MOBILE BANKING -

A LEGAL PERSPECTIVE

September 15, 2011

Kevin M. Levy, Esq.
klevy@gunster.com

GUNSTER – FLORIDA'S LAW FIRM FOR BUSINESS

GUNSTER
ATTORNEYS AT LAW

Introduction

- Socialnomics video
- Generation Now

GUNSTER

ATTORNEYS AT LAW

Introduction

- Standards
- Regulations
- Policies and Procedures
- Authentication
- Conclusion

GUNSTER

ATTORNEYS AT LAW

Standards

- Industry Standards being developed
  - Near Field Communication (NFC) Forum
    - N-Mark certification – indicates NFC technology-enabled mobile device
  - ISIS
    - Verizon Wireless, T-Mobile and AT&T venture with Discover Card and Barclaycard US
    - Smart mobile device (chip-based technology)
    - Mobile payments – moving from plastic to mobile
  - Google
    - new Android OS (mobile wallet)

GUNSTER

ATTORNEYS AT LAW

Standards

- Industry Standards for Privacy and Consumer Data Protection
  - Clear Privacy Policy
    - Opt-In to receive messages
    - Opt-out option
  - Review and conform with checklists from mobile service providers
  - Adapt as the industry and regulations continue to evolve
  - Self-regulation

GUNSTER

ATTORNEYS AT LAW

Regulations

- Regulations are often behind advancements in the technology industry
  - No U.S. mobile banking-specific regulations
    - Covered under various laws and guidance for Internet banking, and other Internet related commerce
    - *Mobile is more risky than online*
  - The next “Wild West” frontier
  - Guidance and self-regulation

GUNSTER

ATTORNEYS AT LAW

Regulations

- Federal Financial Institutions Examination Council (FFIEC)
  - Guidance on *Authentication in an Internet Banking Environment* (2005) (2011 update)
  - Framework for risk management for financial institutions engaged in Internet banking
  - Increased risks in electronic banking mean effective security is essential for financial institutions
- OCC Bulletin 2001-47
  - *Guidance* to national banks on managing the risks that may arise from their business relationships with third parties
  - Regulators recognize outsourcing is beneficial, but IT needs to be done right

GUNSTER

ATTORNEYS AT LAW

Regulations

- Self-Regulation
  - Mobile Marketing Association (MMA)
    - Over the past 5 years, developed a well-defined set of rules and regulations, including the Global Code of Conduct
  - Interactive Advertising Bureau (IAB)
    - Recently made the IAB online self-regulatory program mandatory – includes Microsoft, Google, Yahoo and Facebook
  - Direct Marketing Association (DMA)
    - DMA's Self-Regulatory Program for Online Behavioral Advertising requires member organizations to include an opt-out link within their ads

GUNSTER

ATTORNEYS AT LAW

Federal Regulations

- Examples of Applicable Federal Regulations
  - Gramm-Leach-Bliley Act (GLBA)
    - Privacy Act and Regulation P
  - Fair Credit Reporting Act (FCRA)
  - Fair and Accurate Credit Transactions Act
  - USA Patriot Act
  - Bank Secrecy Act
  - Anti-Money Laundering Compliance Programs
  - Dodd-Frank Act
  - CAN-SPAM Act of 2005

GUNSTER
ATTORNEYS AT LAW

State Regulations

- Examples of Applicable State Privacy Laws
  - Protection of Personal Information
    - Florida
      - Fl. St. Section 655.059 (Banks)
    - Massachusetts
      - MA 201 CMR 17.00
  - Security Breach Notification Protocols
    - Florida
      - Fl. St. Section 817.5681
    - 40 of 50 other states

GUNSTER

ATTORNEYS AT LAW

Regulations

- Location-based services (LBS)
  - 1996 Telecommunications Act
    - Location information as Customer Proprietary Network Information (CPNI)
  - Federal Communications Commission (FCC)
    - Unclear authority interpreting various Federal acts
  - Cellular Telecommunications and Internet Association (CTIA)
    - Industry self-regulation
    - Conform with Privacy Policy
  - CAN-SPAM Act of 2005
    - Requires informed consent to receive messages

GUNSTER

ATTORNEYS AT LAW

Regulations

- Privacy regulations in Europe and Japan are both more developed and more clear with respect to consent
- <u>Europe</u>
  - requires informed opt-in consent for location information-based telecommunications services
  - European directives under review
- <u>Japan</u>
  - "telecommunications carrier shall not disclose the location information (the information indicating the location of the party in possession of a mobile terminal) to another except when the data subject gives consent"

GUNSTER

ATTORNEYS AT LAW

Policies and Procedures

- Customer Relationships
  - Due diligence – “know your customer” (KYC)
    - Proactively understand and address regulations relating to your customer’s industry and your customer’s concerns
  - Strict confidentiality provisions
  - Data ownership, backup and disaster recovery
  - Exceptions to disclaimers, limitations of liability and indemnification
  - Require and enforce applicable policies and procedures
    - Be aware of SAS 70 and SSAE16
  - Monitoring (audits) and reporting requirements

GUNSTER

ATTORNEYS AT LAW

Policies and Procedures

- Vendor Relationships
  - Due diligence – “know your vendor” (KYV)
    - Require vendors to understand and address industry regulations
  - Strict confidentiality provisions (vendor and subcontractors)
  - Data ownership, backup and disaster recovery
  - Be aware of exceptions to disclaimers, limitations of liability and indemnification
  - Require and enforce applicable policies and procedures
    - SAS 70 and SSAE16
    - Strong service level agreements (SLAs)
  - Monitoring (audits) and reporting requirements

GUNSTER

ATTORNEYS AT LAW

Policies and Procedures

- Vendor Relationships
  - Strong service level agreements (SLAs)
    - Strong and clear
    - Functions, deliverables and timelines
  - Subcontractors
    - KYV the subcontractor or require approval
    - If offshore, consider political issues and business continuity in the event of unique natural disasters

Policies and Procedures

- Research, adopt (adapt) and develop applicable policies and procedures
  - Mobile service provider checklists
  - Privacy Policy
  - “Red Flags” Rule on Identity Theft
  - Learn from industry mistakes
- Appoint team and train
- PRACTICE, PRACTICE, PRACTICE
- REVIEW AND UPDATE
  - Learn from circumstances
- Periodic audits

GUNSTER

ATTORNEYS AT LAW

Policies and Procedures

- Notice to customers
  - Privacy
  - Security

- Security
  - Strategic
  - Research, develop and adopt (adapt) applicable policies and procedures

  - Physical
    - locks, not “twisty-tie”

  - Electronic
    - Encryption

GUNSTER
ATTORNEYS AT LAW

Authentication

- Federal Financial Institutions Examination Council (FFIEC) - Guidance on *Authentication in an Internet Banking Environment* (2005) (2011 update)
  - Internet services need to have reliable and secure methods to authenticate customers
  - *Mobile is more risky than online* – extra level of data changing hands

GUNSTER

ATTORNEYS AT LAW

Authentication

- Conduct risk-based assessments
  - Not all customers and transactions pose the same risks
  - *Mobile is more risky than online*
- Evaluate customer awareness programs
  - Educate customers - key defense against fraud and identity theft
- Security Measures
  - Develop, adopt and periodically update security measures to reliably authenticate customers remotely accessing financial and other similarly sensitive services

GUNSTER
ATTORNEYS AT LAW

Authentication

- Single-factor authentication is inadequate for high-risk transactions involving access to customer information or movement of funds via the Internet
- Variety of multifactor authentication (two or more forms of authentication)
  - *Something a person knows* – shared secrets - password, PIN or customer selected images or questions
  - *Something a person has* – tokens - self-contained device, smart card or one-time password (OTP)
  - *Something a person is* – biometrics - physical characteristic

GUNSTER
ATTORNEYS AT LAW

Conclusion

- Proceed with caution and common sense
  - Clear Privacy Policy
  - Informed consent to receive messages
  - Comply with mobile service provider checklists
  - Understand, assess and follow existing regulations
  - Adopt and follow appropriate policies and procedures
  - Update and adapt existing policies and procedures as the industry evolves and legal regulations evolve
  - Constantly evaluate risks
  - Consistently and thoroughly enforce policies and procedures
  - Plan for personnel turnover

GUNSTER

ATTORNEYS AT LAW

Conclusion

- KYC
  - Proactively understand and address industry regulations for your customer

- KYV
  - Scrutinize vendors and vendor agreements, and include a clear understanding of each party's rights and obligations

GUNSTER
ATTORNEYS AT LAW

GUNSTER

ATTORNEYS AT LAW

Kevin M. Levy, Esq.

klevy@gunster.com

GUNSTER – FLORIDA'S LAW FIRM FOR BUSINESS

- Banking & Financial Services
- Business Litigation
- Corporate
- Environmental & Land Use
- Immigration
- International
- Labor & Employment
- Leisure & Resorts
- Real Estate
- Private Wealth Services
- Probate, Trust & Guardianship Litigation
- Securities
- Tax
- Technology & Entrepreneurial Companies