop up online and in the mainstream media on an alarmingly regular basis, it's no surprise that everyone is worried about the security of their information. The prospect of loading sensitive personal and financial data onto a device and then sharing it with a click or a tap leads to survey findings like the ones seen here.

Consumers deem Bitcoin more secure than mobile wallets



Reasons for concern about mobile transactions



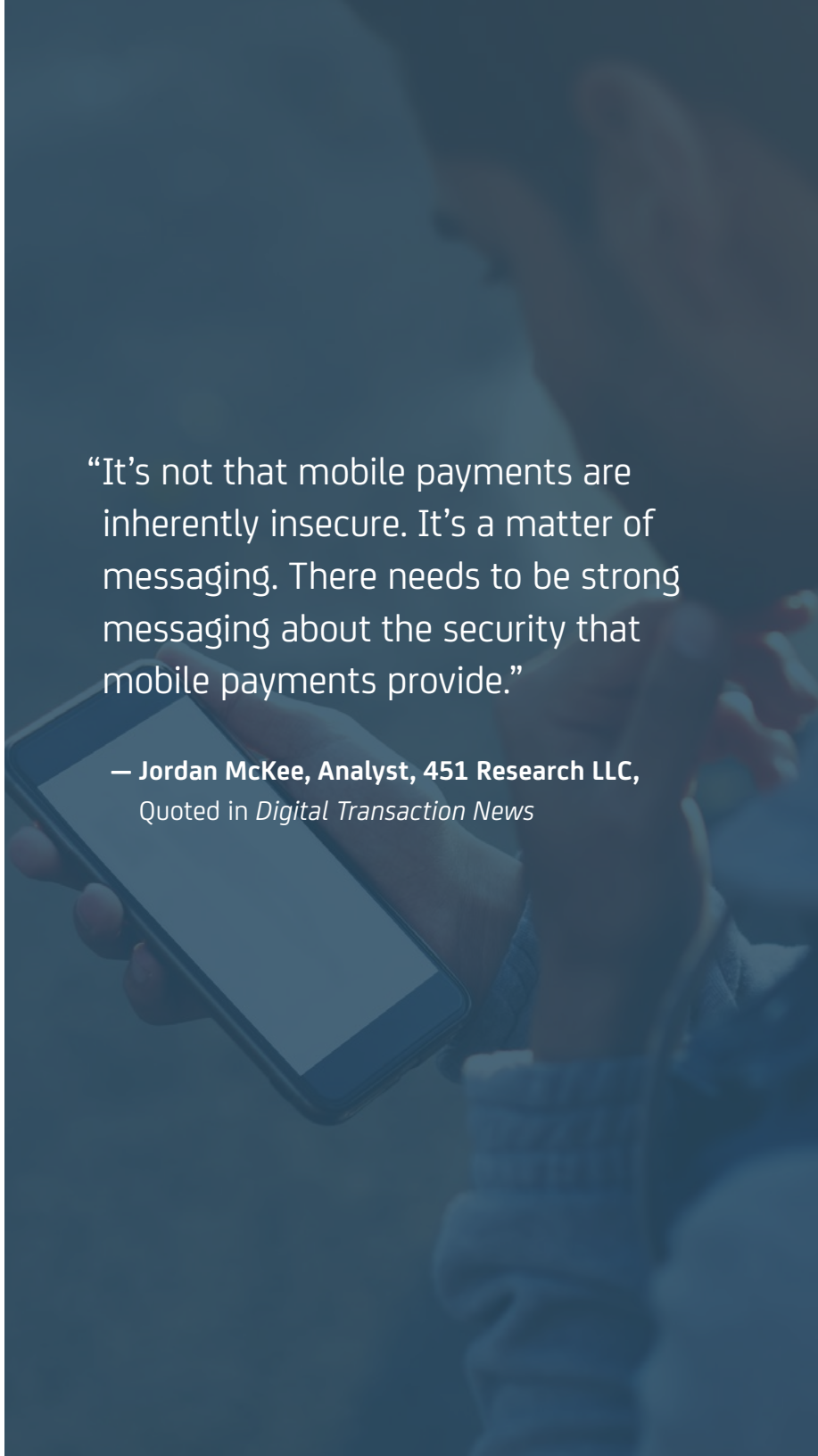
Seamless, Trustworthy Authentication Is the Key

Mobility has the potential to revolutionize the way we traditionally think about authentication. Whereas most consumers have become comfortable initiating online transactions from their desktop computers, performing a similar task with their smartphones still generates anxiety.

Which, when you think about it, doesn't make a lot of sense. Consider that reliable authentication can be confirmed in three basic ways:

- **Something you know**, such as a password
- **Something you have**, such as an encrypted keycard or token
- **Something you are**, such as a fingerprint

Smartphones are capable of supporting all three—individually or in combination. Data can be password-protected. Phones can transmit encrypted data that confirms the bearer's identity. And the ever-increasing computing power of smartphones, combined with their optical capabilities, make them perfect for reading fingerprints, or running facial recognition or retinal scan algorithms.



"It's not that mobile payments are inherently insecure. It's a matter of messaging. There needs to be strong messaging about the security that mobile payments provide."

— Jordan McKee, Analyst, 451 Research LLC,
Quoted in *Digital Transaction News*

In Fact, Mobile Devices Are Ideal Authentication Conduits

Not only do they have the technological capacity to support all three major authentication methods, smartphones actually offer several user-based characteristics that make them superior authentication devices.

Virtually everyone has a smartphone. Most people only use one device, and mobile phones are almost never shared by more than one person. Together, these characteristics make smartphones the perfect medium for individuals to carry their unique authentication data with them wherever they go.

Smartphones also support all authentication schemes

There are three principal authentication technology schemes in use today. And once again, smartphones support all three:

- **With**—Authentication data can be transmitted **with the phone** *(One-time password, Authentication Applications).*
- **To**—Use of the device can be restricted exclusively **to the authorized user** *(Fingerprint, Passkey).*
- **Through**—Identification data can be passed **through the phone for third-party confirmation** *(Facial Recognition).*

Mobile authentication can even combine data from different schemes, such as location tracking, airline ticket purchases and user profile, to create an additional level of certainty.

Different Schemes for Different Needs

Not all applications require the same level of authentication security—nor do all need to remain valid for the same length of time. Imagine if everyone could simply carry a small device in his or her pocket that could be programmed to provide the necessary authentication in virtually any circumstance. For instance:

Short-term authentication—For credentials like boarding passes and hotel room keys, the issuer needs to be able to assign a limited timespan for which they are valid in order to preserve security.

Mid-term authentication—Issuers of credentials such as work badges and credit or debit cards want those items to expire every few months or years to clear "inactives" off their rolls.

Long-term authentication—Because they are virtually impossible to forge, biometric markers like fingerprints and retinal patterns can serve as lifelong authentication credentials.

Again, mobile authentication is the one flexible, technology-capable method that **supports all three scenarios**.

Creating Workable Authentication Credentials

To create the easy, secure, reliable user experience necessary to drive mobile transactions to the next level, mobile devices need to be able to successfully manage three key tasks:

Provision and Lifecycle Management

It needs to be easy—and safe—to download and save sensitive personal and financial data onto a phone and make it accessible whenever it's needed. These smartphone credentials must work properly throughout the valid life of the credential and be quick and painless to renew when necessary.

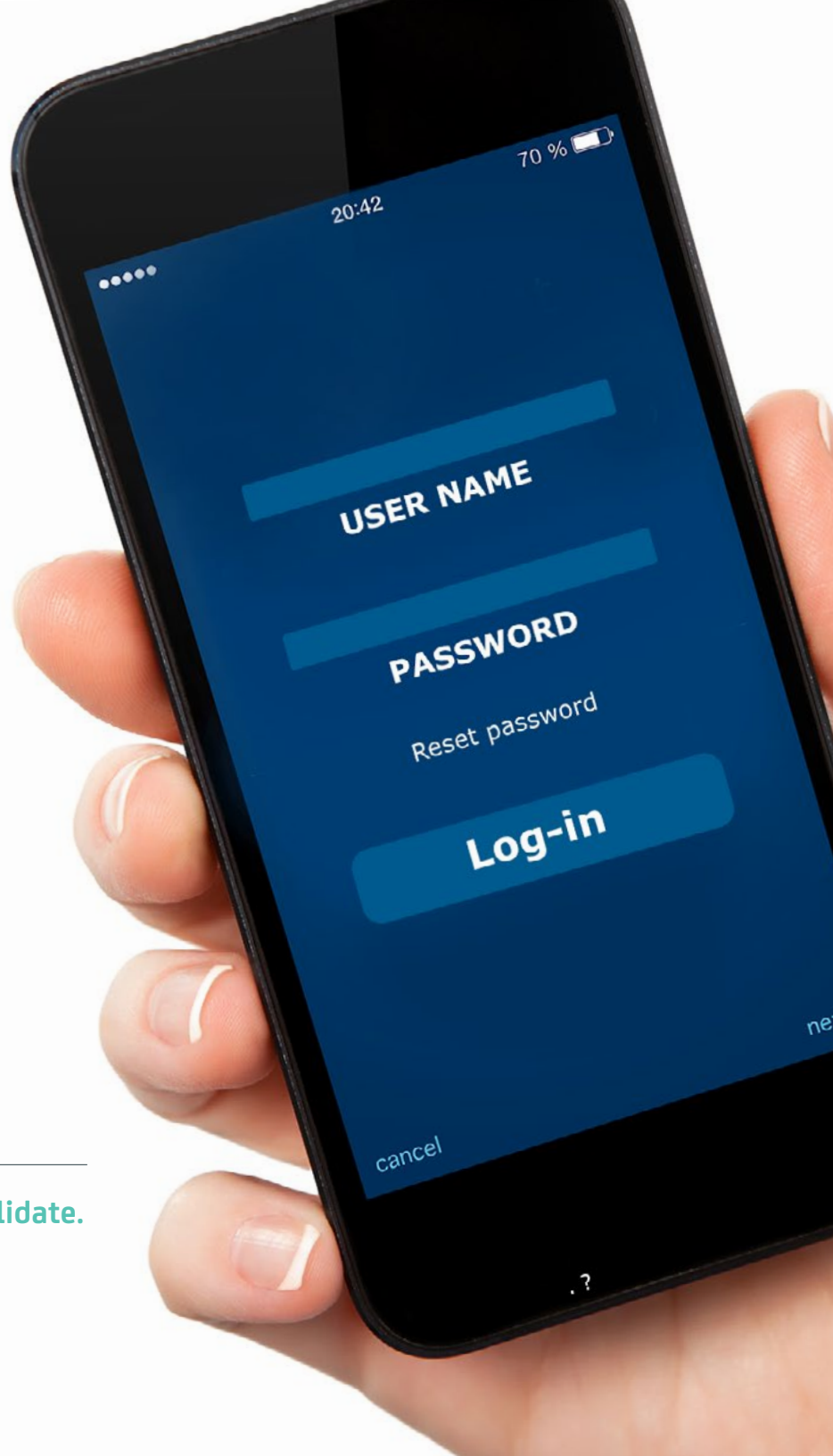
Usage on Demand

Users need to be confident that when they pull out their phone to complete a transaction, everything will go smoothly. Poor cell signals or a lack of Wi-Fi connectivity cannot interfere with the completion of the transaction.

Validation, Reconciliation and Fallback

Users need to be authenticated effortlessly and then provided with confirmation that their transaction was successfully completed. And if their transaction doesn't go through immediately, there needs to be a back-up plan that kicks in automatically to get things back on track.

Once again, smartphones can do it all: **Download, transact and validate.**



Creating Workable Authentication Credentials

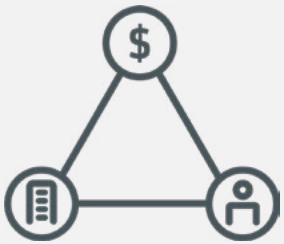
As should be clear by now, not only can smartphones serve as effective authentication credentials, they actually are uniquely suited to the task.

PROVISIONING

With a smartphone, credentials only need to be downloaded once and can be used throughout their lifecycle. Short-term credentials such as boarding passes can be deleted or stored and longer term credentials, such as credit cards reside on the device until they expire.

MULTI-MODE USABILITY

Users can see what's going on with a transaction visually and interact through a direct interface to approve the transaction, add a tip, offer feedback and more. Meanwhile, backend processes are automated and require no user involvement.



USAGE HISTORY IS RETAINED

Users are able to self-audit simply by checking the records on their phone. Charges can be confirmed and errors can be detected immediately.

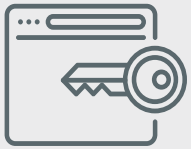
What's Next?

The authentication paradigm is fundamentally changing. The focus is no longer just on keeping the "bad guys" out. **Now, consumers willingly trade more information about themselves for additional security, time and perks**. The TSA Clear program, where travelers submit to a one-time in-depth background check in return for streamlined airport security screening is a perfect example.

1. Provisioning

You need to be able to get your credential

- Personalize and set individual card details
- Verify user and device prior to provisioning
- Support the lifecycle with contingencies for a lost or new phone, new card, profile changes and more



2. Credential Application

You need to be able to use your credential

- Rapid and easy tap-to-pay experience
- Enable or disable the user's virtual card, if required
- Exceptions — error messages for troubleshooting
- Alternate options
- Gaining access to resources: room, building, PC, money

3. Back-end infrastructure

- Validate and verify credential
- Authorize the new payment method
- Deliver confirmation messages or notifications

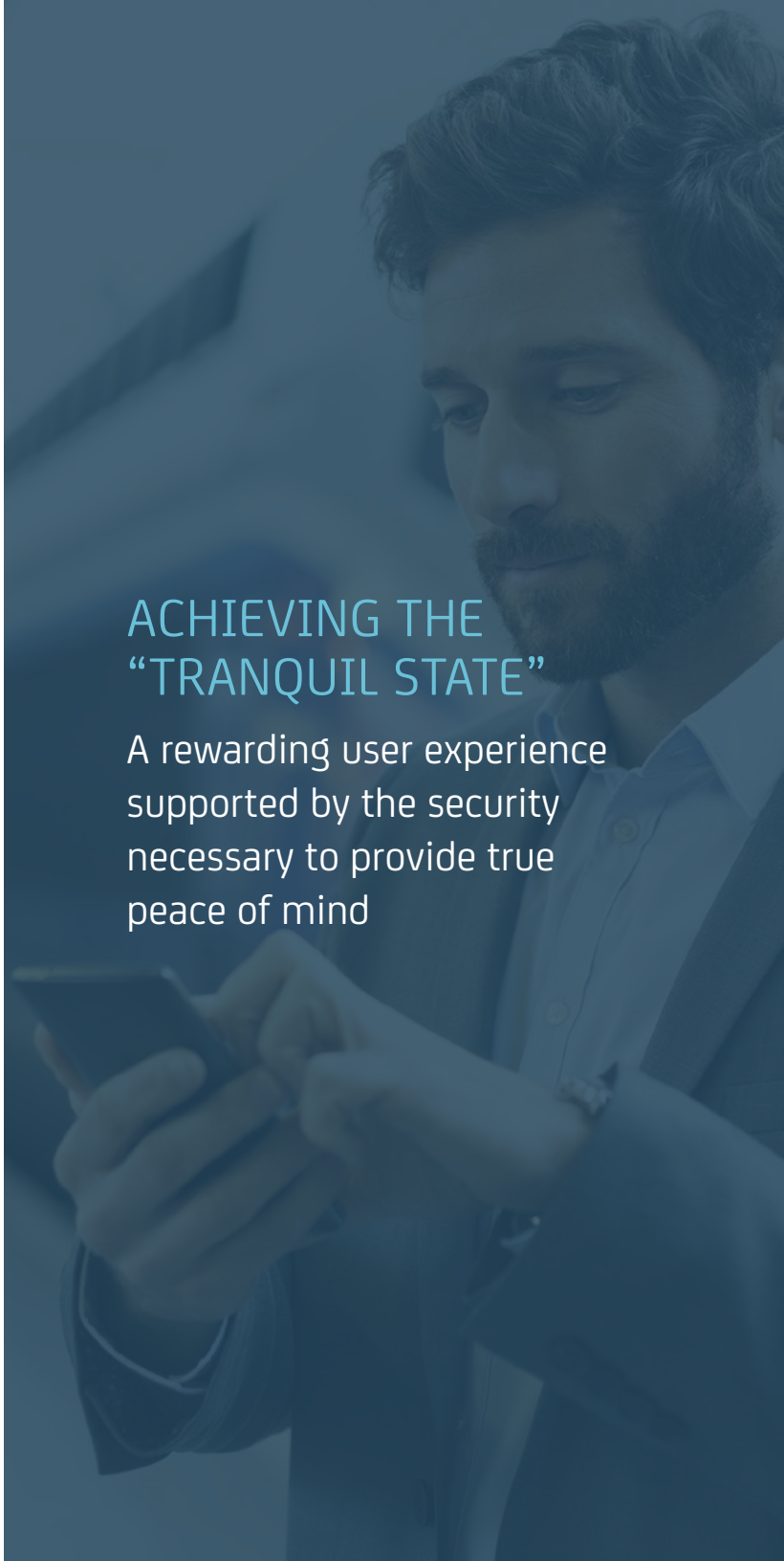
The Ultimate Goal—Frictionless Authentication

Over 95 percent of customers report feeling more **disloyal toward companies** that create a **high-effort mobile experience**.[9] Which helps explain Forrester's prediction that Mobile authentication and security will become increasingly human-factor friendly.[10]

One step you can take today to help reduce friction is to adopt a flexible and scalable solution that incorporates both risk-based authentication using sophisticated analytics, a behavioral neural network model and a flexible set of dynamic rules, as well as a wide variety of multi-factor, strong authentication credentials. The goal is to confirm the user's identity to a degree that does not require companies to make sacrifices that hinder its ability to provide a wonderful user experience for its customers.

Over the past 12 months, mobile payments has seen rapid growth and innovation, ultimately helping consumers become more comfortable with making higher value purchases on mobile devices. A frictionless, "zero-touch" approach to authentication has never been more important than in today's fast-paced and demanding industry. Thanks to the ever-increasing innovative culture of today's leaders, what used to be seen as science fiction is quickly becoming a reality.

[9] Make Service Easy, Salesforce, June 6, 2014
[10] Forrester Research, Inc., Top 15 Trends S&R Pros Should Watch: 2014 (April 18, 2014)



ACHIEVING THE "TRANQUIL STATE"

A rewarding user experience supported by the security necessary to provide true peace of mind

Authentication Solutions From CA Technologies

CA Technologies offers a robust portfolio of advanced authentication and payment solutions to suit every circumstance, including mobile authentication capabilities. Among our offerings are:

STRONG AUTHENTICATION

Deploy and enforce a wide range of strong authentication methods in an efficient and centralized manner. Enable a secure online interaction with your employees, customers and citizens by delivering multi-factor, strong authentication for both internal and cloud-based applications. It includes mobile authentication applications and SDKs as well as several forms of out-of-band authentication.

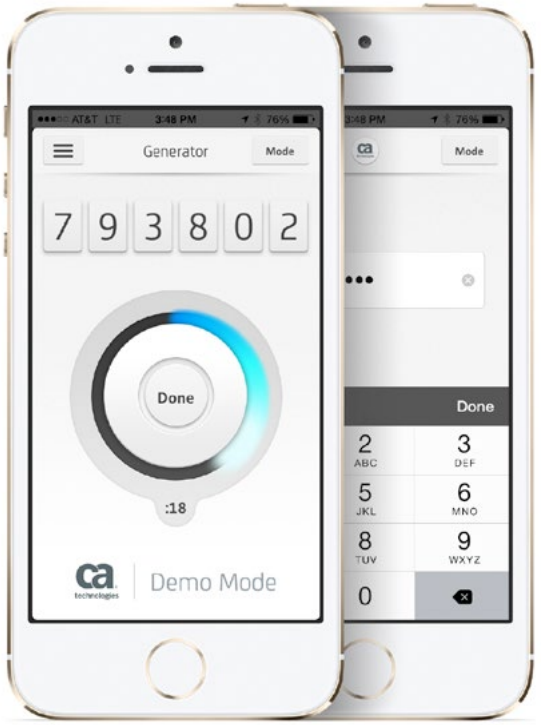
Mobile One-Time-Password (OTP)

Dynamic OTP technology from CA sends a unique, limited-time, single-use password to the user's phone that:

- Simplifies authentication
- Greatly reduces the potential losses due to fraud
- Is SaaS compatible and works with virtually any portal or channel
- Delivers a low-risk, high-gain, universal authentication solution

Mobile Step-Up Authentication

- Combines with OTP to add another layer of security
- Users can opt to receive a SMS, voice or email query when a transaction is initiated
- User must reply to the query and confirm legitimacy to finalize the transaction



Authentication Solutions from CA Technologies

CA RISK AUTHENTICATION

Risk-based rules and statistical analysis detect and block fraud in real-time, without any interaction with the user. You can create an adaptive risk analysis process that calculates the fraud potential of every online login and transaction utilizing contextual factors such as Device ID, geolocation, IP address and user activity information to calculate a risk score and recommend the appropriate action.

CA RISK ANALYTICS

Strike the right balance of security and user convenience with a fraud detection system that transparently assesses the fraud risk of an eCommerce transaction in real-time during authentication. Identify a majority of legitimate transactions to allow customers to continue with their purchase, without impact, using sophisticated analytics, a behavioral neural network model and a flexible set of dynamic rules. Real-time case management provides fraud analysts and Customer Service Representatives (CSRs) with immediate access to fraud data.

CA ADVANCED AUTHENTICATION SAAS

Take advantage of a versatile authentication service that includes multifactor credentials and risk evaluation to help avoid inappropriate access and fraud. It can help you easily deploy and manage a variety of authentication methods to protect your users without the traditional implementation, infrastructure and maintenance costs.

Learn more about how CA is enabling the next generation of mobile authentication:

ca.com/payment-security

.

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at ca.com.

Copyright © 2015 CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. This document is for your informational purposes only. CA assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, CA provides this document "as is" without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or noninfringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, business interruption, goodwill, or lost data, even if CA is expressly advised in advance of the possibility of such damages. The information and results illustrated here are based upon the speaker's experiences with the referenced software product in a variety of environments, which may include production and nonproduction environments. Past performance of the software products in such environments is not necessarily indicative of the future performance of such software products in identical, similar or different environments.

CS200-130570

ca technologies