BITS

FINANCIAL SERVICES ROUNDTABLE

Mobile Technology

Layered Security Model

June 2013

BITS/The Financial Services Roundtable
1001 Pennsylvania Avenue NW
Suite 500 South
(202) 289-4322

Table of Contents

Executive Summary

The mobile layered security model supplements *BITS Mobile Financial Services Threat Assessment* and is another tool that financial services leaders can use to manage risks associated with mobile banking services, including understanding the risks, corresponding controls, and the dynamics of the mobile ecosystem.

This paper is the result of a series of collaborative research discussions assisted by multiple external subject matter experts to collect, analyze, and organize the information utilized to develop the model detailed in this body of work. The paper should be viewed as a reference guide to analyze and design interactive solutions and communicate with responsible parties and oversight bodies. There are numerous layered security tool kits that have been created and they are available for many purposes. This model was created to address the unique strengths and vulnerabilities of mobile technology to support financial service providers as they manage secure mobile access and delivery of these services.

The rapid adoption of mobile technology in the financial services industry has led to the rise of new and evolving risks associated with mobile malware, identity and credentials theft, rogue applications, data theft and many others as identified in the risk assessment process in the *BITS Mobile Financial Services Threat Assessment*. Mobile risk is both a product of emerging mobile financial payment systems and the use of mobile technology in the day-to-day operations of financial institutions. In order to meet the demands of financial services consumers and workforce financial institutions must build systems that continue to provide the level of assurance and function that are found in current financial systems.

The PCI Security Standards Council nicely summarizes guidelines for mobile financial transactions into three security objectives:

- Prevent account data from being intercepted when entered into a mobile device
- Prevent account data from compromise while processed or stored within the mobile device
- Prevent account data from interception upon transmission out of the mobile device.

Though mobile technology has presented new risks, unique aspects of it also supports effective mitigation with the proper use and implementation of security controls. Each objective can be met for both mobile financial information, and for corporate data, by leveraging the controls defined herein with effective implementation and cooperative integration driven by the strategic stakeholders identified in this model.

This tool is organized in a way to show the relationship of a particular function to each actor and mitigating controls for known risks. Each relationship is evaluated to determine which controls can be influenced, or implemented, to provide higher levels of assurance with the use of mobile technology in financial services systems. The mitigating controls shown are a product of selection based on rating established in the *BITS Mobile Financial Services Threat Assessment*, that combines two attributes – effectiveness and importance. The combination of effectiveness and importance lead to an overall rating. This overall rating was used to determine which controls would be represented in the model. The functions described in the model include: trusted communications, regulation and compliance, mobile financial services, secure software development, secure hardware development, and bring your own device (BYOD) or enterprise mobile devices.

Introduction

The application of mobile technology in the financial services industry has led to an evaluation of mobilespecific *security threats and an identification of mitigating controls.*[1] To build on the *BITS Mobile Financial Services Threat Assessment*, BITS has developed a layered security model to show the relationships between the mitigating controls, functional applications of mobile technology, and the key actors. The illustration *Figure 1: Financial Services – Mobile Technology Layered Security Model* brings these dynamic factors into a single view, demonstrating control versus function and key actors. This tool is intended to utilize and be consistent with National Institute of Standards (NIST) guidelines by recognizing the importance of defining roles to determine the basis of recommending security controls.[2]

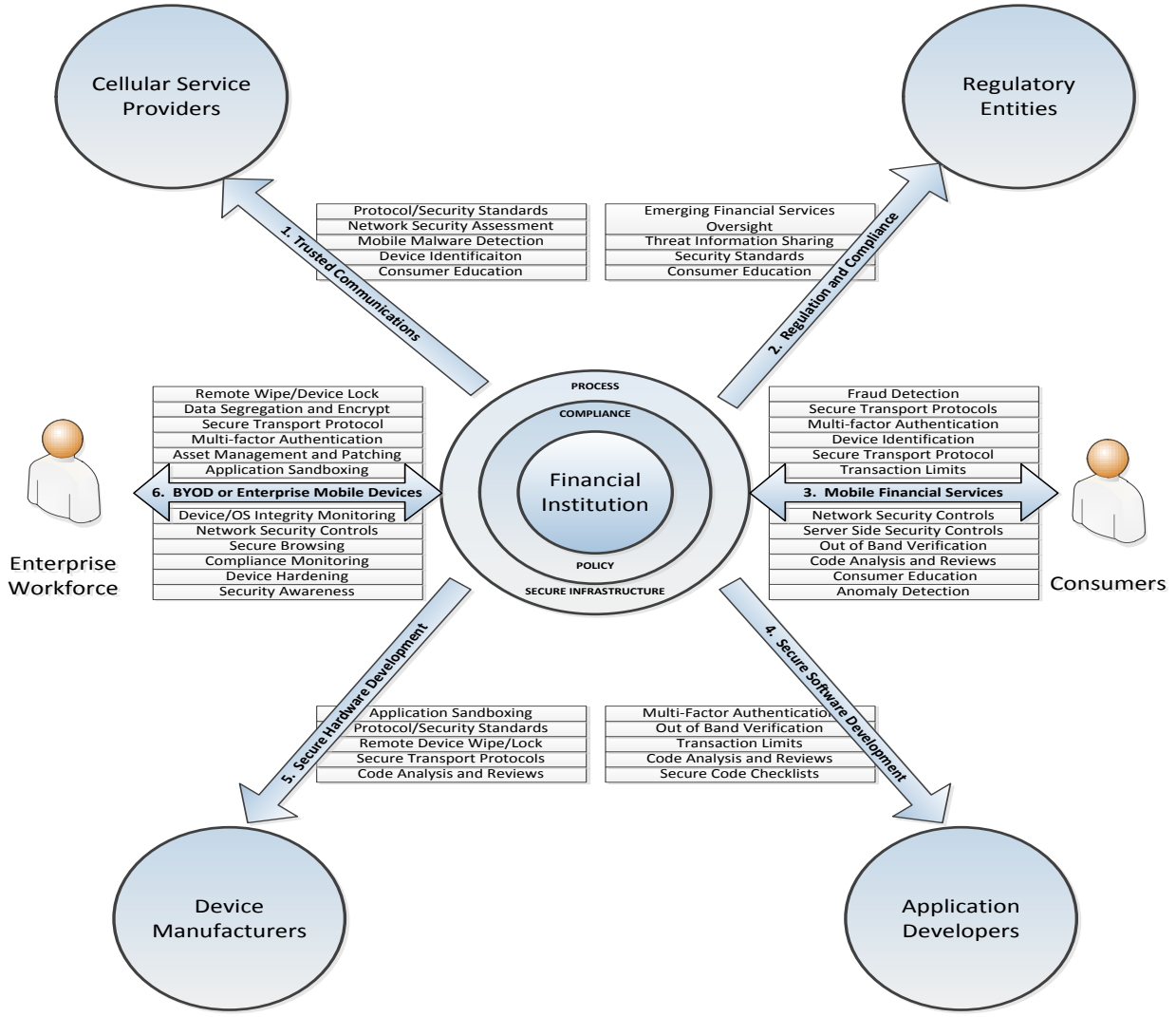


Figure 1: Financial Services - Mobile Technology Layered Security Model

[1] *BITS Mobile Financial Services Security Assessment*, www.bits.org, 20 November 2012.
[2] National Institute of Standards and Technology. "Special Publication 800-164: Guidelines on Hardware-Rooted Security in Mobile Devices," crsc.nist.gov, 12 November 2012.

Each relationship is numbered to provide focus on a particular function and its relationship to a known actor. Each function to actor pairing is in association with mitigating controls for known risks. Each relationship was evaluated to determine which controls can be influenced, or implemented, to provide higher levels of assurance with the use of mobile technology in financial services systems. The mitigating controls shown are a product of selection based on rating established in *BITS Mobile Financial Services Threat Assessment* that combines two attributes: Effectiveness and Importance. The combination of Effectiveness and Importance lead to an Overall Rating. This Overall Rating was used to determine which controls would be represented in the model. Additional controls can be found in *Appendix A: Mobile Control Layer Mapping*.

The functions described in the model are detailed in the following sections of this document:

1. Trusted Communications
2. Regulation and Compliance
3. Mobile Financial Services
4. Secure Software Development
5. Secure Hardware Development
6. BYOD or Enterprise Mobile Devices

Each of these sections will describe how the control relates to the financial institution and the related actor.

Trusted Communications

"Trusted Communications" describes the expectation of the financial institution as a consumer of the cellular service provider networks and devices. Cellular service providers are responsible for the infrastructure for cellular communications and provisioning of mobile devices. This affects all other functional relationships that the financial institution shares with consumers of financial services and the internal workforce consumption of enterprise services. PCI Security Standards Council has published three objectives for security of a mobile payment transaction. Two of these objectives "Prevent account data from compromise while processed or stored within the mobile device" and "Prevent account data from interception upon transmission out of the mobile device" can be addressed at the cellular service provider level.[3] The specific controls that can be provisioned by the cellular service provider can be seen in *Table 1: Mobile Control Layer Mapping – Cellular Service Provider.*

[3] PCI Security Standards Council, "PCI Mobile Payments Acceptance Security Guidelines," www.pcisecuritystandards.org, 12 September 2012.

		Entity	Cellular Service Provider
Importan	**Control**		
8.6	Mobile Malware Detection/ Mobile Anti-Virus		x
8.5	Customer Authentication		x
7.5	Protocol/ Security Standards and Practices		x
7.3	Network and Security Assessments		x
7.2	Device Identification/ Device Fingerprint		x
6.3	Consumer Education		x
6.3	Vendor Contracts, Shared Liability		x

Table 1: Mobile Control Layer Mapping – Cellular Service Provider

The controls are sorted by importance[4] and filtered for their relevance from the mobile control layer mapping found in Appendix A. *Mobile Malware Detection and Mobile Anti-Virus* are considered among the most important controls due to the impact on malicious software which is employed by cyber criminals to breach mobile financial systems. *Customer authentication* is rated next because usage of the device and the cellular network should be restricted to a known consumer. *Protocol/ security standards and practices* determine how the cellular service provider will operate and govern itself. *Network and security assessments* allow providers to determine if their underlying infrastructure is trustworthy and the risk posture of its consumers. *Device identification/ device fingerprinting* can be used to verify end points and accurately disabled if determined untrustworthy. *Consumer education* is important because the inherent risk to privacy and security is not apparent to all consumers. *Vendor contracts and shared liability* create legal responsibility to manage risks.

Regulation and Compliance

"Regulation and Compliance" describes the expectation by regulatory and oversight bodies of the financial institution to assure consumer confidence in the financial services industry to provide trustworthy products. Regulatory entities are in a unique position to evaluate financial institutions and accredit them to operate. This accreditation allows consumers to leverage financial institutions for their savings and loans. The specific controls that can be provisioned by the regulatory entities can be seen in *Table 2: Mobile Control Layer Mapping – Regulatory Entities*.

		Entity	Regulatory Agencies
Importan	**Control**		
7.5	Protocol/ Security Standards and Practices		x
6.3	Consumer Education		x
	Threat Information Sharing		x
	Emerging Financial Services Oversight		x

Table 2: Mobile Control Layer Mapping – Regulatory Entities

[4] BITS Mobile Financial Services Security Assessment, www.bits.org, 20 November 2012.

The controls are sorted by Importance[5] and filtered for their relevance from the mobile control layer mapping found in Appendix A. *Protocol/security standards and practices* are important because the regulatory agencies are best positioned to assure a common security practice across the entire financial services industry. *Emerging financial services oversight* is particularly important due to the rise of non-traditional financial service providers that are leveraging mobile technology to enter the market. *Consumer education* is paramount in the sense that not all risks are readily obvious and do require specific knowledge of proper precautions in the use of mobile technology. *Threat information sharing* is a multiplier to financial institution's protection of mobile financial systems against government verified threats.

Mobile Financial Services

"Mobile Financial Services" includes several products that are commonly offered by financial institutions: mobile banking, alerting, service replacement, and mobile payments. Consumers expect the same level of protection when utilizing these services as they would from traditional means of financial services. In order to provide the same level of confidence, additional controls must be considered for mobile technology as depicted in *Table 3: Mobile Control Layer Mapping – Mobile Financial Services.*

		Entity	Financial Institution and Non-traditional Financial Service Provider
Importan	**Control**		
8.6	Mobile Malware Detection/ Mobile Anti-Virus		x
8.6	Multi-factor Authentication		x
8.5	Customer Authentication		x
8.5	Store Sensitive Data off Device		x
8.4	Server-side Security Controls		x
8	Out of Band Verification		x
7.3	Network and Security Assessments		x
7.2	Device Identification/ Device Fingerprint		x
7.2	Transaction Limits		x
7	Mobile Fraud Detection		x
6.9	Code Analysis and Reviews		x
6.8	Identity/ Brand Management Controls and Processes		x
6.5	Vendor Review Process		x
6.3	Anomaly Detection		x
6.3	Consumer Education		x
6.3	Vendor Contracts, Shared Liability		x
	Posture Checking		x

Table 3: Mobile Control Layer Mapping – Mobile Financial Services

The controls are sorted by Importance[6] and filtered for their relevance from the mobile control layer mapping found in Appendix A. *Mobile malware detection/mobile anti-virus* is important for consumers to

[5] BITS Mobile Financial Services Security Assessment, www.bits.org, 20 November 2012.
[6] BITS Mobile Financial Services Security Assessment, www.bits.org, 20 November 2012.

use if they plan on leveraging their mobile device for online transactions. *Multi-factor authentication,* or c*ustomer authentication*, is a key control for verifying that the end user attempting to access the financial institution's mobile banking solution is the actual authorized consumer. *Storing sensitive data off the device* removes the risk of a stolen device, or malware infected device, being harvested for protected information. *Server side security control* is a combination of end point security to add complexity for an intrusion and configuration hardening to reduce the attack surface area. *Out of band verification* is an additional authorization technique, contacting the customer via means other than the mobile device. *Network and security assessment* allows the financial institution to better understand what opportunities it provides for a potential intruder to compromise the mobile banking environment. All of these controls can be found in greater detail in the *BITS Mobile Financial Services Security Assessment* document.

Secure Software Development

"Secure Software Development" describes the requirement regarding mobile financial applications. Application developers are responsible for providing trustworthy and functional software to consumers. Improper design, or poor coding practices, in mobile financial applications can reduce consumer confidence and generate losses for consumers and financial institutions alike. The specific controls that must be incorporated by all application developers can be seen in *Table 4: Mobile Control Layer Mapping – Application Developers.*

		Entity	Application Developers
Importan	**Control**		
8.6	Multi-factor Authentication		x
8.5	Customer Authentication		x
8	Out of Band Verification		x
7.2	Transaction Limits		x
6.9	Code Analysis and Reviews		x
	Secure Coding Standards and Checklists		x

Table 3: Mobile Control Layer Mapping – Application Developers

The controls are sorted by Importance[7] and filtered for their relevance from the mobile control layer mapping found in Appendix A.

Secure Hardware Development

"Secure Hardware Development" describes the recommendation regarding any mobile platform. Device manufacturers are responsible for providing a secure platform for their consumers. A device compromised at build time can never be trusted from an application perspective. The specific controls that must be included can be seen in *Table 5: Mobile Control Layer Mapping – Device Manufacturer.*

[7] BITS Mobile Financial Services Security Assessment, www.bits.org, 20 November 2012.

		Entity	Device Manfacturer
Importan	**Control**		
8.7	Secure Transport Protocols		x
7.5	Protocol/ Security Standards and Practices		x
7.4	Remote Device Wipe/ Remote Device Lock		x
7.1	Applications Sandboxing		x
6.9	Code Analysis and Reviews		x
6.7	Application Take Down		x
6.6	Device Controls & Settings		x
6.5	Device Specific Patching Process		x
6.3	Consumer Education		x

Table 5: Mobile Control Layer Mapping – Device Manufacturer

The controls are sorted by Importance[8] and filtered for their relevance from the mobile control layer mapping found in Appendix A.

BYOD (Bring Your Own Device) or Enterprise Mobile Devices

"BYOD or Enterprise Mobile Device" addresses the use mobile technology by employees (whether corporately or privately owned) to fulfill the needs of the financial institution regarding related day-to-day operations. xamples of enterprise mobile usage include: corporate browsing, corporate email, corporate applications, and compliance. The specific controls needed to secure this use case can be seen in *Table 6: Mobile Control Layer Mapping – Enterprise Mobile Usage*. National Institute of Standards and Technology (NIST) recognized the importance of mobile technology in 2008 and realized that safe guards were needed "…to enhance security and reduce incidents involving cell phones and PDA devices.[9]" Guidelines developed by NIST were taken into consideration to support the development of these tools and should be a consideration in the development and management of BYOD and Enterprise Mobile Device management.

[8] BITS Mobile Financial Services Security Assessment, www.bits.org, 20 November 2012.
[9] National Institute of Standards and Technology, "Special Publication 800-124: Guidelines on Cell Phone and PDA Security," crsc.nist.gov, 12 November 2012.

		Entity	BYOD or Enprese Mobile Devices
Importan	**Control**		
8.7	Secure Transport Protocols		x
8.6	Multi-factor Authentication		x
7.4	Remote Device Wipe/ Remote Device Lock		x
7.1	Applications Sandboxing		x
6.6	Device Controls & Settings		x
6.3	Consumer Education		x
	Data Segregation and Encrytion		x
	Asset Management and Patching		x
	Device/OS Integrity Monitoring Controls		x
	Network Security Controls		x
	Secure Browsing		x
	Compliance Monitoring		x

Table 6: Mobile Control Layer Mapping – Enterprise Mobile Usage

The controls are sorted by Importance[10] and filtered for their relevance from the mobile control layer mapping found in Appendix A. It is noteworthy that NIST's SP800-164 distinguishes these controls by categorizing them by "User-Oriented Measures" and "Organizational-Oriented Measures."[11] Leveraging these categories, the following can be seen as "User-Oriented Measures": Device controls & settings, device/OS integrity monitoring, remote device wipe/remote device lock, multi-factor authentication, secure transport protocols, data segregation and encryption, and applications sandboxing. The other controls are not device-side and are "Organizational-Oriented Measures": consumer education, compliance monitoring, asset management and patching, and network security controls. Together, these controls address the scenarios that affect all enterprises' "Organization-Issued Devices" and "Non-Organization Issued Devices (BYOD)" as defined by NIST.[12]

[10] BITS Mobile Financial Services Security Assessment, www.bits.org, 20 November 2012.
[11] National Institute of Standards and Technology, "Special Publication 800-124: Guidelines on Cell Phone and PDA Security," crsc.nist.gov, 12 November 2012.
[12] National Institute of Standards and Technology, "Special Publication 800-164: Guidelines on Hardware-Rooted Security in Mobile Devices," crsc.nist.gov, 12 November 2012.

Conclusions and Recommendations

The *BITS Mobile Technology – Layered Security Model* is a strategic level illustration focused on mobile financial services and the necessary controls to mitigate known risks. This model bridges the findings of multiple BITS research activities in the areas of security threat assessment, fraud analysis and prevention, and enterprise mobile device management to integrate layers of security unique to mobile technology and driven by strategic stakeholders.

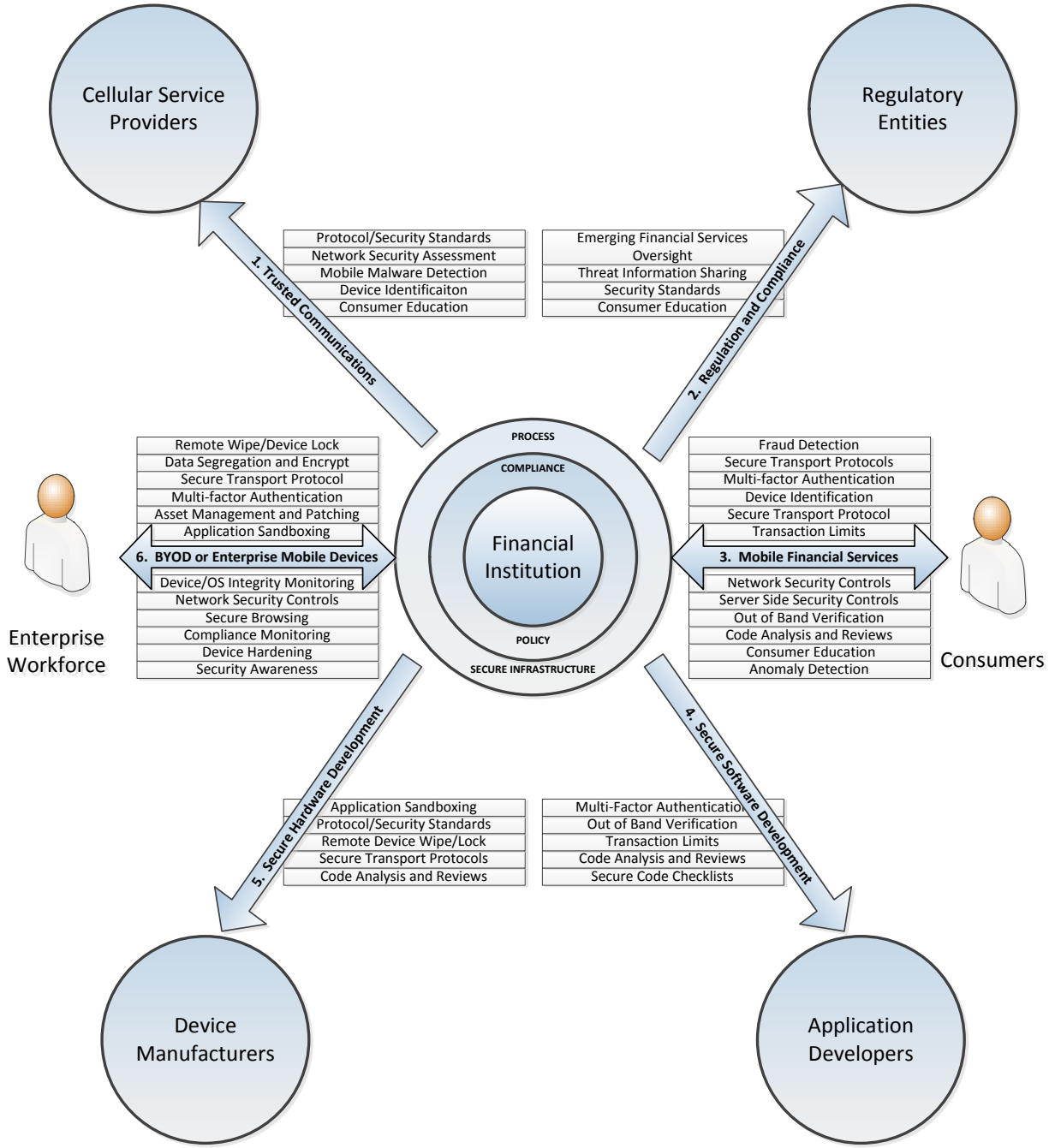
The use of mobile technology requires the same level of diligence that has been applied in the design and implementation of traditional financial systems. This paper has mapped the controls discovered by BITS research to the functional areas most relevant to financial institutions. It is recommended that this document be used as a point of reference with standing BITS research on best practice, policy, and mobile protections.

Control selection should always be a product of risk assessment relevant to the specific use-case(s) for each specific financial institution. To that end, this document is designed so that it may be helpful as a practical tool to assist financial institution leaders to map out security risks, stakeholder drivers and interaction, and risk mitigation controls needed for their specific service offerings.

APPENDIX A: Mobile Control Layer Mapping

Entity			Cellular Service Provider	Regulatory Entities	Financial Institution and Non-traditional Financial Service Provider	Application Developers	Device Manfacturer
Importan	Control						
8.7	Secure Transport Protocols						x
8.6	Mobile Malware Detection/ Mobile Anti-Virus		x		x		
8.6	Multi-factor Authentication				x	x	
8.5	Customer Authentication		x	x	x	x	
8.5	Store Sensitive Data off Device				x		
8.4	Server-side Security Controls				x		
8	Out of Band Verification				x	x	
7.5	Protocol/ Security Standards and Practices		x	x			x
7.4	Remote Device Wipe/ Remote Device Lock						x
7.3	Application Store Development Validation						
7.3	Network and Security Assessments		x		x		
7.2	Device Identification/ Device Fingerprint		x		x		
7.2	Transaction Limits				x	x	
7.1	Applications Sandboxing						x
7	Mobile Fraud Detection				x		
6.9	Code Analysis and Reviews				x	x	x
6.8	Application Stores/ Marketplace Monitoring						
6.8	Identity/ Brand Management Controls and Processes				x		
6.7	Application Take Down						x
6.6	Device Controls & Settings						x
6.5	Device Specific Patching Process						x
6.5	Vendor Review Process				x		
6.4	Developer Identity Verification						
6.3	Anomaly Detection				x		
6.3	Consumer Education		x	x	x		x
6.3	Vendor Contracts, Shared Liability		x		x		
	Posture Checking			x	x		
	Industry Oversight						
	Secure Coding Standards and Checklists					x	

APPENDIX B: BITS Mobile Technology – Layered Security Model



APPENDIX C: Acknowledgements

BITS greatly thanks Peter Staarfanger, TSYS, as the chief architect of the *BITS Mobile Technology – Layered Security Model* and primary creator of this document.

Contributing Organizations

BITS would like to acknowledge the efforts of the many representatives from the following participating institutions, associations, and agencies who also assisted with project research by providing input, insight, and expert content.

Air Patrol
Canadian Bankers Association
Coalfire
CTIA
FixMo
In Auth
iSec Partners
JWSecure
Kaprica Security
Mobile Active Defense
Mobile Iron
NACHA
PCI
Pricewaterhouse Coopers
Smart Card Alliance
StillSecure
Transeq
Trend Micro
Trusteer
Voltage

BITS especially would also like to recognize the following participating member companies.

Ally Financial Inc.
American Trust & Savings Bank
Bank of America Corporation
Bank of Hawaii Corporation
BancWest Corporation
BB&T Corporation
BBVA Compass
BNY Mellon Corporation
Capital One Financial Corporation
Citigroup Inc.
Comerica Incorporated
CUNA
Discover Financial Services
Edward Jones
Federal Reserve Bank of Boston
Fidelity Investments
Fifth Third Bancorp
First Commonwealth Bank
General Electric Company
HSBC North America Holdings, Inc.
JPMorgan Chase & Co.
KeyCorp
The PNC Financial Services Group, Inc.
Principal Financial
Matt McCright - Principal Financial
Prudential Financial Inc.
Raymond James
Regions Financial Corporation
RBS Americas
State Farm Insurance Companies
SunTrust Banks, Inc
Synovus
TD Bank
TSYS
Union Bank
U.S. Bancorp
WebBank
Webster Bank
Wells Fargo & Company

About BITS

BITS addresses issues at the intersection of financial services, technology and public policy, where industry cooperation serves the public good, such as critical infrastructure protection, fraud

prevention, and the safety of financial services. BITS is the technology policy division of The Financial Services Roundtable, which represents 100 of the largest integrated financial services companies providing banking, insurance, and investment products and services to the American consumer. For more information, go to http://www.bits.org/.

