



**SYNDICATED RESEARCH
CUSTOM RESEARCH
STRATEGIC CONSULTING**

2008 Mobile Banking Security Standards: Three-Part Strategy Will Increase Consumer Adoption While Protecting Banks' Assets

December 2008



2008 Mobile Banking Security Standards: Three-Part Strategy Will Increase Consumer Adoption While Protecting Banks' Assets



Audience:

Financial institutions (online banking, mobile banking, fraud, security, product development, marketing, and strategic planning functions); mobile banking platform providers, payment networks, mobile payment vendors, mobile carriers, consortiums and forums, new entrants.

Author:

Tom Wills, Senior Analyst, Security, Fraud and Compliance

Contributors:

Mary Monahan, Managing Partner and Research Director
James Van Dyke, President and Founder
Alan Ruperto, Research Associate

Publication date: December 2008

Price: \$2,200

Length: ► 51 pages
► 27 charts/graphs

Overview

Security concerns are the single biggest factor inhibiting consumer acceptance of mobile banking. These concerns are as much a matter of consumer perception as they are of reality – so getting both right will be key. The volume of attacks on mobile banking systems is negligible in the still-nascent and fragmented market that exists today, but will rise as adoption builds, and in particular, as operating system consolidation and platform standardization increases. With a well-designed security program in place, mobile has inherent safety advantages that make it one of the most protected channels for remote banking. It can be used to improve overall (cross-channel) security via the inherent speed-and-notification advantages of always-on, always-present mobile access. For now, build on the diversity of platforms to maintain confidence that malware isn't likely to infect consumer devices, but be aware that emergence of standard platforms will erase today's advantage in the future. Included in this report is a review of the security of mobile banking vendors: ClairMail, CPNI, Firethorn, Fronde, Harland, Jack Henry, mFoundry, M-Com (marketed by Fiserv in the US), Mobile Money Ventures (MMV), Monitise Americas (marketed by Metavante in the U.S.), MShift, Tyfone, and Yodlee.

Primary Questions

- How will security affect mobile banking consumer uptake?
- What are consumers' perceptions around mobile banking security, and how should FIs address them?
- Compared to other customer interaction channels, how safe is mobile banking?
- What real security issues does mobile banking face, how are they being addressed now, and what still needs to be done?
- How do the three key mobile banking enabling technologies (mobile web, dedicated applications, and SMS text banking) – and the various mobile banking platform vendors – compare in terms of security?

**2008 Mobile Banking Security Standards:
Three-Part Strategy Will Increase Consumer Adoption
While Protecting Banks' Assets**



Methodology

This report is mainly based on data collected online from a random-sample panel of 2,714 respondents in March 2008. The survey targeted respondents based on representative proportions of gender, age and income compared to the overall U.S. online population. Overall margin of sampling error is ± 1.88 percentage points at the 95% confidence level.

This report is also based on data collected online from a random-sample panel of 2,350 households in March 2008. The survey targeted respondents based on representative proportions of gender, age and income compared to the overall U.S. online population. The overall margin of sampling error is $\pm 2.02\%$ percentage points at the 95% confidence level. Secondary data from public sources, such as the U.S. Census Bureau and the Bureau of Labor Statistics, forms part of the projections.

This report is also based on executive interviews with risk and fraud, marketing, and security executives at each of the thirteen mobile banking vendors outlined in this report: ClairMail, CPNI, Firethorn, Fronde, Harland, Jack Henry, mFoundry, M-Com (marketed by Fiserv in the U.S.), Mobile Money Ventures (MMV), Monitise Americas (marketed by Metavante in the U.S.), MShift, Tyfone, and Yodlee.



**2008 Mobile Banking Security Standards:
Three-Part Strategy Will Increase Consumer Adoption
While Protecting Banks' Assets**



Table of Contents

Overview	4
Primary Questions.....	4
Findings & Analysis.....	4
Methodology.....	5
Executive Summary	6
Recommendations	6
Three-Part Strategy for Mobile Banking	10
Consumer Awareness Programs	10
Business Controls	11
Technical Controls	11
Consumer Perceptions of Mobile Banking.....	12
Security Concerns are the Biggest Barrier to Mobile Banking Adoption	13
How Many Consumers Judge Mobile Banking to be Safe or Unsafe?.....	14
What Are Consumers' Top Mobile Security Concerns?	15
Which Mobile Banking Platform Is Rated as Most Secure by Consumers?	16
What Do Consumers Prefer for Authentication?.....	17
Consumers Want to Be Actively Engaged in Security	18
Fraud Loss Guarantees Increase Consumer Perceptions of Security	21
Mobile Banking Security–Current Reality	22
The Mobile Banking Security Landscape	23
Security Comparison of Mobile With Other Electronic Banking Delivery Channels	24
Mobile Malware – A Tempest in a Teacup?	24
Authentication	26
Mobile Banking Enabling Technologies Compared	28
SMS Text Banking	30
Mobile Web	30
Dedicated Mobile Applications.....	31
Cross-Technology Platforms.....	31
The Mobile Banking Platform Vendors	32
Vendor Security Analysis	32
Session Authentication	33
Securing the Client Application	34
Client-Server Communications	36
Appendix	38
Related Research	46
Glossary	49
Companies Mentioned	51

**2008 Mobile Banking Security Standards:
Three-Part Strategy Will Increase Consumer Adoption
While Protecting Banks' Assets**



Table of Figures

Figure 1: Javelin's Three-Part Strategy for Mobile Banking Security 7

Figure 2: Three-Part Strategy for Mobile Banking Security -- Detailed..... 9

Figure 3: Mobile Banking Consumer Education Examples..... 10

Figure 4: Worries Holding U.S. Consumers Back From Banking with their Handsets 13

Figure 5: Consumers' Safety Ratings of Mobile Banking..... 14

Figure 6: Consumers' Top Concerns About Mobile Security..... 15

Figure 7: Consumers' Opinions on the Most Secure Platform for Mobile Banking (By Age)..... 16

Figure 8: Consumers' Preferred Methods of Mobile Authentication 17

Figure 9: Two-Way Interactive Alerts Allow Customer Participation in Fraud Prevention 18

Figure 10: Consumers' Rating of Effectiveness of "UDLAP"s and Mobile Alerts to Prevent Fraud..... 19

Figure 11: Forecast of Consumers Receiving SMS Alerts 2009 to 2013 20

Figure 12: Consumer Preference for Additional Methods to Increase Security..... 21

Figure 13: Mobile Banking Security 23

Figure 14: Security Comparison of Mobile With Other Electronic Banking Delivery Channels 24

Figure 15: Security Best Practices and Key Vulnerabilities 29

Figure 16: Vendors and Their Mobile Banking Offerings Surveyed..... 32

Figure 17: Vendor Comparison – Session Authentication 33

Figure 18: Vendor Comparison – Platform Mobile Banking Client Applications..... 35

Figure 19: Vendor Comparison – Client-Server Communications..... 36

Figure 20: Javelin's Prevention, Detection and Resolution™ Model 38

Figure 21: Why Consumers Don't Try Mobile Banking (by Age) 39

Figure 22: Consumer Perceptions of the Security of each Enabling Technology (by Mode) 40

Figure 23: Consumers' Experience Downloading Content to Mobile Phone (by Age) 41

Figure 24: How Consumers are Accessing Mobile Banking (Browser, Text or Application) 42

Figure 25: Mobile Web (Browser-based) Banking Security by Vendor..... 43












Figure 26: SMS Text Banking Security 44

Figure 27: Dedicated Mobile Application Security by Vendor..... 45

**2008 Mobile Banking Security Standards:
Three-Part Strategy Will Increase Consumer Adoption
While Protecting Banks' Assets**



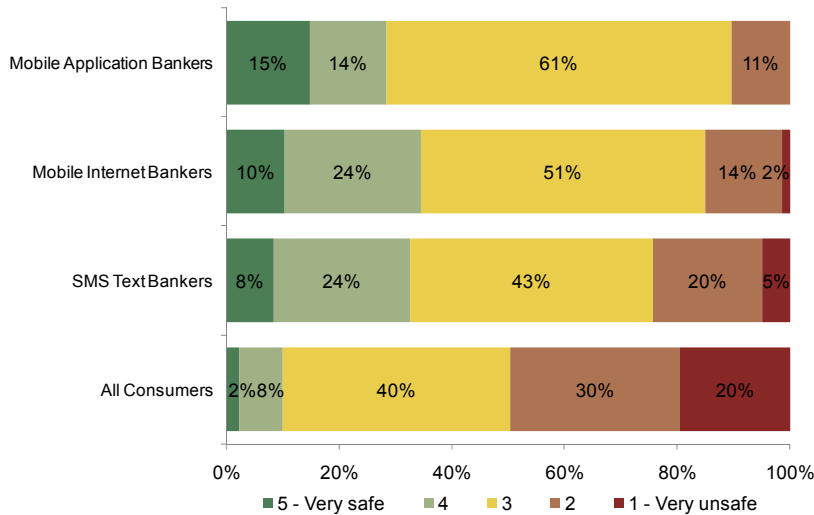
Companies/Organizations Mentioned in Report

Companies Mentioned			
	Android		Jack Henry
	Apple		Linux
	Atrua		M-Com
	AuthenTec		mFoundry
	BREW		Microsoft
	CellTrust		Mobile Money Ventures
	Circle Tech		Monitise Americas
	ClairMail		MShift
	ClassifEye		Palm
	CPNI		RIM
	Firethorn		RSA
	Fronde		Tyfone
	Google		Vervata
	Harland		Yodlee
	J2ME		

**2008 Mobile Banking Security Standards:
Three-Part Strategy Will Increase Consumer Adoption
While Protecting Banks' Assets**



Sample Charts & Excerpts From the Report

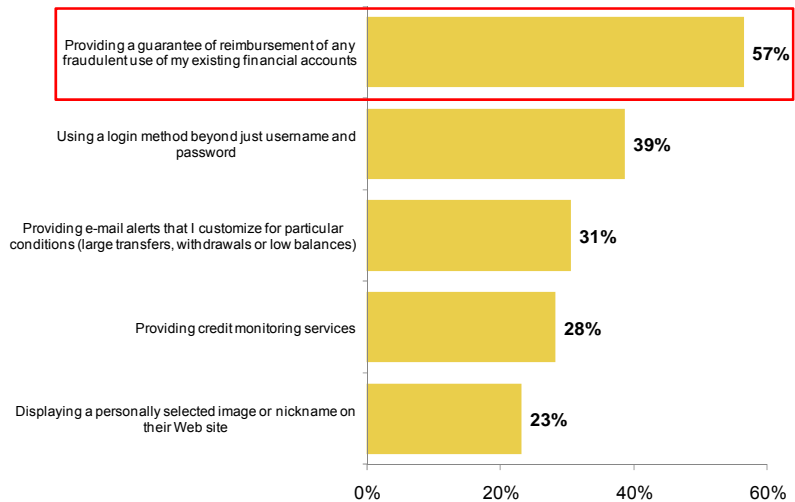


Among the three main mobile banking-enabling technologies, almost triple the number of users find mobile banking to be safe (29 percent of the users of dedicated applications versus 34 percent of mobile Internet bankers and 32 percent of SMS text bankers).

Q36: How would you rate the safety of mobile banking? On a scale of 1 to 5, let 1 represent "very unsafe" and 5 represent "very safe."

March 2008, n = 58,148;103,2,314
Base: All consumers.
© 2008 Javelin Strategy & Research

Possible measures to improve perceived security include multifactor authentication (cited by 39 percent of respondents), user-customized e-mail alerts (31 percent), credit monitoring services (28 percent), and displaying a personalized image or nickname on the institution's Web site – as with RSA's PassMark™ (23 percent).



Q42: Financial institutions are considering other methods to increase security. Which of the following methods or policies would you most like to see your primary financial institution implement? (Top five results included)

March 2008, n = 2,350
Base: All consumers.
© 2008 Javelin Strategy & Research

**2008 Mobile Banking Security Standards:
Three-Part Strategy Will Increase Consumer Adoption
While Protecting Banks' Assets**



Place Your Order as Follows:

- 1) Call us at (925) 225-9100 Ext. 15
- 2) Email us at inquiry@javelinstrategy.com
- 3) Fax or Mail using the form below:

Report Title	Publication Date	Price

Name _____ Title _____

Organization _____ Division or group _____

Email _____ Phone _____ Fax _____

Address _____

Signature to confirm your order: _____

Payment Method: Payment card Check Enclosed Invoice me

Visa, MC, AE or Disc. card #: _____ Exp date: ___/___

Name on Card: _____ Signature _____

For invoicing, provide PO number: _____
(Invoicing is available to financial institutions or publicly owned firms)

Note: Reports are provided in electronic PDF form only. Javelin reports are subject to standard terms and conditions, as described on our web site. Javelin will contact you in the future to provide our free research newsletter or other mailings. If you do not wish to receive our newsletter or other mailings, you may advise us of this. Your contact information will not be sold to other organizations.