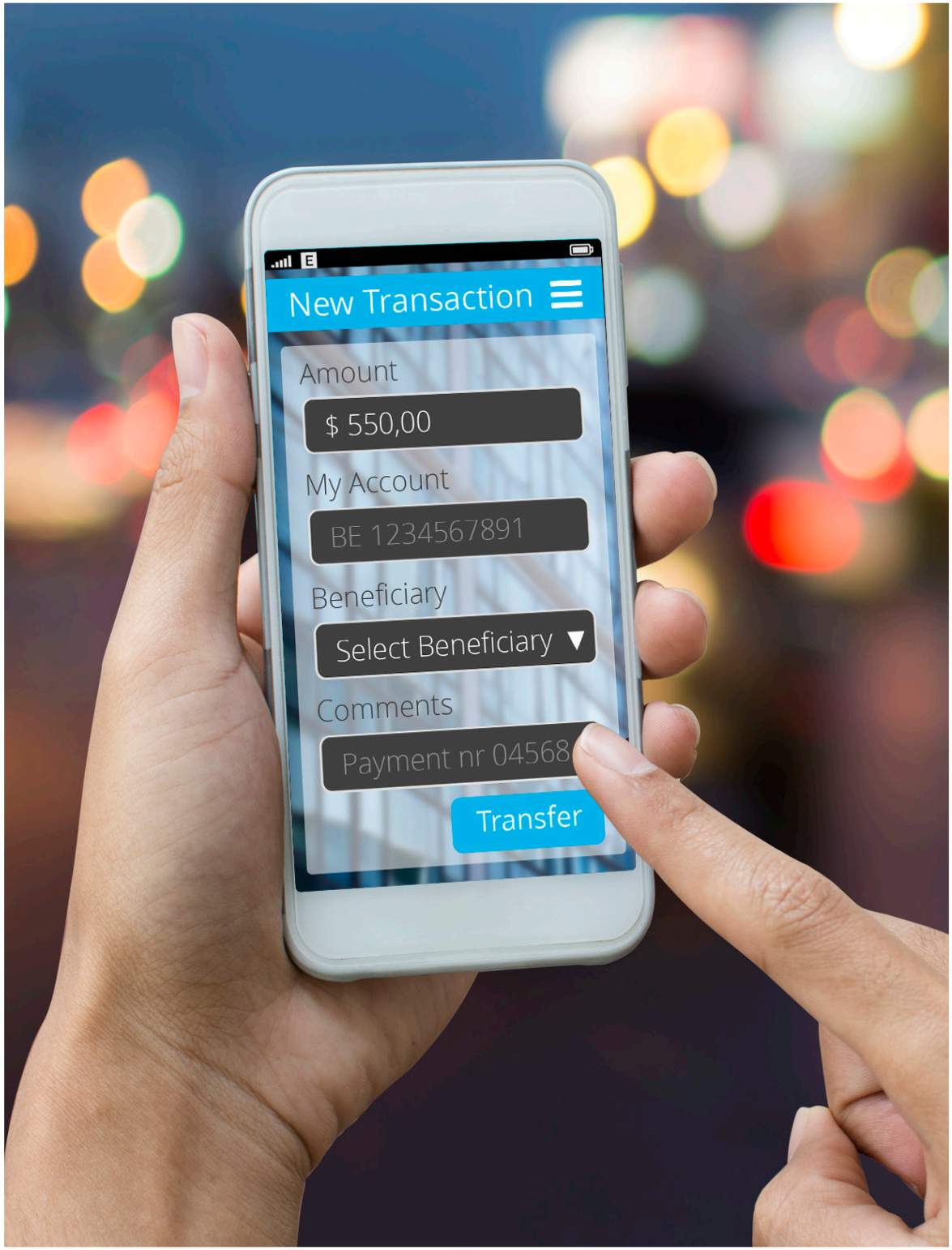


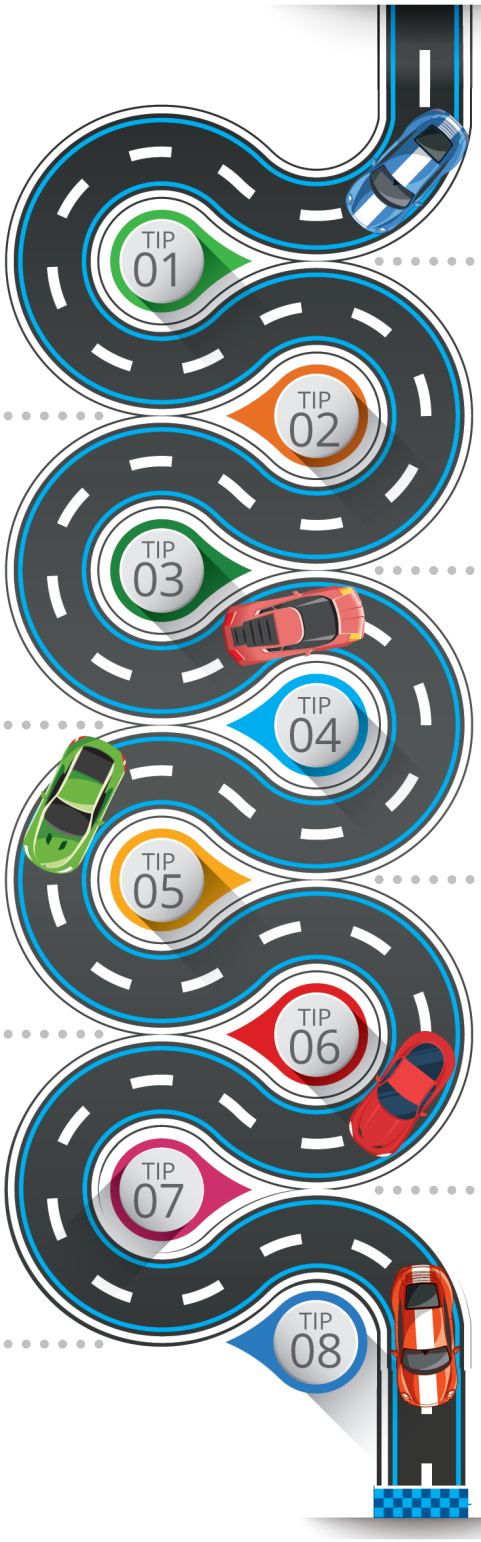
8

Industry Best Practices for a Successful Mobile First Strategy

VASCO®

TRUST FOR THE DIGITAL WORLD

THE ROAD TO A SECURE MOBILE FIRST STRATEGY



QUICK & SECURE LOGIN - PAGE 6

Deploy modern authentication options to support an optimal user login experience

PROTECT MOBILE BANKING APPS - PAGE 10

Attacks on mobile banking apps are increasing both in number and sophistication. Banks need to implement application shielding to detect and mitigate threats.

ADOPT AN OMNI-CHANNEL APPROACH - PAGE 14

Banks seek ways to improve user experience across all channels by using the technological advantages of the mobile platform. This opens new possibilities for real omni-channel banking.

BE READY FOR REGULATION - PAGE 18

With strict and evolving bank regulations in Europe and other regions, banks need to plan ahead and implement future-proof solutions.

PROVIDE A FRICTIONLESS EXPERIENCE - PAGE 8

Provide the most frictionless user experience for your customers without compromising security.

MEASURE RISK ON EACH MOBILE DEVICE - PAGE 12

Detect fraud across multiple channels by implementing multi-layered controls that analyze and score user, device and transaction data.

COMBAT SOCIAL ENGINEERING AND OTHER THREATS - PAGE 16

Social engineering remains a big threat across channels, including mobile. Deploy proven security technologies to protect your customers against these attacks.

SIMPLIFY DOCUMENT SIGNING - PAGE 20

Drive growth and reduce costs by making it easier for customers to securely sign documents anytime, any place, on any device through any channel with e-Signature solutions.

Introduction: The Accelerator for Mobile is Trust

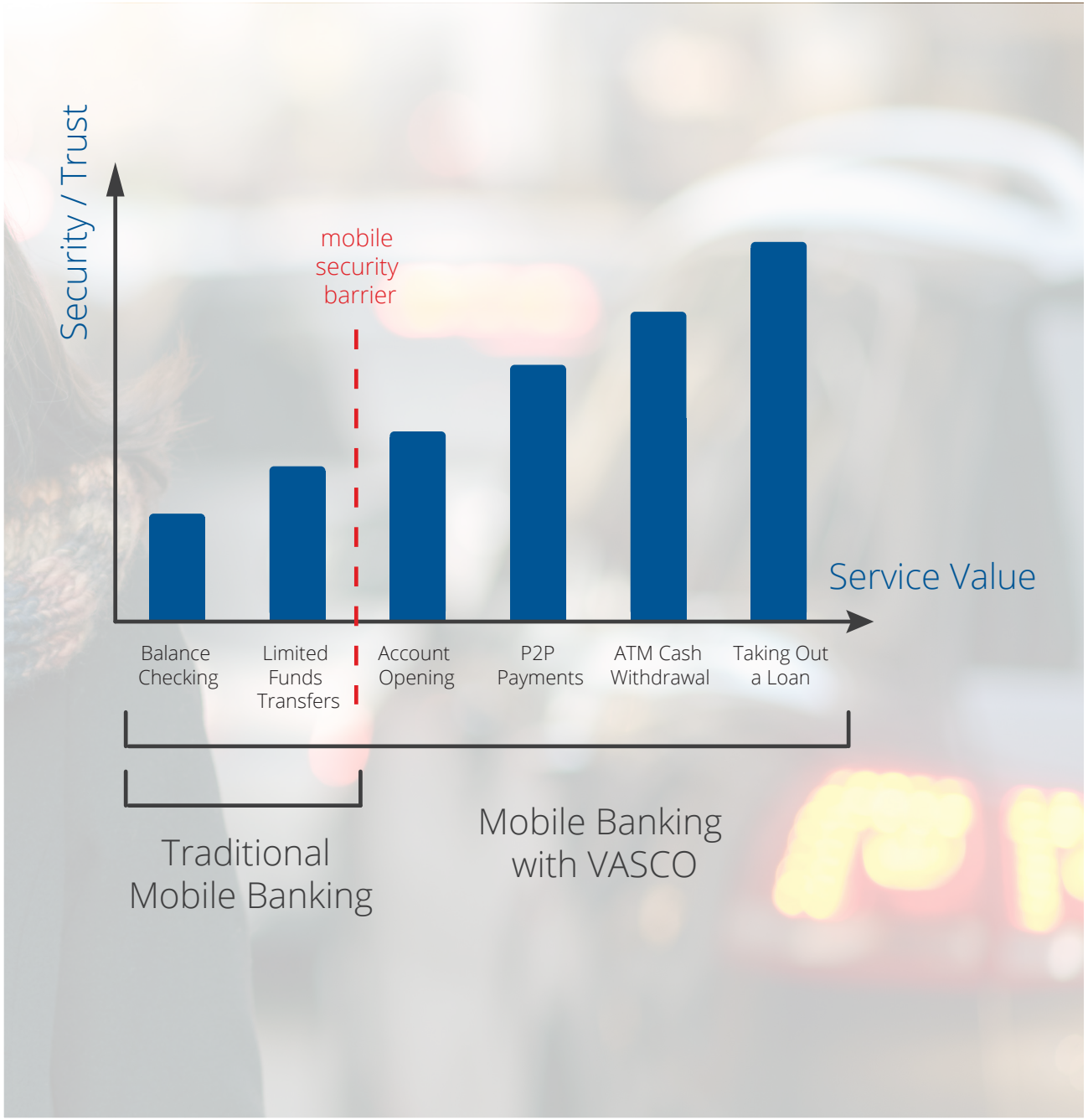
What's Missing from Mobile

Financial institutions strategically aim for customers to do more with mobile while minimizing fraud exposure tied to untrusted, high-risk devices. To enable growth in the mobile channel, financial institutions need to provide fast, convenient and frictionless high-value services delivered as securely and fraud-proof as possible. To achieve this goal, building more trust is Priority One.

Offer Mobile Customers a Trustworthy Service

Banks strive to meet mobile users' expectations and many customers try basic services via mobile that don't require a high level of trust. Services like checking balance and limited fund transfers. Long term, however, mobile banking customers want more than just basic services. Many, in fact, are waiting for banks to step up and prove that offering high value banking services via mobile can be made trustworthy enough to earn their business as well as their loyalty.

More Trust Triggers More High Value Mobile Service



Framework for Trust
Before banks can crack consumers' psychological apprehension regarding mobile security, they must address technical issues that are unique to mobile. Banks need to see mobile security as a complete picture, to create a dedicated, multi-layered and up-to-date strategy focusing on mobile security.

For this reason, VASCO's solution for mobile-oriented strategies:

- **Secures mobile devices** to protect customers and their devices
- **Secures communications & applications** to mitigate hackers' and fraudsters' malicious attacks.
- **Analyzes behavior, context and risk** to increase visibility of bad actors and reduce risk across mobile devices

Quick Start to Success
This e-book describes eight ways to successfully approach a Mobile First Strategy. Each principle describes the business requirements, suggests an implementation strategy, and explains how VASCO can help.

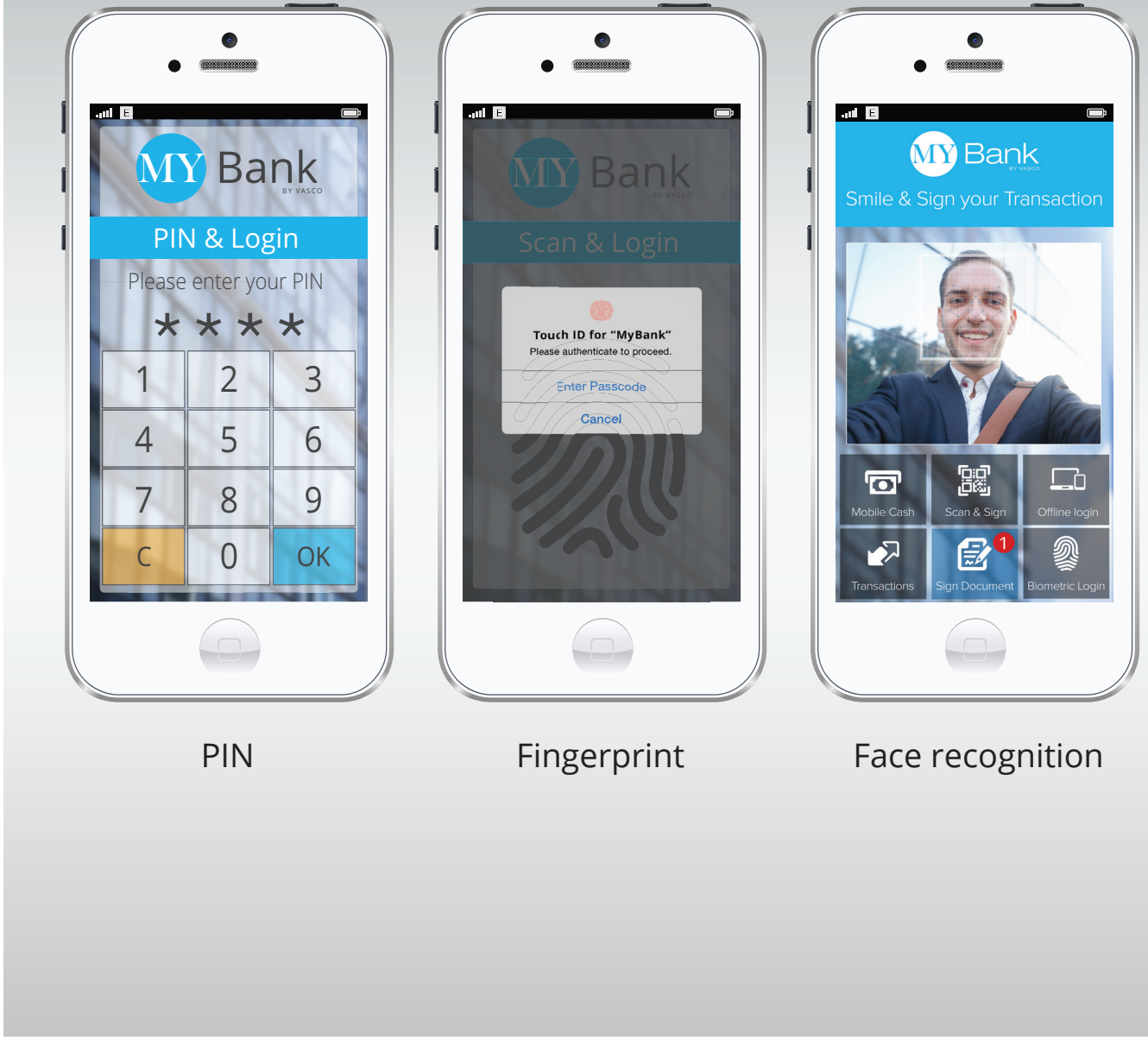
Quick & Secure Login

TIP 01

Faster Login, but is It Secure?
Banks need simple, quick, but secure authentication.

While mobile banking customers' preferences vary somewhat by generation, for the most part, customers want a secure, frictionless mobile experience that gives them the ability to utilize more services using their mobile device. With this convenience, banks have the ability to supplement basic services with more high-value, services that can attract new customers and better retain existing ones.

Implementation Strategy
Banks strive to provide faster, convenient logins by replacing complex passwords with simple PINs, fingerprint scanning or other biometrics. While banks need convenient options, if they are not implemented correctly, they will not be secure. As a result, banks need an underlying security framework to make PIN as well as biometric authentication options secure.



VASCO Solution for Fast & Secure Login

VASCO offers a strong platform for fast and secure login to banking apps. The platform provides banks with a trusted approach to mobile login with quick, secure integration of multi-modal biometrics and multi-factor authentication.

Our solutions enable you to easily integrate not only modern multi-factor and biometric authentication capabilities but also application security directly into any mobile application.

By using a single framework, banks can add new functionality in a fast, cost-effective and secure manner. User-facing security options like PIN, fingerprint or face recognition can easily be added, changed or combined to provide the right level of security for each transaction while increasing user convenience and loyalty.

Provide a Frictionless Experience

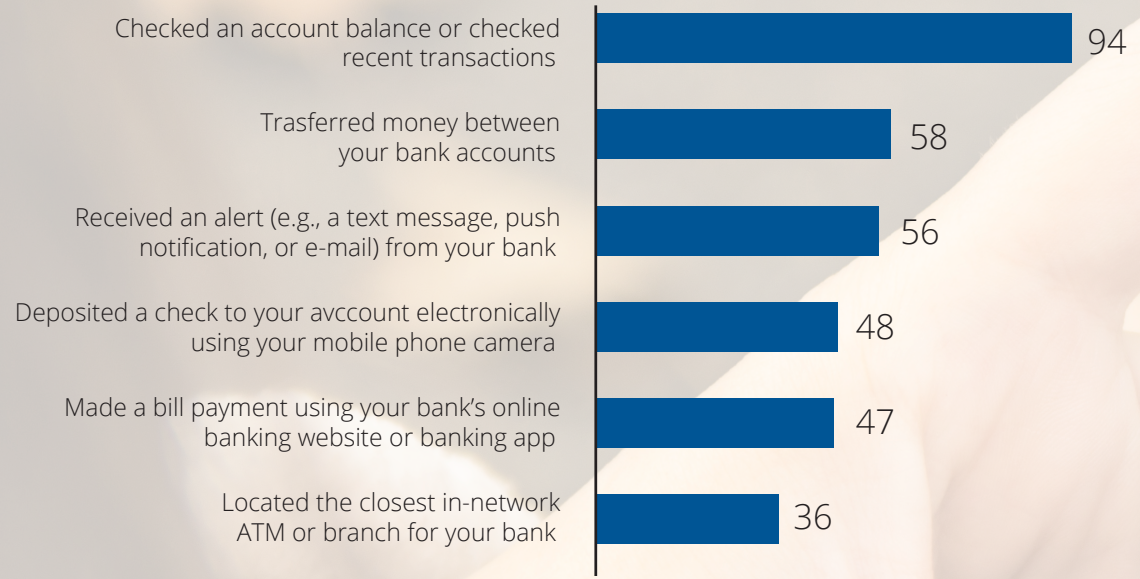
TIP 02

No Experience is the Best Experience
Friction dampens consumer enthusiasm for mobile banking as the login and authentication stage is where delay most often occurs. While most consumers are used to clicking through multiple screens to complete an action on a desktop, they expect their mobile banking to be a much more simple experience.

The chart included here emphasizes the low risk nature of most consumers' interactions on mobile devices (e.g. checking account balances or reviewing recent transactions). Reduced friction enables these rapid and repetitive actions, while providing a positive user experience.

Implementation Strategy
Your mobile banking app and supporting IT will use multiple security technologies for securing devices and communication. Look for ways to tie these processes together without requiring extra actions by customers. For example, a mobile device can authenticate itself when a new session is started. As a result, subsequent application authentication and transaction signing can occur invisibly, regardless of platform. In addition to device authentication, the latest behavioral authentication technology is another frictionless option that should be considered.

Using your Mobile phone, have you done each of these in the 12 past months?



Source: Source: U.S. Federal Reserve, Board of Governors, Consumers and Mobile Financial Services Report, 2016

VASCO Solution for a Frictionless Experience

Our integrated solution components enable banks and financial institutions to offer their users a frictionless experience. These include:

Device Authentication
Device authentication prevents cloning or repurposing of cryptographic keys while leveraging unique attributes of the device to provide a persistent identification that deafeats hackers' attempts to spoof the mobile device.

Contextual Authentication
Analyzing and scoring user, device and transaction data via server side machine learning, enables the real-time ability to throttle up or down security based on the unique risk of each transaction. This means that banking customers will always have the best possible experience with bank services across any channel.

Behavioral Authentication
VASCO's behavioral authentication solution provides an invisible security layer that continously authenticates end users by the unique ways they interact with their mobile device via keystrokes, swipe patterns and more.

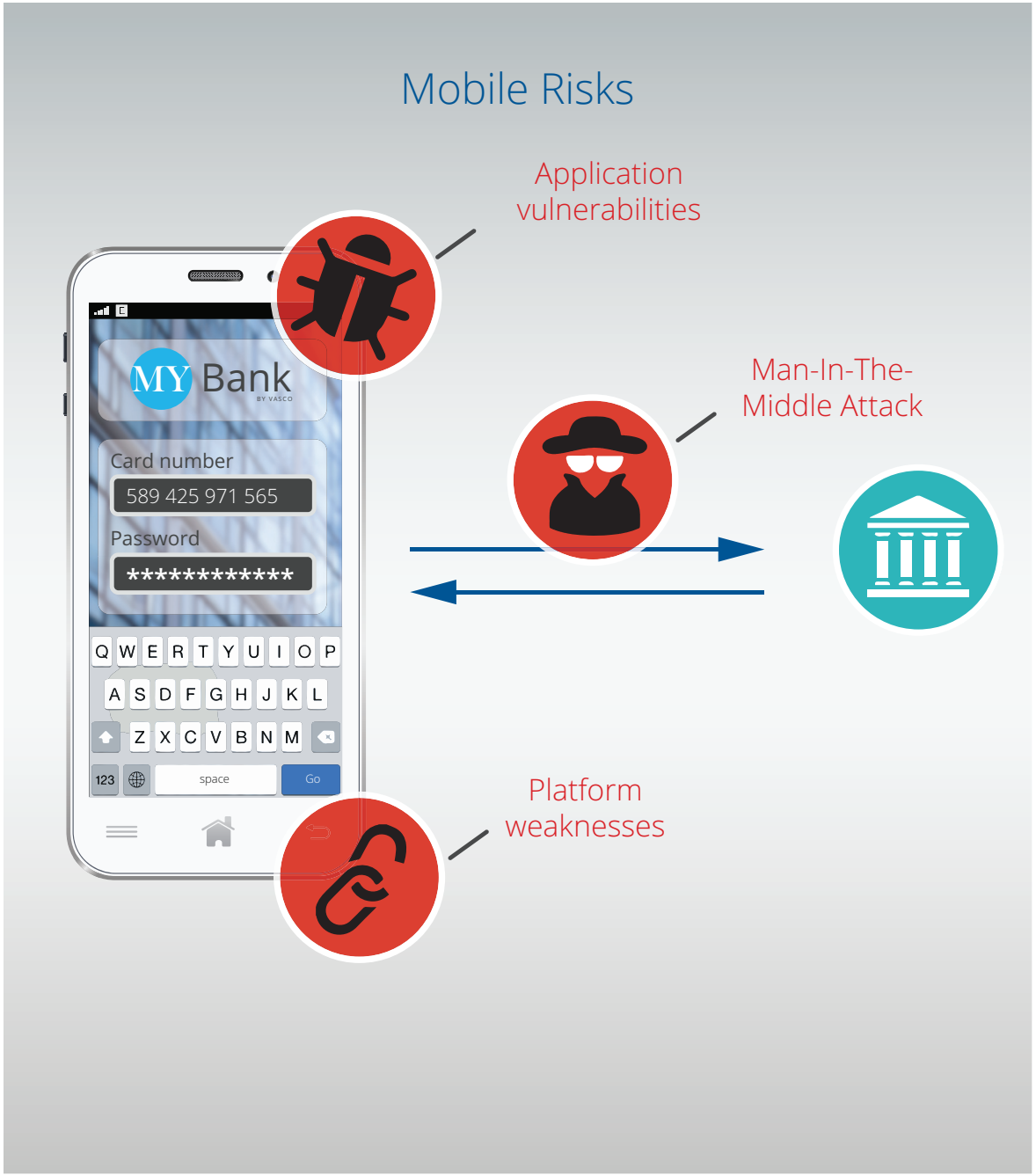
Protect Mobile Banking Apps

TIP 03

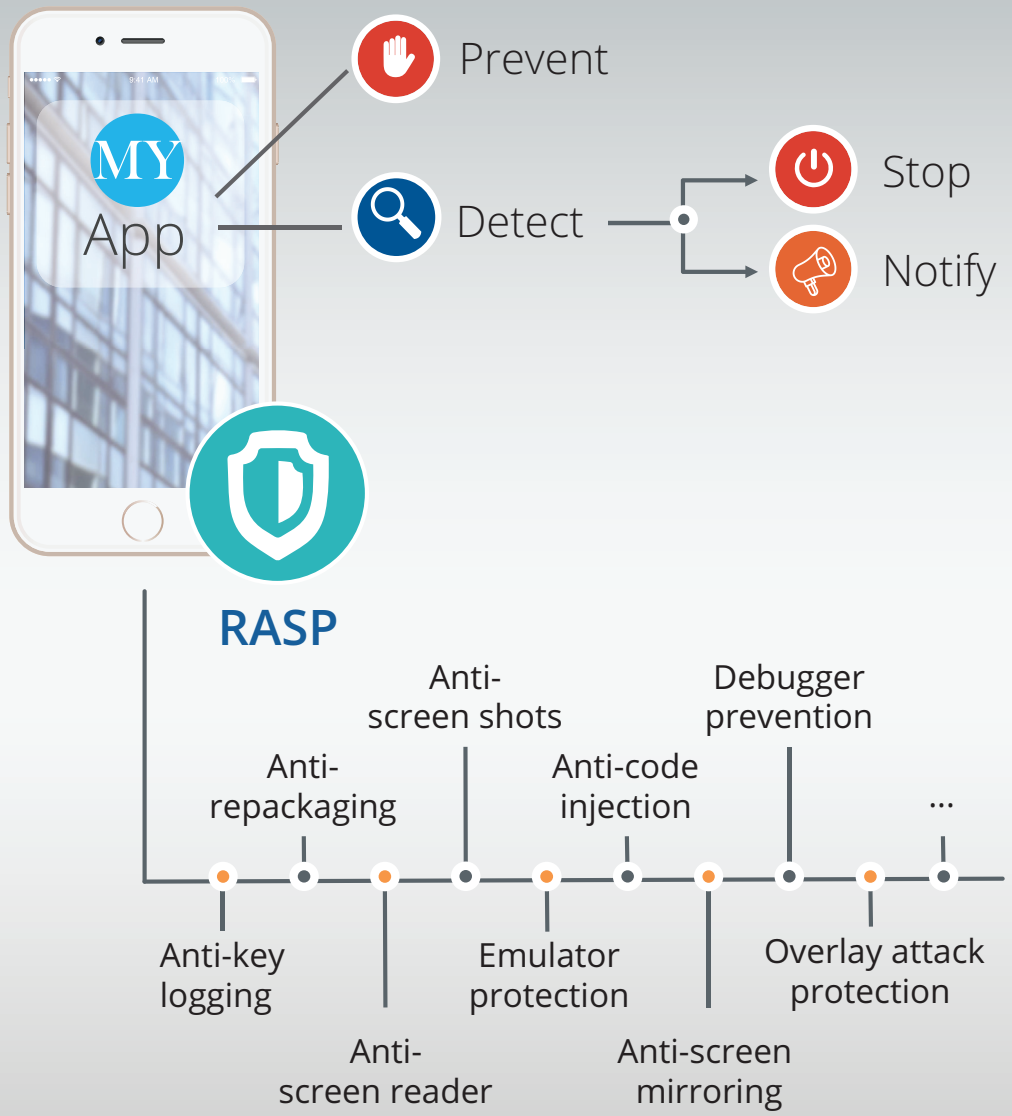
Keeping Up at the Cost of Insecurity
The increased popularity of mobile banking has created a highly competitive and challenging environment, especially among mobile app developers. As a result, releases are often rushed, creating vulnerabilities in the application layer.

The Threat from Mobile Banking Malware
The potential for malware in banking apps is well documented. In fact, these attacks are growing in both number and sophistication. The BankBot Android mobile banking malware, for instance, targeted over 420 leading banks in countries such as Germany, France, Austria, the Netherlands, Turkey and the United States. Using a technique known as overlay, the malware allows attackers to create windows that sit on top of legitimate Android applications and intercept user information that can compromise transactions and privacy.

Implementation Strategy
From an implementation perspective, it's important to harden the app via Runtime Application Self-Protection or RASP. This keeps the app (and your backend systems) safe even when the app is running on devices with disabled OS protection, or devices already infected with malware. For example, in the BankBot malware instance, if RASP determined the app was at risk of an overlay attack, it would shut down the app and open a browser to notify both the IT admin and the end user that an attack occurred.



VASCO Solution to Protect Mobile Banking Apps



VASCO's Runtime Application Self-Protection (RASP) is an advanced mobile application shielding technology. It operates in the full context of mobile app security: preventing, detecting and remediating malicious activities directly attacking your mobile application. It can be built in (or simply linked to) an application or its runtime environment, making it more resistant to know and yet unknown security threats.

VASCO's Application Shielding with RASP creates a shield around the application code, allowing it to operate safely even if the user's device has been infected with malware. It proves effective against threats like tampering, reverse engineering, code injection, code modification or data theft from the app. Additionally, it provides a generic protection against mobile overlay attacks from different malware families. It is one of the most significant threats in the recent years, targeting customers of hundreds of banks worldwide.

While Application Shielding with RASP delivers security from so many angles, it doesn't affect the customer experience: the protection is invisible for the end user and does not require changes in operating system, user's permissions or frequent updates. VASCO's Application Shielding with RASP is very easy to integrate as most of the integration is automated, however, due to very deep binding mechanisms, it becomes an difficult task for hackers to remove RASP shield from the application.

Measure Risk on Each Mobile Device

TIP 04

Enable Multi-Layer Controls

The foundation of strong security is multi-layer controls. If a hacker manages to thwart one layer, other controls mitigate malicious activity. Among these are technologies that analyze each mobile device and associated behaviors of its user while engaged with a mobile banking app.

Implementation Strategy

The goal is to score the risk of each device and provide actionable data for implementation of policy when critical thresholds are too high. For example, unpatched versions of OS or app software carry more risk. So does use of an unknown public Wi-Fi network, a new password, or new biometric factor. Analytics and scoring must automatically occur in real-time to ensure strong security.

VASCO Solutions for Measuring Risk

VASCO's real-time fraud analysis solution for mobile helps banks meet strict compliance requirements while improving the speed and accuracy of fraud detection. This solution provides an efficient anti-fraud system to your existing mobile banking offering that can be achieved with minimal integration cost and time. Our expertise in the mobile ecosystem and fraud prevention is available in an instant, eliminating the lengthy process competing technologies require to achieve efficient and accurate fraud detection.

Our mobile fraud analysis solution identifies risk at critical steps and acts instantly when fraud patterns are identified. Working silently in the background, the solution collects and scores user behavior, device integrity and transaction data to drive the right level of security for each unique transaction, stepping up security only when required. Banks can enhance their current fraud capabilities by adding our risk analysis solution to gain better line-of-sight and ultimately drive down fraud across all digital channels.

Adopt an Omni-Channel Approach

TIP 05

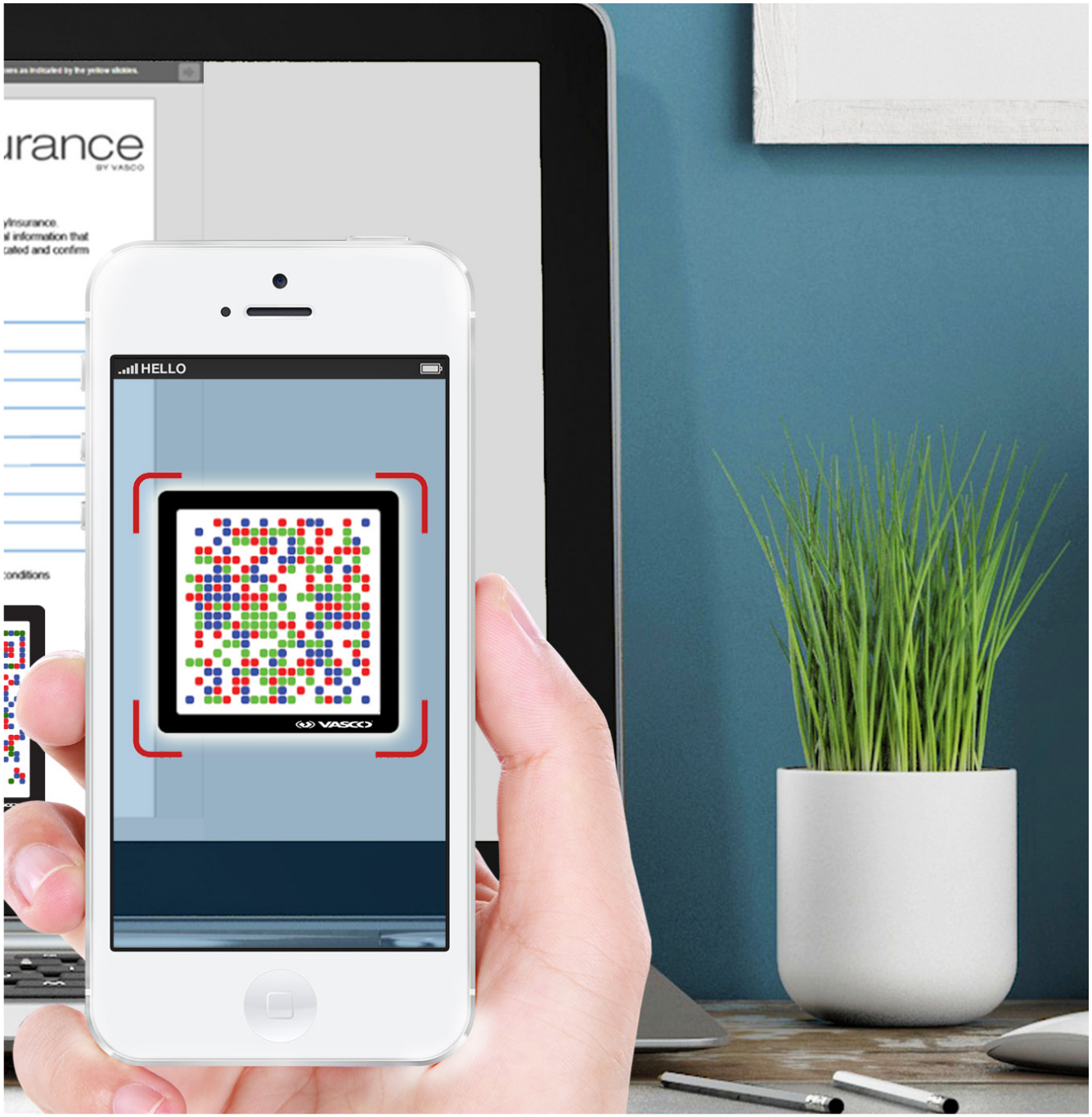
Ensure Simplicity with Mobile

To stay competitive you need to seek ways to achieve a great user experience across channels – including mobile. The challenge for customers is that different channels often require different ways to prove user identity and to authorize operations. Differences can lead to friction and frustration. Using an omni-channel approach optimizes security without impacting usability.

Implementation Strategy

Look for ways to eliminate friction by injecting a simple, intuitive experience with fewer required interactions. Examples include scanning a secure image instead of typing a username, challenge or password or performing similar actions to sign transaction data. Also, consider how to streamline processes for customers who do not use a mobile phone.

VASCO's solution for a multi-channel approach



Customers look for a seamless and consistent banking experience no matter what channel they are using to access their accounts. Omni-channel customer engagement has become a top priority for banks.

Our Scan & Login solutions enable fast adoption and brings both safety and simplicity to banking users when signing online transactions in various channels like internet banking and ATMs.

Using our Push Notification technology, banks can re-use our single security solution for out-of-band authentication or transaction signing. Push notification makes account sign-in & identity-proofing easier than ever.

These solutions are designed to support modern omni-channel environments, enabling banks to more holistically address fraud and optimize the user experience regardless of how, when or where their customers choose to use applications and services.

Combat Social Engineering and Other Threats

TIP 06

Protect Customers from Risky Decisions
Phishing and other types of social engineering by hackers work because most people have a natural human tendency to trust. Hackers exploit this trust to steal valuable information such as usernames, passwords, credit card numbers or other sensitive data.

Many banks have responded with tougher security for users. Even with education and additional user controls, however, phishing is still successful. The simple reason is that the final decision to complete a transaction is made by the user who authenticates to the bank, not vice versa.

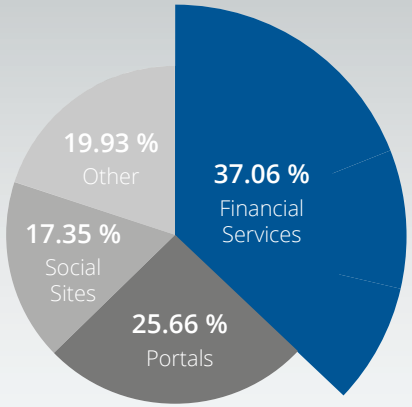
Implementation Strategy
Today, however, social engineering is not limited to email solicitation.

Vishing – where a victim is manipulated by phone into disclosing confidential data, which can then be used for fraud, is also on the rise.

When it comes to combating social engineering schemes in the banking industry, a signature should be generated only for requests known by the bank. The mobile device should automatically reject requests not coming from the bank. And there should be no way to generate a signature without an interaction with the bank.

VASCO Solution to Combat Social Engineering

Types of organizations affected Q1 2015



Spear Phishing

70%

open rate, compared with a 3% open rate for mass spam emails

Voice Phishing ("Vishing")

23%

of people in the UK have received a cold call requesting personal or financial information

39%

admitted they found it hard to tell the difference between a genuine and fraudulent call

VASCO provides several solutions that protect customers from increasingly sophisticated Social Engineering attacks.

Social Engineering attacks have evolved dramatically over the years, making every person susceptible. The best approach to reduce the human risk in banking fraud is to make the bank the sole initiator of a transaction signature request.

VASCO's CRONTO solution has been designed to thwart social engineering and phishing attacks by taking the "trust" decisions out of the hands of the user, and ensuring only the bank can initiate a transaction signature request.

CRONTO shifts transaction authorization controle from the user to the trusted device and the bank.

This is the ideal solution for high value transactions that require strong security that protects against fraud through Phishing attacks, Trojans, Man-in-the-Middle (MitM) and Man-in-the-Browser (MitB) attacks.

Be Ready for Regulation

TIP 07

New Rules for Mobile Banking Security
Due to global payment fraud, the banking industry is one of the most heavily regulated, and more regulations are on the way. For example, in the EU, the new Payment Services Directive 2 (PSD2) will be effective beginning January 2018. It regulates the security of electronic payments – including mobile banking and retail payments' security – and establishes a minimum security level for payments in the EU.

Compliance requirements include:
- Confidentiality/integrity/authenticity of payment verification
- Strong customer authentication
- Device and app protection
- Transactional Risk Authentication

Other regulations such as GDPR and PCI-DSS require multi-factor authentication to protect data or access control.

Implementation Strategy
Deploy solutions that fulfill requirements of PSD2 and other similar regulations. Use technology to automatically implement security requirements for compliance.

VASCO Solution to Address Strict Regulations

Our security experts and proven solutions ensure that your bank meets or exceeds evolving regional regulatory requirements.

A broad portfolio of strong and easy to deploy authentication solutions, including leading biometric and other multi-factor authentication options are designed to help you meet requirements fast. Biometric options include fingerprint scan, face recognition and behavioral biometrics. Additionally, our fraud management solution satisfies risk-based authentication and profiling requirements.

Many regional and global regulations require the use of multi-factor authentication such as PSD2 (Europe), NDI (Singapore) and PCI DSS (Global). Other regulations such as GDPR (Europe) , NIST (US) and FFIEC (US) strongly recommend the use of biometrics.

Specifically for eIDAS regulations we also provide a compliant e-signature solution.

With respect to AML requirements, VASCO delivers a proven transaction monitoring solution. Through a combination of tailored rule sets and Machine Learning, our solution provides real-time analysis of each unique transaction to quickly approve low risk transactions, decline high-risk transactions, or flag transactions for manual review based on established policies.

Electronic Document Signing

TIP 08

Removing Paper from Business Processes
As digitization efforts mature and organizations realize the benefits in customer experience, compliance, productivity and hard cost savings, they are looking for ways to rapidly extend those benefits to every business line, channel and area of the organization.

This requires an electronic signature platform that has the flexibility to accommodate the requirements of any business process and can be implemented across any channel – online, the call center, the retail branch and mobile. E-signatures allow employees to securely send and manage document-based transactions, while ensuring customers can quickly and easily sign documents – anywhere, anytime and on any device.

Implementation Strategy
Mobile has become the central access point for digital transactions because it provides a level of freedom and flexibility that wasn't available just a decade ago. If your mobile experience includes paper and pen-and-ink signatures at any point during the transaction, it isn't a fully digital one. E-signatures help keep business processes completely digital by eliminating the need to drop to paper to complete contracts, open accounts and sign off on documents.

VASCO Solution for Secure Document Signing

VASCO Solution for E-Signature
VASCO's eSignLive balances high-levels of security and compliance with ease of use. Our e-signature solution allows banks to automate any process – from the simplest, internal signing workflows to demanding, high volume customer-facing transactions.

By implementing our e-signature solution in your mobile channel, you can deliver mobile-optimized signing experiences to your customers when accessing documents through a mobile device or web browser. Leverage our out-of-the-box e-signature mobile apps or integrate e-signing capabilities into any mobile banking app using our mobile SDKs for iOS and Android. Additionally, you can add strong authentication such as fingerprint and facial recognition biometrics to the e-sign process.

Your brand matters in the mobile world. Our solution can be fully white-labeled, ensuring your brand is front and center at all times to provide a trusted and seamless customer experience.

Conclusion: Focus on Your Core Business

VASCO helps banks to apply the 8 tips in this e-book to create seamless and secure mobile banking experiences for their customers. By designing holistic solutions based on trust at every level, VASCO allows you to focus on your core business objective: helping your bank to acquire new customers and delight existing customers with high value services.

We deliver the strongest and most cost-effective suite of security solutions trusted by more than half of the world's largest 100 banking institutions. Proven technology drives compelling results. Ask how VASCO can help make your Mobile First strategy a success.

About VASCO

VASCO is a global leader in delivering trust and business productivity solutions to the digital market. VASCO develops next generation technologies that enable more than 10,000 customers in 100 countries in financial, enterprise, government, health care and other segments to achieve their digital agenda, deliver an enhanced customer experience and meet regulatory requirements. More than half of the top 100 global banks rely on VASCO® solutions to protect their online, mobile and ATM channels. VASCO's solutions combine to form a powerful trust platform that empowers businesses by incorporating identity, fraud prevention, electronic signatures, mobile application protection and risk analysis.

Trusted by Leading Brands Worldwide

+250.000.000 devices sold | +10.000 companies
1.700 financial institutions | in +100 countries

Bank of America
HSBC
Garanti
VASCO
TRUST FOR THE DIGITAL WORLD
Santander
CONSUMER BANK
MIZUHO
Deutsche Bank
eSignLive™ by VASCO®
Rabobank
KBC
MUFG

Contact Us

For more information please visit www.vasco.com
or contact us through one of the following methods:

www.vasco.com/contact - info@vasco.com

VASCO®
TRUST FOR THE DIGITAL WORLD

BR201712 - v1