Secure Mobile Banking: Protecting Your Customers and Your Bottom Line

A Webroot publication featuring analyst research

Issue 2
2 Welcome
3 From the Gartner Files: 14 Banking Apps for 2014
7 The Mobile Banking World
11 Summary
11 About Webroot
Welcome

Mobile banking apps continue to gain in popularity, and the time has come to refine the mobile banking experience. This includes addressing the security concerns of banking customers who remain fearful of using those apps, despite their convenience. Whether you are tasked with network security, fraud management, or promoting mobile banking, this brief will offer strategies to improve the user experience by segmenting the functionality of apps, and present a simple, yet powerful solution to securing mobile banking.

As Moyer and Cohen point out in the 14 Banking Apps for 2014 section that follows, creating value in new ways from digital assets is an urgent imperative for CIOs, given the pressure on global net projects. The incentives for delivering a quality, secure mobile experience include:

- Reduced operational costs: as much as 50 times over in-branch transactions and 23 times over online transactions\(^1\)

- Increased customer satisfaction: 82 percent of mobile banking users are satisfied with their bank, compared with only 71 percent among those who do not use a mobile banking app\(^2\)

- Customer referrals: 76 percent of the mobile app users are likely to recommend their bank, compared with only 67 percent of the non-users\(^3\)

The statistics clearly indicate that mobile banking has become a critical customer engagement channel. This brief will provide insight into improving the mobile banking experience, including the value of creating new apps focused on the highest transaction demand, addressing security concerns, managing risks, and gaining the rewards of operational cost reductions.

---
\(^{1}\)Bruce Alexander, CEO, Vectra Bank – Denver Post, April 12, 2013
\(^{2}\)FICO Survey, Mobile Banking Drives Customer Loyalty and Satisfaction, July 30, 2014
\(^{3}\)Ibid
It’s time to stop building out smartphone mobile banking functionality. We are advising CIOs and CMOs to focus on deploying narrowly focused smartphone apps that digitalize existing processes and create value in new ways from digital assets.

**Key Challenges**
- Many mobile banking applications replicate the online banking experience on smartphones, and do not fit the way customers use smartphones in their digital lives.
- User ratings decrease as the number of function points in a smartphone banking app increases.
- Apps with broad functionality take longer to deploy and cost more than narrowly focused apps.

**Recommendations**
CIOs and chief marketing officers (CMOs):
- Streamline existing smartphone mobile banking apps by eliminating functionality that is rarely used.
- Deploy narrowly focused apps that digitalize existing processes for frequently used smartphone mobile banking functionalities.
- Create a road map for 14 apps for 2014 that create value in new ways from digital assets.

**Strategic Planning Assumption**
By 2015, 25% of banks will decommission current smartphone mobile banking apps in favor of more narrowly focused apps.

**Introduction**
Smartphone mobile banking strategies for retail, commercial and investment banking have relied on using mobile channel servers and other technologies to replicate online banking application functionality for mobile devices. Most banks have deployed smartphone mobile banking with some degree of successful adoption, with 33% of customers using smartphones and 15% using tablets to access services in a recent Gartner survey. However, user ratings of smartphone mobile banking apps are nearly always lower than those of more narrowly focused banking apps. As the number of function points in a banking app increases, user ratings decrease. Apps with more narrow and focused functionality can usually achieve higher user ratings and be deployed more quickly and less expensively.

At issue is the definition of an app. Apps have narrow, focused functionality and are a minimalist interpretation of software design. In this regard, most “all purpose” smartphone mobile banking is not really an app. We believe the next phase of smartphone banking app maturity will need to embrace a minimalist design and functional footprint, which will lead to the gradual reconstruction of smartphone mobile banking in the 2015 to 2017 time frame. Smartphone mobile banking will be supplemented over time with a larger number of banking apps that are narrowly focused and create new types of customer value from physical and digital assets. This reconstruction will provide customers with a full range of narrow and broad functionality to meet their mobile context and location.
CIOs should focus on streamlining existing smartphone mobile banking apps and deploying more narrowly focused apps that do one thing very well. However, these apps should not be extended for tablets, because tablets will have different use cases.

Analysis

Streamline Existing Smartphone Mobile Banking Apps by Eliminating Functionality That Is Rarely Used

CIOs can begin the process of narrowing smartphone mobile banking by collecting and analyzing app function point usage data. For example, CIOs should identify:

- What percentages of customers are downloading the app?
- What types of users download the app most frequently? (What is the bank product mix of users using the app – new vs. established customers, age, geographic location, income, and so on?)
- What is the average frequency of app usage per month?
- What time of day is the app being used most often, and by what types of users?
- What function points are rarely used? What function points are most used?
- What function points are used in combination with one another?

In 2014, CIOs should continue to support smartphone mobile banking apps because reasonable adoption has occurred in many cases. For example, 40% of consumers in developed and emerging markets have used a smartphone to transfer money between accounts. At the same time, CIOs should use app data and analytics to identify smartphone banking functionality that is rarely used and begin eliminating it.

Deploy Narrowly Focused Apps for Frequently Used Smartphone Mobile Banking Functionality

Function points that are frequently used in the bank’s mobile banking application could warrant being deployed as narrowly focused stand-alone apps. These smartphone apps do not replace the bank’s existing mobile banking application that supports broad functionality. Rather, they are an opportunity for the mobile banking team to construct an improved platform of mobile financial services – one that supports a broad function application as well as narrow apps for smartphones (and eventually tablets and other devices). Security and customer authentication will play an important part of the success of these apps.

Based on primary and secondary research that we have conducted on function points, we would expect to see the stand-alone, narrowly focused apps in Table 1 become more broadly available in 2014.

These apps are primarily focused on digitalizing key areas of existing processes and are important enablers of digital banking, but do not create value in new ways from digital assets. CIOs and CMOs will want to draft a road map for apps that create value in new ways.

Create a Road Map for 14 Apps for 2014 That Create Value in New Ways From Digital Assets

There is no magic number for the exact number of apps that CIOs should plan to deploy in 2014 and beyond. In early 2013, the average number of apps deployed by the top 20 banks in the world, by assets, was three. We expect to see the number of apps grow by at least 100% year over year in both 2013 and 2014, which would mean that many large banks will have somewhere near 12 to 14 apps by 2014. The point is not how many apps a bank has, but which apps will enable a transition to digital banking.

Creating value in new ways from digital assets is an urgent imperative for CIOs, given the pressure on global net profits. We have created a road map for 14 apps for 2014 and beyond that create value in new ways from digital assets. The app road map is constructed based on user needs or use cases and the digital banking taxonomy.
<table>
<thead>
<tr>
<th>Apps</th>
<th>Examples</th>
<th>Potential Lines of Business That Each App Could Support</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Retail Banking</td>
</tr>
<tr>
<td>Account balance or health</td>
<td>Westpac (Westpac Cash Tank)</td>
<td>x</td>
</tr>
<tr>
<td>Account opening</td>
<td>Moven and GoBank</td>
<td>x</td>
</tr>
<tr>
<td>Approving, sending or receiving</td>
<td>RBS Citizens Financial (accessMOBILE – although not a stand-alone app, it is part of the mobile banking app)</td>
<td>x</td>
</tr>
<tr>
<td>payment</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>ATM and branch locator</td>
<td>State Bank of India (SBI ATM/Branch Locator) and Starbucks (Starbucks – it shows the closest stores, directions, store hours and amenities)</td>
<td>x</td>
</tr>
<tr>
<td>Check deposit</td>
<td>Citi (Citi Mobile – although not a stand-alone app, it is part of the mobile banking app)</td>
<td>x</td>
</tr>
<tr>
<td>International remittances</td>
<td>Riyad Bank (RiyadMobile – although not a stand-alone app, it is part of the mobile banking app) and Western Union</td>
<td>x</td>
</tr>
<tr>
<td>Market intelligence</td>
<td>Citi (Citi Private Bank Mobile)</td>
<td></td>
</tr>
<tr>
<td>Peer-to-peer (P2P) payment</td>
<td>Barclays (Pingit) and National Australia Bank (NAB Flik)</td>
<td></td>
</tr>
<tr>
<td>Personal financial management</td>
<td>Sumitomo Mitsui Banking (Smart Balance)</td>
<td>x</td>
</tr>
<tr>
<td>(PFM)</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>Photo bill pay</td>
<td>U.S. Bank (U.S. Bank Mobile – although not a stand-alone app, it is part of the mobile banking app)</td>
<td>x</td>
</tr>
<tr>
<td>Real-time exchange rates</td>
<td>Industrial and Commercial Bank of China (Currency Widget)</td>
<td></td>
</tr>
<tr>
<td>Recent or pending transactions</td>
<td>Crédit Agricole (GeoFacto)</td>
<td>x</td>
</tr>
</tbody>
</table>

Source: Gartner (January 2014)
<table>
<thead>
<tr>
<th>Needs or Use Cases</th>
<th>Identity</th>
<th>Access and Delivery</th>
<th>Location and Context</th>
<th>Data and Intelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plan</td>
<td>Identity management (helping users manage public vs. private information and data)</td>
<td>Digital banking advisor (offering proactive advice based on products that are held with the bank)</td>
<td>Photo-generated savings goals (setting a savings goal using the image of an item that the customer wants to buy)</td>
<td>Shopping for a home or property locator</td>
</tr>
<tr>
<td></td>
<td>Nonbanking example: MyPermissions</td>
<td>Example: iQuantifi</td>
<td></td>
<td>Examples: Commonwealth Bank of Australia (CommBank Property Guide) and JPMorgan Chase (Chase My New Home)</td>
</tr>
<tr>
<td>Buy</td>
<td>Location-based authentication (using the location of the mobile device as part of decisioning for authentication)</td>
<td>Digital banking advisor (offering proactive advice based on products that are held with the bank)</td>
<td>Location- and/or context-aware line-of-credit offer (opting in based on location, social media stream, price checking and so on)</td>
<td>Comparing prices and purchasing an automobile</td>
</tr>
<tr>
<td></td>
<td>Example: PayPal Beacon</td>
<td></td>
<td></td>
<td>Example: USAA Car Buying Service (USAA Mobile App)</td>
</tr>
<tr>
<td>Use</td>
<td>Location-based travel notification (using the location of the mobile device to indicate international travel for users, rather than forcing them to notify the bank in advance)</td>
<td>P2P split payment (splitting payment between two or more friends via social media)</td>
<td>Transaction pre-staging (preordering a cash withdrawal from a nearby ATM)</td>
<td></td>
</tr>
<tr>
<td>Manage</td>
<td>Preference management (helping manage social media ID, mobile phone numbers and so on for P2P payments or other banking service)</td>
<td>Digital property inventory (storing images of property with estimated value)</td>
<td>High-risk-behavior notification (notifying users when they are at high risk of incurring negative financial consequences — for example, lacking sufficient cash flow for upcoming bills)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Example: MyPreferences</td>
<td>Example: Allstate (Allstate Digital Locker)</td>
<td>Nonbanking example: Intelligent Marmalade (sending alerts to drivers when their telematics data indicates high-risk driving)</td>
<td></td>
</tr>
</tbody>
</table>

Source: Gartner (January 2014)

App security will increasingly need to be balanced with convenience. In a digital world, the ability to conveniently, quickly and accurately identify a customer will become a differentiator in most markets. In the financial services market, with higher value attributed to customer privacy and security, this differentiation will be amplified. Institutions that can quickly validate a customer’s identity and get the balance right between strength of authentication and ease of access will dominate the digital markets.

Source: Gartner Research, G00260192, Kristin R. Moyer, Stessa Cohen, 23 January 2014
Refinement of mobile banking apps is important to retaining users, yet a large percentage of banking customers are reluctant to access mobile banking due to security concerns (see Figure 1). At the same time, banking customers have high expectations for account access via “new” technology, which they expect to be comparable to the experience of companies like Amazon® – very retail and social. This combination of familiarity and ease-of-use flies in the face of the fraud, risk management, and compliance demands of the financial industry, making the digital world a tough place for financial institutions to truly succeed.

Creating more narrowly focused apps can help improve the user experience and save development costs, but according to Gartner’s Kristin Moyer and Stessa Cohen, “security and customer authentication will play an important part of the success of these apps.”

Securing Mobile Banking Apps

Why are banking customers concerned about leveraging mobile banking applications, despite their convenience and ease-of-use? Quite simply, mobile apps are attractive targets for malicious activity. Of the nearly 11 million mobile apps under review by the Webroot Mobile Threat Research team as of July 2014, only 45 percent are Benign or Trustworthy.

Examples of attacks presenting severe risks for financial institutions include:

Trojans

- Zitmo – steals mTAN codes sent by banks in text messages
- Banker – steals passwords and other sensitive information
- Perkel/Hesperbot – uses JS injection on PC to request mobile number, delivers Trojan via SMS. Trojan poses as a security app.
- Wrob – poses as the Google Play app and replaces installed banking apps with Trojan clones
- Bankum – replaces legitimate versions of banking apps with fake ones
- ZertSecurity – impersonates bank login, steals credentials
Rootkits

- DroidDream – uses rageagainstthecage exploit to root the device, steal data, install additional apps, and execute remote commands

Spyware

- Keyloggers – pose as third party keyboards that send keystroke and contextual information

Fortunately, securing the mobile banking experience does not need to be a paralyzing task requiring endless messaging to customers who may or (more likely) may not execute the security practices designed to keep them safe. Nor is an extensive, cutting-edge IT effort required to protect the financial institution and its mobile banking customers. In fact, robust security can be deployed in a matter of weeks, and it’s available today.

The Webroot® Mobile Security SDKs (for Android and iOS devices) are designed to be embedded within a financial institution’s mobile banking app, working behind the scenes without interfering, changing or modifying the customer experience or transaction processes. Security scans do not slow the device or hinder productivity, and collection of risk data is completely invisible to the user. To alleviate privacy concerns, customer specific data is not captured or stored by Webroot. The user interface is under the full control of the financial institution, with all user interaction configured and controlled by the financial institution.

Know Your Customer

The first rule of fraud prevention is Know Your Customer. The Webroot Mobile Security SDK creates a unique device ID for each mobile banking user and reports the location of the user during each mobile banking session. “In a digital world, the ability to conveniently, quickly and accurately identify a customer will become a differentiator in most markets,” according to Moyer and Cohen.

How it works:

- The customer engages the financial institution via the mobile banking app
- The Mobile Security SDK scans and collects security data within 2 seconds of the app launching
- The SDK performs a device health check, authenticates the customer by the device ID, and identifies risks, such as location of the device
- The SDK provides the financial institution with the risk data for instant analysis, interrogation, and action
- Based on the Risk Score, decisions can be made locally or fed into a financial institution’s risk engine to deny action that poses a threat – reducing risk, or simply flagging an issue (see Figure 2).

Source: Webroot
The mobile device health check compiles a risk score based on the following criteria:

- Device Rooted
- Up-to-date Webroot configuration
- Host application in debug-able state
- Host application is run in an emulator
- Allow side-loading/unknown sources option detected USB debugging option detected
- Up-to-date OS version

**FI-Defined Risk Scoring**

Self-defined risk scoring allows financial institutions to address geo-specific circumstances and score based on the unique profiles of individual customers. Identifying the location of the device can indicate international travel without requiring customers to notify the FI in advance, allowing the FI to contact the customer for verification.

Another benefit of geo-identification is factoring in the tendencies of the locale. For example, rooted devices are more common in Asia. In some geos a rooted device may present an immediate red flag, blocking the device from account access. But in Asia, such a policy decision could cause customer service and customer retention issues. The financial institution may apply customized weights to malware detection categories and device state criteria to balance device risk with legitimate customer access demands. The financial institution may apply customized weights to malware detection categories and device state criteria to balance device risk with legitimate customer access demands. Risk scoring can be as simple as a traffic light system or more complex with individual weights on each feature allowing granular control over the scoring mechanism.

The modular interface permits financial institutions to initialize only what is needed, for example:

**Monitor Module:**

- Set scan engine to run continuously or on-demand
- Monitor device events - download, app execution, install

**Scan Module**

- Full file system or all apps or actively running apps
- Turn on/off cloud lookup; Download on/off definition file
- Quarantine/delete malware options

**App info module**

- Software inventory list

**Device info module**

- Hardware specific attributes
- Root status, OS info, network/Wi-Fi status, disk/memory/battery info
- Risk score assessment based on above criteria

**Threat Intelligence Sources**

Risk scoring is one element of a security management strategy, but quality of threat risk intelligence that powers the security solution is equally important. The torrent of new malware is forcing security providers to continually update their signature/protection files, with more than 5MB of updates per day being commonplace. The underlying problem is that despite these advances, devices are still becoming infected.

Simply put, the modern threat landscape is too vast and too dynamic for reactive, signature-based defenses to be effective. Waiting for signature updates doesn’t work against zero-day threats, exposing banking customers and institutions alike, to dangerous and potential costly risks. Fraud, of all types, is eating up financial firms’ resources and revenue. Certified examiners (AACFE) have found that crime costs an estimated five to six percent of a company’s revenue each year.

Real-time, contextual threat intelligence is required to address the variety and evolution of mobile malware.

---

*Security Intelligence.com, June 12, 2013*
Next-Generation Threat Intelligence

The Webroot® Mobile Security SDK accesses the Webroot® Intelligence Network (WIN) to leverage next-generation threat intelligence that is highly accurate and always up to date (see Figure 3). This architecture incorporates the patented, fourth generation Webroot threat processing and malicious code identification system, which has intimate knowledge of more than 300 million executables, including their runtime behavioral characteristics.

These systems, along with another 150+ terabytes of threat data, ensure that Webroot security solutions are ready to detect new threats as they emerge. While this collective intelligence helps provide comprehensive real-time protection to millions of Webroot customers, their endpoints collect over 200 gigabytes of behavioral execution data each day to feed back into WIN. Unique URL and IP data feeds from strategic partners further enrich Webroot threat intelligence to provide a comprehensive view of the threat landscape. This ensures the Mobile Security SDK is always up to date to protect against even new, previously unknown threats.

Financial institutions have the option of incorporating additional Webroot Intelligence Network solutions, including the IP Reputation Service to track malicious IP addresses. This actionable data enables financial institutions to make well-informed decisions based on reliable intelligence. The SecureWeb™ Browser SDK integrates to block malicious sites using the Webroot Web Classification and Reputation services. The financial institution can also set the URL block list and category level restrictions as part of their network infrastructure.

Source: Webroot
Summary

Providing account access through mobile channels has proven to deliver operational savings while increasing customer retention. Improving the mobile banking experience can be achieved through refining the functionality of mobile banking apps. Focusing on specific customer needs, i.e. account balance and funds transfer, lending, wealth management, can reduce app development costs.

Still, the concern for customers and financial institutions alike is security. As Gartner’s Kristin R. Moyer and Stessa B. Cohen point out, “App security will increasingly need to be balanced with convenience. Institutions that can quickly validate a customer’s identity and get the balance right between strength of authentication and ease of access will dominate the digital markets.”

Armed with real-time, actionable intelligence, assessing and managing security is what financial institutions do best. Supplied with a risk scoring mechanism that is self-driven, easy to deploy, and that does not impact the customer experience, financial institutions have the information to manage risk within the tolerances of their organizations. If you get it right, the benefits are hard to ignore. SunTrust Bank found their mobile banking customers were 32 percent more profitable than online banking customers. The costs of not properly securing your customers transactions can be devastating, but if you get it right the benefits are impossible to ignore.

Source: Webroot

About Webroot

Webroot is bringing the power of software-as-a-service (SaaS) to Internet security with its suite of Webroot SecureAnywhere® offerings for consumers and businesses, 30 financial institutions worldwide, as well as offering its security intelligence solutions to cybersecurity organizations, such as Palo Alto Networks, F5 Networks, Corero, RSA, Cisco, and others.

Founded in 1997 and headquartered in Colorado, Webroot is the largest privately held security organization based in the United States – operating globally across North America, Europe and the Asia Pacific region.

To learn more about Webroot, please visit www.webroot.com/mobilebanking or write to financial@webroot.com.

Contact us
Webroot
385 Interlocken Crescent
Suite 800
Broomfield, CO 80021 USA
1 800 772 9383

SunTrust Consumer Mobile Banking Value Analysis, 2010