Foreword by David Strom 1
Research Findings: Current State of Mobile Banking 2
The Scope of the Mobile Banking Problem 3
Best Practices for Securing Mobile Banking Applications 5
Summary 7
About the Authors 8
About VASCO 8
Foreword by David Strom

Mobile banking has the opportunity to become just as disruptive in the modern era as ATMs were back in the 1970s. From the convenience of our own homes, and with our own devices, we now have the opportunity to do just about everything except get cash from our bank.

I have been a mobile banking customer for the past several years. As an independent businessman, I get paid with a lot of checks from my clients. It used to be a chore to walk on over to the ATM to wait for a free machine to deposit them. Now I rarely visit the ATM, and having my bank email me a receipt is a nice touch. Plus, I can quickly pay my bills from my mobile phone too, so I am using my Web-based online banking access less and less. Mobile banking is not just convenient; it’s a great time-saver!

In this white paper, we see the results of some research around what consumers want from their mobile banking applications, discuss some of the current issues surrounding the evolution of mobile banking, and finally, review best practices that will help secure mobile banking apps without compromising user experience.

David Strom is one of the leading experts on network and Internet technologies.
Research Findings: Current State of Mobile Banking

A survey of 1600 consumers by the Tower Group found that price is paramount for a customer to use a mobile banking app. Almost half of those who answered want a clear understanding of what prices and fees they will be charged by their bank for mobile account access. But getting beyond price, security and ease of use and the reliability of the transactions were also important to at least a third of the respondents.

What do customers want?

<table>
<thead>
<tr>
<th>Feature</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Price (example: fees/rates)</td>
<td>48.7 %</td>
</tr>
<tr>
<td>Security and reliability of transactions</td>
<td>41.4 %</td>
</tr>
<tr>
<td>Convenience of access and hours (example: branches, online)</td>
<td>39.4 %</td>
</tr>
<tr>
<td>Safety of customer savings and investments</td>
<td>33.2 %</td>
</tr>
<tr>
<td>Competence and helpfulness of employees</td>
<td>26.1 %</td>
</tr>
<tr>
<td>Ease of product to understand and use</td>
<td>17.2 %</td>
</tr>
<tr>
<td>Speed and effectiveness of problem resolution</td>
<td>15.5 %</td>
</tr>
<tr>
<td>Simplicity and ease of purchase process</td>
<td>11.8 %</td>
</tr>
<tr>
<td>Fit of products and services with my lifestyle</td>
<td>11.8 %</td>
</tr>
<tr>
<td>Guidance on how to better manage my finances</td>
<td>9.2 %</td>
</tr>
<tr>
<td>Guidance on how to best use my financial products or services</td>
<td>8.0 %</td>
</tr>
<tr>
<td>Guidance on purchasing products or services</td>
<td>6.1 %</td>
</tr>
</tbody>
</table>

[1] https://info.bai.org/Vasco_BAI_Banking_Strategies_Webinar_120914_Archive.html
When it comes to consumers’ concerns, both identity theft and unauthorized use of their credit cards top the list. And while consumers have concerns about data breaches, they aren’t too worried about the consequences and are slow to take particular actions to protect their credit and accounts. Perhaps this is because they haven’t been educated in what they need to do, or because they are mostly complacent about their banking needs. And even the most proactive consumers still wonder what else they need to do to or what specific tools they should have in their arsenal.

Identity theft tops list of consumer fears

- Other people obtaining and using your credit or debit card details: 59%
- Unauthorized access to or misuse of your personal information: 57%
- The US’s national security in relation to war or terrorism: 47%
- The security of shopping or banking online: 37%
- Computer security in relation to viruses or unsolicited emails: 36%
- A serious health epidemic occurring in the U.S.: 34%
- Ability to meet essential financial obligations: 30%
- Overall personal safety over the next six months: 25%

As a result of data breaches, have you ever done any of the following?

- Checked your credit report: 41% Yes, 57% No
- Use cash instead of cards: 37% Yes, 61% No
- Shopped at different stores: 66% Yes, 32% No
- Changed password for online retailers: 31% Yes, 66% No
- Requested a new card number from your bank: 29% Yes, 69% No
- Signed up for credit monitoring: 18% Yes, 80% No
The survey also found out that banks heavily rely on their customers to tell them when a breach or misuse occurs, with nearly two-thirds of them notifying their banks this way. More than half of the banks find out about the breach through automated data and transaction analysis systems. However, there is a big gap in knowing and identifying the fraud and what the user has to do to resolve fraudulent claims. And consumers still feel it is the bank’s responsibility to protect them in case of a data breach or theft of account credentials.

Most common ways victims discovered identity theft

- Contacted by financial institutions about suspicious account activity
- Noticed fraudulent charges on account
- Noticed money missing from account
- Contacted by company or agency
- Contacted financial institutions to report a theft
- Credit card declined, check bounced, or account closed due to insufficient funds
- Received a bill or contacted about an unpaid bill
The Scope of the Mobile Banking Problem

Rising Threats

Financial institutions are tremendous targets of opportunity for electronic thievery. Blended threats, improvements to man-in-the-middle/browser exploits, and advances in malware have made threats more numerous and even more available to less-skilled cybercriminals. And historically, banks have purchased different systems to manage different risks, but the result is that they have too many different controls that don’t necessarily integrate or work well with each other. Banks typically have had different fraud prevention departments, and used different tools for each type of exploit. Further, as these exploits continue to blossom, regulators have struggled to figure out best practice recommendations. Payment Card Initiatives and other banking regulations are a great start, but they haven’t kept up with the threat.

Increasing Complexity

When it comes to mobile, it’s critical that we understand the complexity of the problem we are trying to solve. The number of connected devices has passed the total number of people on the planet. And there are more devices per person and this number is increasing. There are also many different types of passwords to secure these devices, and many different accounts across a variety of non-bank institutions and many different channels and methods to do the banking itself (ATM, phone, Web). On top of this, hackers are targeting everyone and using any method they can, making things increasingly difficult.
Evolving Environment

Certainly the computing environment has evolved over the years, and while we have access to a great amount of information, we also have the opportunity to be exposed to more fraudulent activities. Phones now have multiple uses and functions with their data and Internet connections. Consumer attitudes towards security are also evolving as they become more familiar with a variety of mobile apps and not just for their banking needs. Look at the interest towards mobile payment mechanisms from Apple, MasterCard and others in the past year. However, adoption will always lag because of security perceptions, technology complexity, or other reasons.

Advancements in Authentication

There has also been an evolution in the use of authentication in online banking too. Back in the early days, if you wanted stronger authentication, you had to ask a user to change their behavior and carry something such as a one-time password (OTP) token. But some users were reluctant to do this. Ten years ago there weren’t a lot of other solutions that were very secure and convenient, but that has changed, thankfully for the better. There are more cryptographic apps that are cost effective and secure.

According to the Federal Reserve, users expect the same level of functionality on mobile banking regardless of platform or device. Limiting functionality isn’t going to cut it. And many users didn’t want to limit their options by going with those early mobile banking apps, or because of perceived security concerns.
Evolution of Authentication in Online banking

<table>
<thead>
<tr>
<th>Security Level</th>
<th>Class 1</th>
<th>Class 2</th>
<th>Class 3</th>
<th>Class 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sophistication Level of Attacks</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Static Passwords</td>
<td>Keyloggers</td>
<td>Keyloggers</td>
<td>Keyloggers</td>
<td>Keyloggers</td>
</tr>
<tr>
<td>Virtual keyboards</td>
<td>Keyloggers</td>
<td>Keyloggers</td>
<td>Keyloggers</td>
<td>Keyloggers</td>
</tr>
<tr>
<td>Counter-based OTP</td>
<td>Time-based OTP</td>
<td>Time-based OTP</td>
<td>Time-based OTP</td>
<td>Time-based OTP</td>
</tr>
<tr>
<td>Electronic signature</td>
<td>Electronic signature</td>
<td>Electronic signature</td>
<td>Electronic signature</td>
<td>Electronic signature</td>
</tr>
<tr>
<td>Meaningful User Prompts</td>
<td>Meaningful User Prompts</td>
<td>Meaningful User Prompts</td>
<td>Meaningful User Prompts</td>
<td>Meaningful User Prompts</td>
</tr>
<tr>
<td>MitM</td>
<td>MitM with Social Engineering</td>
<td>MitM with Social Engineering</td>
<td>MitM with Social Engineering</td>
<td>MitM with Social Engineering</td>
</tr>
<tr>
<td>WYSIWYS</td>
<td>WYSIWYS</td>
<td>WYSIWYS</td>
<td>WYSIWYS</td>
<td>WYSIWYS</td>
</tr>
</tbody>
</table>
Best Practices for Securing Mobile Banking Applications

Now, let’s address some of the best practices that can be used to secure your mobile app both on the client and server sides, to try to fight some of these perceptions and also to make mobile banking easier and more productive.

Adjust Authentication Methods to Meet User Demands

It’s increasingly clear that some of the older methods just aren’t useful in today’s hyper-mobile world. The notion of using OTP tokens, or using voice prompts to deliver access codes aren’t very convenient when you want to do your banking on any device, wherever you might be. New technologies like visual transaction signing and risk-based authentication can enhance security while matching the new demands for user and device flexibility, making certain that mobile users have transparent authentication and signing methods and that these methods are implemented behind the scenes.

Enhance Client-side Protections

Simple authentication with a user and PIN combination is no longer good enough for mobile banking, because many users share these combinations with a variety of online services, making their authentication information subject to exploitation. When it comes to mobile applications and users, a better solution is to have a user’s PIN combined with other information to lock a phone and an account down.
Further, employing a variety of risk-based methods to determine if a device is in an acceptable geolocation to conduct a transaction, or if it has been jailbroken or has malware present, can add additional layers of protection. And with mobile banking, you can also use strong OTPs behind the scenes so users don’t have to remember and type it in all those numbers.

**Strengthen Security for Client-Server Communications**

Beyond the mobile app, there are use cases where having multiple authentication factors makes sense. These devices (or software tools) can generate the OTP but can transmit the password via a Bluetooth connection as an example. This way an OTP fob can send the OTP directly to the app, so the user doesn’t have to type in the password. This is just one way that a Bluetooth device can secure a transaction and transmit the information to a more hardened environment for subsequent validation.

**Convenient Strong Authentication**

Fast login communicates directly with your authentication token by Bluetooth.

ATM
Internet banking
Mobile banking
Use a Variety of Risk-Based Methods

Another issue is that users want to do more with mobile banking, not just replicate what they could have done inside the branch or their Web browsers. But that means banks have to meet the added risks for these tasks and scale up their security measures accordingly. One problem is that as cryptologic tools get better, hackers are getting better too – for example, using “man-in-the-middle” types of attacks to get around traditional defenses. This creates a requirement for stronger and more transparent signatures that can be sent digitally without worrying about these kinds of attacks.

One potential solution is the use of encrypted signatures and public key cryptographic infrastructure, which haven’t been quite satisfactory up till now. These solutions are painful to manage, both for IT staff and banking customers. In the mobile world, we can cut out some of this pain and take better advantage of these technologies by making use of native security inside the device to sign particular encrypted data and digital signatures of the transaction.

Get Proactive with Fraud Prevention

Stopping potentially dangerous activity before it starts is critical in the new mobile world, especially when it comes to fraud. Managing risk as part of a self-protected application strategy is very different from a reactive security model, where the fraudulent activity can happen, but is stopped on the back end. With risk scoring capabilities built in to a mobile application, organizations can proactively stop fraudulent activity by creating a barrier that a hacker cannot easily circumvent, and further, can be done in a way that doesn’t impact the user experience. Risk scoring capabilities within the mobile application can limit risk on the client side before the transaction ever occurs, and if the transaction is still allowed to occur, tools like risk-based/adaptive authentication on the server side can help to further mitigate risk.

Watch for Evolving Regulatory Requirements

If banks are playing catch up when it comes to mobile security, banking regulators are playing catch up too. The FFIEC has issued guidelines that are still based on some historical usage patterns, and some of these guidelines don’t always apply to the new mobile world. Just as the banking technology is evolving, so do the regulations and compliance mechanisms. Regulators will need to augment the existing FFIEC rules and help banks prepare for more mobile users.

Take a Comprehensive Approach to Mobile App Security

No matter how secure you make the various communications channels, ultimately it comes down to how well a bank builds its apps and understands the inherent security weaknesses. You still have to balance security with ease of use, and you still have to ensure that your core business logic isn’t subject to any exploits too.
In the end, mobile banking security is the combination of a secure application, running on a secure platform, over a secure communication channel (between the bank and the user), and then being able to gather and analyze user and session data to make real-time, risk-based decisions that can protect against account takeover and prevent fraud. Bringing these concepts together into a singular mobile banking security strategy can satisfy the high demands of banking organizations when it comes to security and service delivery, while also satisfying the mobile banking user demands for functionality, convenience, and data and identity protection.

In order to enhance security, improve user experience, and drive more mobile banking usage, VASCO recommends that banks and financial institutions consider these key areas as they continue to build their mobile banking security strategies:

- Better protect the client platform and continuously evaluate its security posture
- Employ a variety of multiple-factor user authentication tools that can leverage mobile devices to make them less onerous
- Use a variety of risk-based methods to evaluate transactions in near real time
- Use these methods on both servers and core apps to enforce validation methods
About the Authors

Benjamin Wyrick
Benjamin Wyrick is Vice President of Sales and Business Operations at VASCO Data Security. Mr. Wyrick joined the company in 2005 and has been a key contributor to the overall growth of the VASCO strong authentication business in North America. Benjamin and his team have successfully managed strong authentication security projects with some of the largest financial institutions, enterprises, and online applications around the world. Benjamin is a frequent presenter at many banking and financial industry conferences and web seminars throughout North America on preventing cyber fraud, account and transaction security for online and mobile applications.

Will LaSala
Will LaSala is Director of Services, North America for VASCO Data Security. LaSala joined the company in 2001 and since then, has been involved in many aspects of product implementation, provisioning, and logistics. He also oversees the VASCO professional services group helping financial institutions in North America with custom two-factor authentication projects. Prior to joining VASCO, Will has worked as a Sr. Systems Engineer and Developer for a prominent consulting firm in New England. He brings over 20 years of software and cyber security experience, and his research interests are focused around the use of mobile and wireless technology to simplify security.

David Strom
David Strom (@dstrom, strominator.com) is one of the leading experts on network and Internet technologies and has written and spoken extensively on topics such as VOIP, convergence, email, cloud computing, network security, Internet applications, wireless and Web services for more than 25 years. He has had several editorial management positions for both print and online properties in the enthusiast, gaming, IT, network, channel, and electronics industries, including the editor-in-chief of Network Computing print, DigitalLanding.com, and Tom’s Hardware.com. He began his career working in varying roles in end-user computing in the IT industry. He has a Masters of Science, Operations Research degree from Stanford University, and a BS from Union College.

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