New Banking Agency Guidance on Mobile Financial Services
FFIEC Appendix E

Andy Lorentz, Partner

ACI Emerging Payment Systems Conference
San Francisco
July 28, 2016
Context
More context
FFIEC Appendix E: Mobile Financial Services

- Roadmap for risk management and mitigation for financial institutions providing mobile financial services (MFS)
- Emphasizes enterprise-wide risk management to manage and mitigate risks (*including third party service providers*)

Appendix addresses:

- MFS technologies
- Risk identification
- Risk measurement
- Risk mitigation
- Monitoring and reporting
MFS Technologies

- Short message service (SMS)/text messaging
- Mobile-enabled Web sites and browsers
- Mobile applications
- Wireless payment technologies
  - Near field communication (NFC)
  - Image-based
  - Carrier-based
  - Mobile P2P
Risk Identification and Measurement

Categories of Risk

- Strategic
- Operational
- Compliance
- Reputation

- MFS presents particular concerns due to degree of customer control, number of access points, and presence of third parties

Measurement

- Measure potential risks across all applicable risk categories
- Prioritize results to determine appropriate controls for the services provided
- Ongoing process that is updated whenever management implements a change to the strategy or MFS
Risk Mitigation (overview)

- Management should mitigate identified risks by implementing effective controls across the institution.

- MFS requires the coordinated and secure exchange of information among several unrelated entities (application developers, mobile network operators, device manufacturers, specialized security firms and other nonfinancial third-party service providers).

- General operational controls an FI “should consider” include enrollment, authentication and authorization controls (user and application), application development and distribution, application security, contracts, customer awareness, and logging and monitoring.
Operational Risk Mitigation

- **SMS Technology**
  - Functionality limitations, token and PIN usage and customer awareness

- **Mobile-Enabled Web Sites and Mobile Applications**
  - Focus is on developers (Web-site and application design, testing and employing tools) and customers/users (education, training and security awareness)

- **Mobile Payments**
  - Traffic filtering to help prevent or minimize denial-of-service attacks
  - Trusted platform modules
  - Secure telecommunications protocols
  - Tokenization and encryption
  - Anti-malware software
  - Authentication controls of both the user and application
Compliance and Reputation Risk Mitigation

- **Compliance Risk Mitigation**
  - Ongoing review and assessment of MFS offerings
  - Management to consult with compliance, legal and training staff
    - Disclosures
    - Policies and procedures
    - Legal and regulatory changes

- **Reputation Risk Mitigation**
  - Management to adopt appropriate and effective controls over customer information accessed, transmitted or stored to minimize or prevent disclosure of personal information and the potential for fraudulent transactions
# Monitoring and Reporting

## Performance monitoring systems to assess whether MFS is meeting expectations

- Include limits on the level of acceptable risk exposure of management and the board
- Identify specific objectives and performance criteria, including quantitative benchmarks
- Periodically compare actual results with projections and qualitative benchmarks
- Modify the business plan, when appropriate, based on the performance of the MFS

## Reports

- Content structured to meet the needs of the various levels of management
- Addresses point-in-time as well as trend activity for both individual customers and mobile channel activities
- Emphasize the volume of activity from the onset and reports on changes in usage/volume
- Document the various demographic and industry sectors served and monitor changes
Conclusion: Be careful what you wish for…
because MFS is a complex ecosystem....
and guidance may slow (or divert) innovation.

- Mobile phones are prevalent among unbanked and underbanked
- Curbed innovation and slower implementation by banks
- Compliance costs increase for banks
- Detailed policies and procedures created for banks
- Increasing doption of mobile financial services
- Increasing (?) security and privacy risks
- Regulators provide detailed guidance to banks

Compliance costs increase for banks

Increasing doption of mobile financial services

Increasing (?) security and privacy risks

Regulators provide detailed guidance to banks

Curbed innovation and slower implementation by banks

Detailed policies and procedures created for banks
This presentation is a publication of Davis Wright Tremaine LLP. Our purpose in making this presentation is to inform our clients and friends of recent legal developments. It is not intended, nor should it be used, as a substitute for specific legal advice as legal counsel may only be given in response to inquiries regarding particular situations.

Attorney advertising. Prior results do not guarantee a similar outcome.

Davis Wright Tremaine, the D logo, and Defining Success Together are registered trademarks of Davis Wright Tremaine LLP. © 2015 Davis Wright Tremaine LLP.