Mobile Banking Applications
Balancing Security and Convenience
Table of Contents

Introduction 1

Comprehensive Security for the Mobile Channel 5

Mobile Application Security 6

Multifactor Authentication 8
Introduction

Today’s financial services institutions compete for market share while faced with an increasingly complex challenge of balancing opposing forces. On one side of the equation, they must satisfy escalating demands from mobile banking customers who want instant anytime/anywhere access, uncompromised convenience, and user-friendly functionality on all devices. At the same time, banks must protect customer information and transactions from a daunting cadre of malicious perpetrators who view the mobile ecosystem as an irresistible target of opportunity. Digital thieves continue to morph their practices in order to maximize profitability and minimize detection. Cyber attackers are exploiting mobile application vulnerabilities, launching sophisticated fraud schemes, and stealing sensitive data. How can banks deliver the “cool” apps required to lure selective mobile customers and grow the business in an ecosystem fraught with risk?

The world’s leading financial institutions are adopting “Mobile First” strategies to leverage the game-changing platform that has revolutionized banking and become the customer’s channel of choice. But while mobile presents enticing business opportunities, it also stretches the boundaries of the threat landscape, dramatically expanding the attack surface. Vulnerabilities in mobile applications can expose a bank to data loss, fraud, and damaged brand reputation. Attacks are on the rise. Nearly all Android finance apps were hacked in 2014. Yet, two-thirds of fraud attacks remain undiscovered, and it is end users—bank customers checking their account statements—who typically discover the one-third of attacks that eventually rise to the surface.

Savvy banks understand that mobile application security is not their core business. Successful financial institutions will encourage their valuable software developers to focus less on security and more on designing the innovative features and high-value banking services that will maximize return on investment and propel competitive advantage. Intelligent business and security leaders will choose to partner with a player like VASCO, positioned to deliver the comprehensive threat expertise and protection banks cannot efficiently maintain in house and will not find elsewhere. VASCO protects the mobile platform from evolving threats, enabling banks to securely and rapidly develop and deliver new and enhanced offerings for the mobile channel.

“Tackling Internet fraud is an ongoing battle. HSBC Brazil is therefore committed to providing its customers with the highest level of security. By deploying an authentication solution based on social security numbers in combination with DIGIPASS for Mobile, we are able to provide secure m-banking services in a convenient and cost effective manner.”

Marcello Veronese, Head of One HSBC Distribution, Latin America.
Enhancing Protection without Sacrificing Market Share

Investing in and delivering banking services on mobile devices is smart business. It’s a core component of every successful bank’s growth strategy, given the potential revenue opportunities and the mobile channel’s promise of attracting and retaining the next generation of customers. Today’s consumers are addicted to mobile convenience. Account holders engage with their banks via mobile and online channels 30 times per month, on average, and visit a branch only one or two times a year. A robust and secure mobile application enables customer engagement, increased transaction volume and lower costs.

“A bank’s average cost per transaction ($4.25 at a physical branch) is reduced to 10 cents on a mobile device.”

How to Modify Mobile Banking Behaviors to Maximize Cost Savings

However, the risks embedded in mobile banking are real… and formidable. Mobile apps are exposed to additional exploitation due to the open nature of the mobile platform. Financial institutions walk the tightrope trying to establish a balanced position while being pulled in different directions. To cite one example, many banks are taking a bath in financial losses associated with fraud connected to remote capture deposits. According to the U.S. Federal Reserve, more than 50 percent of U.S. mobile banking users deposited a check using a mobile phone in 2014. The banks are essentially forced to absorb the cost of this vulnerable service in the interest of winning and keeping mobile banking customers who have a lot of banking choices in a fiercely competitive marketplace. More than 60 percent of U.S. smartphone and tablet users reported that mobile banking capabilities are the most important driver in their decisions to switch banks.

“Concerns about security continue to be one of the main impediments to consumer adoption of mobile financial services.”

Consumers and Mobile Financial Services Report 2015
Outlined below are just a few of the prevailing known threats in the mobile environment. There are hundreds of others… not to mention the countless number of undiscovered threats.

**Social Engineering Schemes**
Social engineering preys on the natural human tendency to trust. Hackers masquerading as legitimate entities use manipulative phishing emails to direct unsuspecting bank account holders to spoofed websites where they divulge confidential information, including login credentials, which attackers then use to compromise online accounts. Voice phishing (vishing) specifically targets the mobile channel. In 2014, UK bank customers alone lost £24 million from vishing attacks. Fraudsters pose as bank employees, requesting payment card data and credentials via phone or text message (SMiShing). The data is then used for online shopping or encoded into new cards used by criminals. Hackers can convince users to authorize fraudulent transactions without a bank’s involvement. The financial institution typically has no control over the authorization decision, which is why phishing continues to be such a successful tactic.

“Social engineering attacks undermine consumer confidence in a bank’s brand, put customers at great risk of financial loss, and collectively cost the financial industry countless millions of dollars every year.”

VASCO Blog
Losses associated with security incidents in the finance sector increased by 24 percent in 2014, per a PricewaterhouseCoopers survey. According to Verizon’s annual Data Breach Investigations Report, in the first quarter of 2015, more than 35 percent of phishing exploits targeted financial institutions. Gartner estimates that theft through phishing activities costs U.S. banks and credit card issuers an estimated $2.8 billion annually. In social engineering attacks, the user is the weak point, but the bank is the ultimate target. Banks need better ways to mitigate the potential damage of these attacks.

“The goal of these actors in the black markets is to make money for the least amount of effort with the highest probability of success. That means going after the weakest systems.”

Top 5 Security Threats Banks Will Face in 2015

Reverse Engineering Schemes
When a user downloads an app, it is in binary code format. If steps have not been taken to protect this binary code, the app is susceptible to reverse engineering. Many readily available tools help hackers reverse an application from binary format into source code, which then gives them access to sensitive data. Also, the code can be modified (removing security controls, for example), targeted attacks can compromise the integrity of runtime behavior, and/or malicious code can be injected into the application. Once tampered with, an application can be repackaged and circulated to look as though it originated from a known/safe source. Apps are extracted from an online store, for instance, injected with malware, and redistributed to victims. Rogue apps looks like “real” mobile banking apps but unleash a cascade of fraud and theft via untraceable prepaid cards and many small transactions that often remain hidden under the radar.
Comprehensive Security for the Mobile Channel

Constantly evolving mobile fraud in the banking arena requires strong and constant surveillance. No single point solution can address the inherent complexity of today’s threat landscape or all potential weaknesses in a financial institution’s mobile platform. In addition, many currently available mobile app security tools and technologies rely on traditional infrastructure and perimeter defenses, creating a cybersecurity blind spot since these technologies are ineffective in detecting vulnerabilities and protecting against application-level attacks in the digital banking environment. At the same time, banks struggle to satisfy the nearly 60 percent of mobile bankers who are tech-savvy Gen Y users (age 18 to 34) demanding innovative, simple and secure services.

VASCO, the industry leader in multifactor authentication, offers a comprehensive end-to-end suite of innovative security solutions that effectively protect against evolving fraud schemes while delivering a frictionless user experience. We secure digital banking channels and every component of advanced mobile transactions (such as unlimited funds transfers, bill payments, P2P payments and remote check deposits), continuously evaluating the security of platforms, users and transactions.
Mobile Application Security

VASCO DIGIPASS for Apps: Built-in authentication for mobile

DIGIPASS for Apps is a comprehensive software development kit that natively integrates application security, two-factor authentication and electronic signing into mobile applications. DIGIPASS for Apps empowers banks to extend and strengthen application security, deliver unprecedented convenience to users, and streamline application deployment and life cycle management processes.

Features and benefits include:

• Strengthens mobile app security via a unique single framework that authenticates both transactions and users
• Deploys 360-degree security to protect the integrity of every component of the app—communication, storage, platform, provisioning, interface and user
• Integrates strong and flexible two-factor authentication and protects entire transaction from any exploit
• Facilitates unobtrusive hands-free user experience with convenient and secure biometric or simple PIN authentication options vs. username and password login
• Prevents reuse of dynamic one-time passwords obtained during phishing attack
• Verifies authenticity of websites via host authentication
• Ensures validity of transaction or document and secure transit using e-signatures
• Combats man-in-the-middle attacks by generating unique e-signatures for all transactions based on account numbers, transaction amounts and timestamps
• Elevates trust across mobile banking ecosystem—users, devices, applications and platforms
• Improves consistency of service delivery across mobile and e-banking systems
• Secures the world’s most popular, top-rated mobile banking apps

“Using a single mobile banking application with an integrated one-time password generator results in a safe and faster login process that provides a better user experience. DIGIPASS for Apps proved to be the best solution.”

Tayfun Küçük, Chief Technology Officer, Odeabank (Turkey)
VASCO Runtime Application Self-Protection (RASP)

VASCO Runtime Application Self-Protection (RASP) is intrinsic app security that controls execution, detecting and preventing real-time attacks. For any mobile application, creating a secure environment for the user authentication process is critical.

Runtime security protection is more than just analyzing traffic between applications and external devices such as firewalls or intrusion prevention systems. In order to accurately detect and block attacks configuration, data and event flow as well as application logic are equally critical.

Self-protection capabilities built into the app's runtime environment offer better protection. DIGIPASS goes beyond authentication to ensure that any application running on a mobile platform is self-protected in all aspects of application runtime.

Features and benefits include:
- Protects application by detecting and blocking attacks in the runtime environment
- Verifies app integrity at runtime
- Internally tests and diagnoses security vulnerabilities
- Prevents code from being copied or modified
- Detects jailbreaks and rootkits that remove security and allow malware and rogue apps to infect a device and control critical functions
- Hardens application with memory zeroing, reverse engineering protection, secure storage and white box cryptography
- Securely links authorized users to authorized devices, preventing cloning of cryptographic keys
- Ensures integrity of digital transactions by providing encrypted cross-platform secure channel between server and client device
- Embeds risk scoring capabilities into authentication and signing processes
- Accurately differentiates attacks from legitimate traffic, stopping only what is malicious
- Prevents malicious apps from compromising legitimate apps via drive-by attacks at runtime
Multifactor Authentication

VASCO CrontoSign: Visual transaction signing that thwarts social engineering attacks and prevents fraud

CrontoSign technology utilizes a high-definition color QR code to provide a unique and secure authentication and visual transaction signing solution. A cryptogram image comprised of a matrix of colored dots (QR code) is displayed on the user’s screen.

The mobile banking customer simply points a Cronto-enabled device at the screen to capture the cryptogram, instantly decoding, decrypting and displaying transaction data for verification. If the image is legitimate, the customer receives transaction details via a secure channel. Cronto technology helps banks protect customers against attacks that incorporate hacking techniques like phishing and social engineering by replacing less secure methods of login (username and password, for example) and transaction verification.

Features and benefits include:

- Mitigates human risk in online banking transactions
- Shifts transaction authorization control from user to trusted device and bank
- Delivers bank-initiated transaction signature and authorization requests
- Facilitates two-way validation and transaction authorization over secure communication channel; sender knows that only intended receiver reads message and receiver knows message is from trustworthy sender
- Creates mutual authentication between user and service provider for strong protection against man-in-the-middle and man-in-the-browser attacks
- Improves user experience with simple and safe “sign what you see” digital signatures
- Elevates trust in online transactions with convenient strong authentication
- Adds additional layer of protection for high-value transactions with out-of-band signing for push notifications

Use Case: Mobile Cash

User opens banking app on mobile phone, enters PIN, selects account and amount of withdrawal, and receives secure QR code that can be scanned at an ATM for cash.
IDENTIKEY Risk Manager:
Proactive fraud prevention

IDENTIKEY Risk Manager is a server-side risk management platform that adds an innovative layer of intelligence to authentication management, enabling financial institutions to proactively and rapidly detect and prevent fraud across multiple channels. Through sophisticated real-time risk analysis, IDENTIKEY Risk Manager identifies risk at critical steps, predicting risk levels and taking quick action as fraud patterns emerge. IDENTIKEY Risk Manager works silently in the background to collect and score activities and operations based on intelligent analysis of behavioral, contextual, qualitative and quantitative data.

Features and benefits include:
• Dynamically monitors, analyzes and reduces volume of fraudulent transactions
• Creates barriers hackers and fraudsters cannot easily circumvent
• Invisibly keeps users safe via risk-based authentication, access and transactions
• Simplifies and streamlines compliance with evolving regulations
• Easily integrates MFA and local application security policy based on server-side risk assessment
Conclusion: VASCO Secures the Mobile Banking Environment

Rely on a partner with proven expertise and documented results in global banking. VASCO manages security for most of the world’s largest banks and serves more than 10,000 customers in 100+ countries. More than 1,700 financial organizations trust VASCO to secure their sensitive data. Our collective knowledge translates into an unprecedented understanding of hostilities in the mobile threat environment. We are committed to cost-effectively protecting our financial services customers against future attacks, enabling them to fully leverage explosive growth in the mobile channel.

Find out more about how we can help you reduce threats, combat fraud, lower transaction costs, elevate customer trust in your mobile apps, and improve the mobile user experience. VASCO solutions make data harder to steal while making mobile services easier to use.

Download the ‘Increasing Business with Mobile Banking’ security ebook:

www.vasco.com/MobileBanking
About VASCO

VASCO is the world leader in providing two-factor authentication and digital signature solutions to financial institutions. More than half of the Top 100 global banks rely on VASCO solutions to enhance security, protect mobile applications and meet regulatory requirements. VASCO also secures access to data and applications in the cloud, and provides tools for application developers to easily integrate security functions into their web-based and mobile applications. VASCO enables more than 10,000 customers in 100 countries to secure access, manage identities, verify transactions, and protect assets across financial, enterprise, E-commerce, government and healthcare markets.

Learn more about VASCO at www.vasco.com or visit blog.vasco.com