Mobile Banking: Overcoming Legal and Regulatory Challenges
Minimizing Liabilities in Wireless Financial Transactions

A Live 90-Minute Teleconference/Webinar with Interactive Q&A

Today's panel features:
Frederick M. Joyce, Partner, Venable, Washington, D.C.
Peter E. Heyward, Partner, Venable, Washington, D.C.

Thursday, January 14, 2010
The conference begins at:
1 pm Eastern
12 pm Central
11 am Mountain
10 am Pacific

You can access the audio portion of the conference on the telephone or by using your computer's speakers. Please refer to the dial in/log in instructions emailed to registrations.

CLICK ON EACH FILE IN THE LEFT HAND COLUMN TO SEE INDIVIDUAL PRESENTATIONS.

If no column is present: click Bookmarks or Pages on the left side of the window.
If no icons are present: Click View, select Navigational Panels, and chose either Bookmarks or Pages.

If you need assistance or to register for the audio portion, please call Strafford customer service at 800-926-7926 ext. 10
For CLE purposes, please let us know how many people are listening at your location by

- closing the notification box
- and typing in the chat box your company name and the number of attendees.
- Then click the blue icon beside the box to send.
MOBILE BANKING: OVERCOMING LEGAL & REGULATORY CHALLENGES

Rick Joyce, Chair, Communications Practice Group
RJoyce@Venable.com

Peter Heyward, Partner
Financial Services Group
PHeyward@Venable.com
VENABLE LLP

One of *The American Lawyer’s top 100 law firms*. Venable LLP:

- Practices in all areas of corporate & business law, complex litigation, intellectual property & government affairs.
- Nearly 600 lawyers serving corporate, government, nonprofit & individual clients throughout the U.S. & around the world.
- Headquartered in Washington DC with offices in New York, California, Maryland & Virginia.
- Founded more than 100 years ago, the firm has enjoyed a long history of steady growth, quality service & sound management.
Speakers:

Frederick ("Rick") Joyce

Rick Joyce is the chair of Venable’s Communications Group. He focuses on wireless communications and new communications technologies such as Voice Over the Internet (VOIP) services and Broadband over Power Line (BPL).

He has represented clients in matters involving domestic and international regulations and treaties, public and private financial transactions and appellate and civil litigation pertaining to telecommunications and state/federal telecommunications legislation.

Mr. Joyce’s experience with wireless operations goes back to the first cellular radiotelephone networks in the United States and the first deployment of overseas wireless networks. He helped create the first clearinghouse and standards for Short Messaging Services (SMS) throughout South America and the first inter-carrier roaming agreements in South America.
Peter Heyward

Peter Heyward’s practice focuses on U.S. and international financial regulation. He has more than 20 years’ experience in representing financial institutions, advising clients on a broad range of matters that are subject to regulation by federal or state agencies. Areas of special focus include:

- regulation of depository institutions and their holding companies;
- application of U.S. laws to internationally active banking organizations;
- restrictions on transactions between depository institutions and their affiliates;
- regulation of government-sponsored enterprises; and
- enforcement matters.

He is recognized as one of The Best Lawyers in America® for Banking Law.

Mr. Heyward served as a senior attorney in the international section of the Federal Reserve Board’s Legal Division from 1986 to 1989.
“Mobile Financial Services” Defined:

- **Mobile Banking**: Use of a mobile phone to connect to financial institutions for customer services (account balances, fund transfers; bill payments). **This is the focus of our presentation today.**
- Mobile Payments: Use of a mobile phone to make a purchase or payment (“mobile wallet”, using SMS, software, and embedded NFC).
- Mobile Commerce: Extends e-commerce to mobile devices to buy/sell goods.
Mobile Banking Platforms:

- **Short Message Service (SMS)**
  - Easy to use/common to most phones
  - Cost effective for FI’s
  - Limited capabilities; “bank texting”

- **Wireless Application Protocol (WAP)/Browser**
  - Most common platform; secure specifications
  - Browser software allows users to access bank’s online services via mobile device

- **Downloaded Applications (Mobile Client Apps)**
  - More robust features and highest security
  - Bank/vendor supported and proprietary software
<table>
<thead>
<tr>
<th>Topic</th>
<th>Dec-08</th>
<th>Dec-05</th>
<th>Dec-00</th>
<th>Dec-95</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Subscribers</td>
<td>270.3M</td>
<td>207.9M</td>
<td>109.5M</td>
<td>33.8M</td>
</tr>
<tr>
<td>Wireless Penetration</td>
<td>87%</td>
<td>69%</td>
<td>38%</td>
<td>13%</td>
</tr>
<tr>
<td>% of total U.S. population</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless-Only Households</td>
<td>17.5%</td>
<td>8.4%</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>% of U.S. Households</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct Carrier Jobs</td>
<td>268,500</td>
<td>233,000</td>
<td>184,000</td>
<td>68,000</td>
</tr>
<tr>
<td>Wireless Carrier Payroll</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct Carrier Wages</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Direct Carrier Wages</td>
<td>$13B</td>
<td>$12.2B</td>
<td>$1.8B</td>
<td>$1.7B</td>
</tr>
<tr>
<td>Annualized Total Wireless Revenues</td>
<td>$148.1B</td>
<td>$113.5B</td>
<td>$45.3B</td>
<td>$19B</td>
</tr>
<tr>
<td>Annualized Wireless Data Revenues</td>
<td>$32.3B</td>
<td>$8.5B</td>
<td>$211.2M</td>
<td>N/A</td>
</tr>
<tr>
<td>Annualized Incremental Capital Investment</td>
<td>$20.1B</td>
<td>$25.2B</td>
<td>$18.4B</td>
<td>$5.1B</td>
</tr>
<tr>
<td>Annualized Minutes of Use</td>
<td>2.2T</td>
<td>1.5T</td>
<td>533.8M</td>
<td>431.9M</td>
</tr>
<tr>
<td>Monthly SMS Messages</td>
<td>110.4B</td>
<td>9.8B</td>
<td>14.4M</td>
<td>N/A</td>
</tr>
<tr>
<td>Annualized Yearly SMS Messages</td>
<td>1T</td>
<td>81B</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Cell Sites</td>
<td>242,130</td>
<td>183,689</td>
<td>104,288</td>
<td>22,663</td>
</tr>
</tbody>
</table>
Chart 2.10
Percent of U.S. Households
With Computers, Internet Access, and High Speed Access
Selected Years (1997 - 2007)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Computer</strong></td>
<td>38.6%</td>
<td>42.1%</td>
<td>51.0%</td>
<td>56.2%</td>
<td>61.8%</td>
<td>61.7%</td>
</tr>
<tr>
<td><strong>Internet Access</strong></td>
<td>18.6%</td>
<td>26.2%</td>
<td>41.5%</td>
<td>50.5%</td>
<td>54.6%</td>
<td>61.7%</td>
</tr>
<tr>
<td><strong>High-Speed Access</strong></td>
<td>4.4%</td>
<td>9.1%</td>
<td>19.9%</td>
<td>30.8%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 7.1
**Total U.S. Wireline Telephone Lines**
*(End of Year Data)*

<table>
<thead>
<tr>
<th>Year End</th>
<th>CLEC and ILEC Lines $^1$</th>
<th>Annual Growth (%)</th>
<th>ILEC Local Loops $^2$</th>
<th>Annual Growth (%)</th>
<th>ILEC Access Lines $^3$</th>
<th>Annual Growth (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1980</td>
<td>102,216,367</td>
<td></td>
<td>105,559,222</td>
<td>3.3 %</td>
<td>113,832,113</td>
<td></td>
</tr>
<tr>
<td>1981</td>
<td>107,519,214</td>
<td>1.9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1982</td>
<td>107,519,214</td>
<td></td>
<td>110,612,689</td>
<td>2.9</td>
<td>113,832,113</td>
<td></td>
</tr>
<tr>
<td>1983</td>
<td>112,220,739</td>
<td>1.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1984</td>
<td>115,983,813</td>
<td>3.1</td>
<td>117,384,865</td>
<td>3.1 %</td>
<td>113,832,113</td>
<td></td>
</tr>
<tr>
<td>1985</td>
<td>118,289,121</td>
<td>2.0</td>
<td>120,730,205</td>
<td>2.8</td>
<td>113,832,113</td>
<td></td>
</tr>
<tr>
<td>1986</td>
<td>122,789,249</td>
<td>3.8</td>
<td>124,625,693</td>
<td>3.2</td>
<td>113,832,113</td>
<td></td>
</tr>
<tr>
<td>1987</td>
<td>127,086,765</td>
<td>3.5</td>
<td>126,899,632</td>
<td>1.8</td>
<td>113,832,113</td>
<td></td>
</tr>
<tr>
<td>1988</td>
<td>131,504,568</td>
<td>3.5</td>
<td>130,860,026</td>
<td>3.1</td>
<td>113,832,113</td>
<td></td>
</tr>
<tr>
<td>1989</td>
<td>136,114,201</td>
<td>3.5</td>
<td>134,685,732</td>
<td>2.9</td>
<td>113,832,113</td>
<td></td>
</tr>
<tr>
<td>1990</td>
<td>139,412,884</td>
<td>2.4</td>
<td>139,613,309</td>
<td>3.7</td>
<td>113,832,113</td>
<td></td>
</tr>
<tr>
<td>1991</td>
<td>143,341,581</td>
<td>2.8</td>
<td>142,367,463</td>
<td>2.0</td>
<td>113,832,113</td>
<td></td>
</tr>
<tr>
<td>1992</td>
<td>148,106,159</td>
<td>3.3</td>
<td>147,033,132</td>
<td>3.3</td>
<td>113,832,113</td>
<td></td>
</tr>
<tr>
<td>1993</td>
<td>153,447,946</td>
<td>3.6</td>
<td>151,543,061</td>
<td>3.1</td>
<td>113,832,113</td>
<td></td>
</tr>
<tr>
<td>1994</td>
<td>159,658,862</td>
<td>4.0</td>
<td>158,152,644</td>
<td>4.4</td>
<td>113,832,113</td>
<td></td>
</tr>
<tr>
<td>1995</td>
<td>166,445,580</td>
<td>4.3</td>
<td>165,350,308</td>
<td>4.6</td>
<td>113,832,113</td>
<td></td>
</tr>
<tr>
<td>1996</td>
<td>173,866,799</td>
<td>4.5</td>
<td>173,857,193</td>
<td>5.1</td>
<td>113,832,113</td>
<td></td>
</tr>
<tr>
<td>1997</td>
<td>179,849,045</td>
<td>3.4</td>
<td>180,516,161</td>
<td>3.8</td>
<td>113,832,113</td>
<td></td>
</tr>
<tr>
<td>1998</td>
<td>185,002,911</td>
<td>2.9</td>
<td>186,594,497</td>
<td>3.4</td>
<td>113,832,113</td>
<td></td>
</tr>
<tr>
<td>1999</td>
<td>189,397,096</td>
<td>-1.6 %</td>
<td>188,499,586</td>
<td>1.9</td>
<td>187,581,092</td>
<td>0.5</td>
</tr>
<tr>
<td>2000</td>
<td>192,432,431</td>
<td>-0.4</td>
<td>185,587,160</td>
<td>-1.5</td>
<td>179,811,283</td>
<td>-4.1</td>
</tr>
<tr>
<td>2001</td>
<td>189,750,143</td>
<td>-1.2</td>
<td>180,095,333</td>
<td>-3.0</td>
<td>177,745,546</td>
<td>-4.2</td>
</tr>
<tr>
<td>2002</td>
<td>182,933,281</td>
<td>-3.3</td>
<td>173,140,710</td>
<td>-3.9</td>
<td>161,374,473</td>
<td>-6.3</td>
</tr>
<tr>
<td>2003</td>
<td>177,690,711</td>
<td>-2.9</td>
<td>165,979,938</td>
<td>-4.1</td>
<td>154,039,066</td>
<td>-4.5</td>
</tr>
<tr>
<td>2004</td>
<td>175,160,940</td>
<td>-1.4</td>
<td>157,037,503</td>
<td>-5.4</td>
<td>147,993,264</td>
<td>-3.9</td>
</tr>
<tr>
<td>2005</td>
<td>167,504,016</td>
<td>-4.4</td>
<td>146,848,926</td>
<td>-6.5</td>
<td>140,029,044</td>
<td>-5.4</td>
</tr>
</tbody>
</table>

---

$^1$ CLEC and ILEC Lines

$^2$ ILEC Local Loops

$^3$ ILEC Access Lines
How it Works: Traditional Banking ATM & Teller Using Dial and Wired Service
How it Works: Typical Bank ATM & Teller Using Internet
Typical Wireless Network Design
“Third Generation” Digital

3G Network Architecture Model

RAN (Radio Access Network)
- Node-B
- Base Station
- Radio Network Controller

CN (Core Network)
- Packet Switch Domain
  - SGSN
  - GGSN
  - IMS
- Circuit Switch Domain
  - MSC
  - GMSC

INTERNET
PSTN

MSC: Mobile Switching Center
GMSC: Gateway Mobile Switching Center
SGSN: Service GPRS Support Node
GGSN: Gateway GPRS Support Node
IMS: IP Multimedia Subsystem
Putting it all together: From Bank to Mobile Customer
Is Mobile Banking Safe?

Pros:
- Handsets have 2 forms of Unique ID
- Network Operator can Monitor Use 24/7 (customer consent?)
- Few known mobile viruses or malware, BUT ...
- Diversity of networks/handsets/applications (no one target for bad guys)

Cons:
- Radio signals can be intercepted (but, digital can be encrypted)
- Handsets can be lost
- Public perception is that PCs are “safer” than mobile phones
- More targets due to mobile’s popularity
Q: Who Regulates Mobile Banking?

- A: No One. No Legal Framework is Specific to Mobile Banking
- Many Agencies “Involved” in Mobile Finance Transactions: Federal Reserve, FCC, FTC, SEC, FDIC, OTC, OCC, NCUA
- Financial Services Sector and Mobile Wireless Sector Subject to Starkly Different Regulatory Environments
Regulatory Framework for Wireless Carriers:

- Federal Communications Commission’s Plenary Authority: Title 3/Radio Licensing/the Communications Act
- Section 332: States preempted from “rate and entry” regulation of wireless carriers
  - But, “other terms and conditions” of service can be determined by states/PUC/police powers
- Title 2 of Act also applies: Wireless Carriers are “Telcom Common Carriers”
Legal/Regulatory Characteristics of Wireless Industry Relevant to Mobile Banking

- Telecom Common Carriers: Limited Liability
- Mobile Rates: Market Dictates/Essentially Unregulated
- Multiple Carriers/Marketplace Dictates Service Standards (for now); FCC has no minimum service standards
- State PUCs/Congress threaten “wireless customer rights”
- Different Digital Standards (CDMA/GSM/WiMAX/LTE) begat Compatibility Problems (U.S. laws don’t require one format)
- Carriers Rely on 3d Parties for Network and Handset Hardware and Applications (FCC has limited jurisdiction)
- Potential Liability for Conduct Outside “Common Carrier” Role
- Business Reputational Risk
Wireless Carrier Concerns Related to Mobile Banking:

- Network Security, Capacity and Control
- Customer Privacy and Consents (but remedies mainly statutory, and, differs from bank privacy)
- Liability (but, Limited Liability for transmissions)
- Fraud Prevention
- Interoperability/Standardization
- Ease of Use
- Parental Controls
- Financial Risks/Rewards
- Potential for Unwanted Regulation
Wireless Industry “Best Practices” for Mobile Financial Services

- Service Guidelines/Best Practices (CTIA, Jan 2009)
- Ensure that Liability Rests with Service Providers
- Clear & Conspicuous Disclosures to Users
- Extra Layer of Security for Financial Data
- Fraud Prevention (fraud vs. carriers = $30-40B annum)
- Compatibility Standards: Networks & Handsets
- Collection, Use and Control of Data
- Customer Service/Complaints
Regulatory Framework for Banking Institutions

- Financial Institutions Far More Heavily Regulated Than Telcos
- Virtually All Areas of Operations Subject to Laws, Regulations, “Guidelines”, Supervisory Expectations, or a Combination of the Foregoing
Regulatory Framework for Banking Institutions (cont’d)

- Laws, Regulations, Guidelines Relevant to Mobile Banking Include:

- INFORMATION SECURITY/ PRIVACY
  - Gramm-Leach-Bliley Act, Section 501 (15 U.S.C. 6801) declares a Congressional policy that financial institutions have an affirmative obligation to “respect the privacy of . . . customers and to protect the security and confidentiality of those customers’ nonpublic personal information.”
Regulatory Framework for Banking Institutions (cont’d)

- Law requires the agencies to establish appropriate standards for financial institutions relating to administrative, technical, and physical safeguards—
  - (1) to insure the security and confidentiality of customer records and information;
  - (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
  - (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.
Regulatory Framework for Banking Institutions (cont’d)

- The banking agencies have promulgated Interagency Guidelines Establishing Information Security Standards
  - 12 CFR Part 30, Appendix B (national banks)
  - 12 CFR Part 208, Appendix D-2 (state member banks)
  - 12 CFR Part 364, Appendix B (state nonmember banks)
  - 12 CFR Part 570, Appendix B (savings associations)
Regulatory Framework for Banking Institutions (cont’d)

- ANTI-MONEY LAUNDERING/BANK SECRECY ACT COMPLIANCE

  - Under 31 USC § 5311 et seq., including customer identification requirements imposed by Section 326 of the USA PATRIOT Act, codified at 31 USC § 5318(l), financial institutions are subject to stringent requirements regarding customer identification, prevention of money laundering and other illegal transactions.

  - Regulations at 31 CFR Part 103
Regulatory Framework for Banking Institutions (cont’d)

- Establishes a general rule (with various exceptions) that financial institution is liable to a consumer for all damages proximately caused by the financial institution’s failure to make an electronic fund transfer, in accordance with the terms and conditions of an account, in the correct amount or in a timely manner when properly instructed to do so by the consumer.
- Regulation E implements EFTA, 12 CFR Part 205.
Regulatory Framework for Banking Institutions (cont’d)

- Electronic Fund Transfers under Regulation E
  - Pro-consumer: The “primary objective” of the Electronic Fund Transfer Act and the regulation “is the protection of individual consumers engaging in electronic fund transfers.”
  - Consumer liability is generally very limited.
  - Wireless carriers “off the hook”?
Regulatory Framework for Banking Institutions (cont’d)

- BANKING AGENCY EXPECTATIONS REGARDING BANKS’ MANAGEMENT OF SERVICE PROVIDERS AND OTHER THIRD PARTY RELATIONSHIPS
Regulatory Framework for Banking Institutions (cont’d)

- OVERARCHING REQUIREMENT OF OPERATING IN A SAFE AND SOUND MANNER
  - “Safety and Soundness” Concerns Pervade Banking Law and Regulation.
  - Interagency guidelines promulgated by all federal banking agencies
Banking Institution Concerns

- Demographics/Technology Trends/Competition/ROI
- Managing Mobile Banking Relationships Profitably And In Compliance with Regulatory Requirements
- Risks/Rewards Analysis Differs from Wireless Carriers’ (Carriers Generate Revenue with Every Transaction)
Banking Sector: Mitigating the Risks

- Understanding the Technology
- Contractual Solutions
  - Contracts with Telcoms
  - Consumer Contracts
- Uniform Technical Standards/Protocols
- Legislative/Regulatory Change
Questions?

Rick Joyce
rjjoyce@venable.com
(202) 344-4653

Peter Heyward
peheyward@venable.com
(202) 363-8565
Mobile Banking

BY VENABLE'S TELECOMMUNICATIONS AND FINANCIAL SERVICES GROUPS
MOBILE BANKING: CHALLENGES & OPPORTUNITIES

Financial transactions that are based on wireless handsets may soon prove to be as pervasive as Internet-based financial applications. Recent surveys indicate that as many as seven percent of mobile phone customers use their handsets for mobile banking. While mobile banking technology is still in a developmental stage, that is most certainly true for the legal and regulatory framework that governs these services.

The term "Mobile Finance" encompasses a wide array of services and products of interest to financial services institutions: Mobile Banking, Mobile Payments/Fund Transfers and Mobile Commerce. The common element is that a handheld wireless device is used by the customer to initiate a financial transaction. In this article, we examine some of the many legal and technical challenges that will need to be met before Financial Institutions can safely deploy mobile transactions on a wide scale to their interested customers.

CATCHING THE WIRELESS WAVE

Demographic and technological trends suggest that financial institutions can't afford to sit out the Mobile Banking wave waiting for a number of technical, legal and regulatory issues to be sorted out. Traditional wireline phone services are declining at an annual rate of six to seven percent per year; meanwhile, wireless market share continues to grow at roughly 10 to 15% per year. In the United States alone, 85% of the population now has at least one wireless phone; 16% of the population uses only a wireless carrier for their home service. Overseas, these trends are even more pronounced; some countries have over 100% wireless market penetration, meaning that the average consumer pays for more than one wireless device.

The manner in which wireless devices are being used has also changed in a relatively short period of time. Text messaging and data services are growing as a source of revenue for wireless carriers at exponential rates, compared to traditional voice services. There can be no doubt that consumers will soon consider their portable wireless devices to be an alternative means of access to their accounts, if not a complete substitute for the personal computer. To the extent that the financial services industry is not prepared to make the mobile banking experience as easy, painless and reliable as the online banking experience,
there could be substantial room for consumer disappointment, and product differentiation, much sooner than most bankers would like to consider.

At the same time, it is by no means apparent whether these mobile services will prove to be profit centers, or sunken costs, for Financial Institutions. By contrast, from the wireless carrier’s perspective, even if mobile banking products are not priced at a premium to the wireless customer, carriers will benefit from the additional data/airtime charges that will be incurred by consumers every time they initiate a wireless transaction.

**NETWORK COMPLICATIONS**

Financial services companies that provide their customers with Mobile Finance services are accustomed to regulatory disclosures and consumer protection requirements that apply to electronic delivery of services. In Mobile Finance, they also need to be mindful of three distinct communications networks that play a part in originating and terminating mobile finance transactions: the traditional wireline network (a.k.a. the “Public Switched Telephone Network”), the Internet, and wireless cell phone/PCS networks.

Unlike the early days of electronic funds transfers, when Financial Institutions were working mainly with one monopoly phone company, there are far more carriers to deal with today to make Mobile Banking a reality. Most parts of the country are served by more than one wireless carrier, each with proprietary technology and their own ways of doing business. Throughout each of these three layers of communications, there are a wide array of legacy regulations and technologies to contend with before a Mobile Banking transaction can be initiated and completed. Safe, secure and cost-effective deployment of Mobile Finance services requires an understanding of how all of these networks inter-operate.

**ABSENCE OF UNIFORM STANDARDS**

Financial Institutions find today’s environment for these services to be far different from the Electronic Funds Transfer networks of last century, which evolved using essentially open standards designed around one phone company. Today, the communications platform is dramatically different; each community is served by multiple wireline, wireless and cable carriers; and, there are a wide array of vendors trying to promote their proprietary mobile banking products. Moreover, there are no uniform regulations – or even industry guidelines – to consult for anyone interested in offering mobile banking services to their customers.

What we have instead today is a bewildering array of proprietary arrangements, typically led by a wireless carrier and a third party vendor. Financial Institution customers subscribe to one or more of at least four different nationwide wireless carriers. Consequently, banks that want to make mobile banking available to all of their customers must deal with four or more wireless
carriers to initiate even the simplest mobile transaction.

**COMMON CONCERNS, COMMON OBJECTIVES**

Despite differing cost/benefit analyses, there are quite a few areas of concern that are common to financial institutions and wireless service providers. It is precisely because of these common concerns that the two sides would seem to have incentives to jointly face these issues and come up with bilateral solutions as soon as possible. Here's a list of just a few of the problem areas that need to be addressed for the safe and functional deployment of Mobile Banking products and services:

- Network Security, Capacity and Control
- Customer Privacy and Informed Consent
- Liability
- Fraud Prevention/Authentication
- Interoperability/Standardization
- Data Access and Use
- Parental Controls
- Financial Risks/Rewards

**WIRELESS CARRIER'S VIEWPOINT**

Although bankers and wireless carriers do have common areas of concern, there is no doubt that these are also entirely different industries in ways that have created fundamental tensions for Mobile Bank services. One area of tension has to do with customer "ownership." Unlike a typical ATM or electronic funds transfer situation, where the banking customer is for the most part indifferent about the back-office telephony network that is handling the transaction, the bank customer has an established billing or service relationship with a particular wireless carrier in Mobile banking transactions. Not surprisingly, wireless carriers want to both exploit and protect that relationship.

Wireless carriers also have decidedly different legal risks and obligations with respect to mobile transactions. Fundamentally, they are common carriers that, by law, have only limited liability for the data that traverses their networks. Other than in extraordinary circumstances, wireless carriers have no legal responsibility to a consumer if a call or transmission is completed other than to reimburse that customer for any service charges incurred. This is dramatically different for financial institution's where the customer's expectation, and the financial institution's legal obligation once the customer's order is received, is to complete each financial transaction initiated by the customer.

At the same time, wireless carriers are subject to a wide array of federal, and to a lesser extent state, laws and regulations governing the way in which they handle customer information. These legal obligations create inherent tensions in the way that wireless carriers work with financial institutions in the Mobile Banking world. For instance, some customer information that would be terribly useful to Financial Institutions for purposes of authenticating transactions would be deemed "customer
proprietary network information” under federal communications laws. This information cannot be given out to third parties by wireless carriers without the customer’s consent.

Wireless carriers, because they are common carriers, have a legal obligation to make their services available to any interested customer on “just, reasonable and non-discriminatory terms,” according to the federal Communications Act. But, many financial institutions have found this legal obligation to be a hollow promise; some carriers have simply refused to allow bank-initiated products to be downloaded and deployed over proprietary wireless networks. It remains to be seen whether the Federal Communications Commission, or other state or federal regulators, may be called upon to resolve these smoldering disputes.

FINANCIAL INSTITUTION CONCERNS

The financial services sector may share some things in common with wireless carriers, particularly with regard to risk management and consumer protection but, pretty soon, the similarities end. Understandably, financial services companies view these transactions as not merely another application; rather, every mobile finance transaction runs to the very heart of their raison d’être: to initiate and complete safe and secure transfers of money. If even one of these transactions goes awry, they have much more at stake than simply reimbursing a customer for a $1.50 transaction fee. For Financial Institutions, mobile banking and mobile finance raise a number of legal, regulatory and operational issues that have yet to be resolved on a comprehensive basis.

Security, Security, Security

When a consumer identifies a transaction as an unauthorized electronic fund transfer, there is only nominal liability under Regulation E. Unlike the closed ATM and credit and debit card networks, the use of wireless technology creates additional risk that information (not limited to financial transaction information) will be stolen, triggering concerns under the privacy provisions of the Gramm-Leach-Bliley Act, as well as the Fair and Accurate Credit Transactions Act amendments to the Fair Credit Reporting Act. Without the use of highly secure encryption technology to prevent third party data intrusion and losses, the ubiquitous tools of Mobile Finance open the door to enormous potential for monetary as well as reputational risk.

Examiners can be expected to demand proof that the security of a Financial Institution’s Mobile Banking products and services are commensurate with the size of the Financial Institution as well as the complexity of the products and services offered. Moreover, the duty does not end with the download of the security system offered as part of the Mobile Finance package. It is an ongoing process of monitoring, evaluating and adjusting to new threats. This means that the Financial Institution must have an ongoing capability to download upgrades, patches and changes to its Mobile Banking product which the customer must
install to continue using the product.

Customer Authentication

One of the most difficult problems facing banks is the issue of customer authentication. While in many ways a mobile handset is inherently more secure than a desktop computer (for instance, the handset is assigned a distinct telephone number and is owned by a customer with a regular billing or service arrangement with a particular mobile services carrier), the mobility of the device and the nature of wireless communications create additional authentication and security issues for financial institutions and their customers.

At the outset, the Financial Institution has to consider its obligations under the USA PATRIOT Act to correctly identify the party seeking Mobile Banking services to access an account. The now familiar “Know Your Customer” rules must be reviewed to see whether and how the Financial Institution providing a Mobile Banking service can accurately determine the identity of an existing customer. Will it provide the service at account opening or only after services are established and a relationship formed, e.g., after 30 days? Will the traditional account number, PIN and test questions suffice for authentication? Will a Financial Institution treat a request to change phone numbers as a "Red Flag"?

As is the case with all electronic transactions (wire transfers, ACH and internet banking, for instance), money laundering is also a significant concern in Mobile Banking. The Financial Institution must integrate Mobile Banking into its BSA, AML and OFAC compliance programs. Given that each mobile handset to an extent represents its own teller window, the prospects for financial mischief on a broad scale by techno-savvy bad-guys is very real.

Obviously, security issues need to be resolved across the board before you can safely provide these services to even one customer; hence, there are up-front costs that can be intimidating, particularly for smaller financial institutions. Moreover, some regulatory requirements with respect to customer security can exacerbate these costs, making Mobile Banking a costly option for some institutions.

Given the ambulatory nature of mobile devices, you also have to take into consideration the possibility that a device can be used in a foreign country to initiate a financial transaction. Consequently, security and regulatory compliance issues have to be mindful of international laws and international banking regulations.

Clearing and Settlement

The U.S. and many countries have a variety of advanced electronic payment laws and regulations. These laws and regulations govern the clearing and settlement of transactions between banks.
Mobile Banking services must have the ability to track each transaction throughout the payment stream, recreate the path of commerce, and allocate responsibility for errors, including unauthorized transfers. All of this must be documented on a periodic statement with the information required by Regulation E in consumer transactions.

While commercial transactions may not be covered by similar disclosure and error resolution requirements, businesses are likely to demand that Mobile Banking services be integrated with positive pay and other advanced fraud detection and prevention tools commonly used in the clearing and settlement process. Before Mobile Banking products and services can be rolled out, they will have to be in compliance with these laws and regulations.

**Liability/Dispute Resolution**

One of the distinct areas of tension between Financial Institutions and mobile services providers with respect to mobile banking and mobile finance has to do with risk allocation and liability. In a variety of different ways, Financial Institutions are responsible for ensuring that banking transactions are properly initiated and closed. For a variety of different financial transactions, such as those involving ATMs and credit cards, there are detailed laws and regulations regarding the liabilities of financial institutions.

Mobile carriers, on the other hand, are by law deemed to be "limited liability" entities; they have no affirmative obligation to do anything but to ensure that a voice or data communication is originated and terminated, and to refund the calling party for the cost of that transmission if the communication fails. As the volume of mobile banking and mobile finance traffic increases, the tension inherent in this risk allocation is likely to grow; financial institutions will undoubtedly be interested in seeing that these risks are shared in ways not currently required by law.

**Customer Ownership/Funds Management**

Organizations that take deposits from customers and hold them on their behalf are the core concern of U.S. and international banking regulators. Mobile Banking and finance create interesting challenges to this model because, as a practical matter, a mobile banking customer is simultaneously doing business with both a financial institution and a mobile carrier. But, mobile carriers are not, at present at least, regulated by the same institutions that regulate banks.

When deploying Mobile Banking solutions, many unanswered questions remain as to who will be responsible to financial regulators for all aspects of transactions that employ a "mobile wallet" or pseudo bank account. Regulatory responsibility will also be of interest in those instances where clearing a financial transaction is delayed for some period of time due to wireless technology or network problems.
NEXT STEPS FOR MOBILE BANKING

Clearly, there are many daunting issues that need to be addressed before Mobile Banking can become as ubiquitous, safe and seamless as other forms of electronic funds transfer. From the wireless carriers’ perspective, they have already begun to formulate "best practices" under the aegis of industry trade associations, with informal input from the Federal Communications Commission. For now, unless something goes decidedly wrong in one or more of these wireless transactions, there is no sign that the FCC intends to take a more aggressive regulatory role with respect to Mobile Banking. And it is by no means clear what, if any, role the FCC might take in mediating any disputes that may arise between Financial Institutions and wireless carriers as Mobile Banking services are deployed.

From the Financial Institution’s perspective, there’s much work to be done before Mobile Banking and mobile finance services will be on a par with other forms of electronic funds transfer. At a minimum, "best practices" for the financial services sector would be a welcome start toward the creation of safe and reasonable Mobile Banking procedures.

At the same time, the Federal Reserve Board and other significant regulatory entities are taking a close and concerned look at Mobile Banking services and transactions. Whether the banking regulators will take steps to expand their current guidance on electronic banking (see the current guidance on e-Banking and related issues at http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html) to address the unique aspects of Mobile Banking remains to be seen. In any event, financial services entities would be well-advised to formulate their own self-regulatory practices, before the government does it for them.
Best Practices and Guidelines

for

Mobile Financial Services


Effective Date: January 28, 2009
# TABLE OF CONTENTS

Section 1 - Purpose ................................................................................................................ 1  
Section 2 - Applicability ........................................................................................................ 1  
Section 3 – Guidelines ........................................................................................................... 2  
  A. Guidelines Specific to Mobile Banking and Mobile Payments ................................. 2  
     1. Authentication and Authorization .............................................................. 2  
     2. Banking and Payment Alerts; Transaction Records................................... 2  
     3. Limiting Liability for Unauthorized Transactions ................................. 3  
  B. Guidelines Specific to Mobile Commerce ................................................................. 3  
     1. Disclosure of Material Terms of Purchase ................................................. 3  
     2. Obtaining User Authorization .................................................................... 3  
     3. Receipts, Order Status and Account Information ....................................... 3  
     4. Mobile Coupons, Rebates, Loyalty Programs, etc. .................................... 3  
     5. Minors ......................................................................................................... 4  
  C. General Guidelines ............................................................................................ 4  
     1. Disclosure of Terms; Disclaimers .............................................................. 4  
     2. Consent to Enrollment in MFS ................................................................. 4  
     3. Compliance with Laws and Regulations .................................................... 4  
     4. Security of Data Transmissions ................................................................. 5  
     5. Security on the Mobile Device or in Storage ............................................. 5  
     6. Access Controls and Security of Sensitive Information ............................ 5  
     7. Fraud and Identity Theft Protection ........................................................... 6  
     8. Collection, Use, and Disclosure of Information ......................................... 6  
     9. Dispute Resolution Processes and Customer Service ............................... 6 
Section 1 - Purpose

Mobile financial services (“MFS”), such as mobile banking, mobile payments and mobile commerce, represent a growing and promising class of mobile services for consumers. CTIA, in association with the leading U.S. wireless carriers, has developed these Best Practices and Guidelines (“Guidelines”) to promote clear and rewarding consumer experiences, to establish an environment where MFS transactions are authorized, secure, and compliant with applicable laws and industry guidelines, and to protect user privacy and financial data.

Section 2 - Applicability

These Guidelines apply to MFS Providers. MFS Providers are the parties that provide MFS to mobile users or provide back-end services supporting MFS transactions. Wireless carriers can be MFS Providers in certain circumstances, but do not constitute MFS Providers for purposes of these Guidelines merely because they provide wireless data services, application provisioning services, or similar standard functions to mobile users and MFS Providers.

Examples of MFS Providers:

1) A financial institution that provides its banking, brokerage or other financial services (e.g., account balance inquiry, bill payment) via the mobile channel is an MFS Provider.

2) A software developer or platform provider that develops and/or supports mobile banking or mobile payment services on behalf of financial institutions is an MFS Provider.

3) A provider of an online payment service (e.g., online commerce, bill payment, person-to-person transfer) that provides such services via the mobile channel is an MFS Provider.

4) A payment card issuer or payment network that provides credit cards, debit cards, stored value cards, or transit fare intended to be provisioned to mobile handsets is an MFS Provider.

5) A provider of an application for mobile parking meter payments is an MFS Provider.
Section 3 – Guidelines

A. Guidelines Specific to Mobile Banking and Mobile Payments

1. Authentication and Authorization

MFS Providers should use methods consistent with industry best practices to authenticate user identity and obtain user authorization for mobile banking and mobile payment transactions.

Examples of industry best practices may include multifactor authentication, PINs, shared secrets, challenge questions, one-time use passwords and codes, and express authorization of transactions.

2. Banking and Payment Alerts; Transaction Records

MFS Providers should provide controls that allow users the ability to receive banking and payment alerts and notices in accordance with user preference. MFS Providers should also provide systems that allow users to access transaction records and other information about their accounts.

Industry Guidelines for MFS Providers
3. Limiting Liability for Unauthorized Transactions

MFS Providers of mobile payment systems should disclose all material information regarding the liability, if any, that the user may have for unauthorized transactions or fraudulent use. MFS Providers of mobile payment systems should create policies that cap liability for unauthorized transactions. Such policies should, at a minimum, comply with liability caps required under existing legal requirements (e.g., $50 or other applicable liability cap for unauthorized credit card transactions or electronic funds transfers). MFS Providers should consider incorporating into the MFS controls that limit financial risk to the consumer, such as usage caps and spending limits.

B. Guidelines Specific to Mobile Commerce

1. Disclosure of Material Terms of Purchase

MFS Providers should disclose, in a clear and conspicuous manner, the material terms of each purchase, including a description of the product or service being purchased, taxes, surcharges, and other fees, and refund policies. This may include disclosures off of the mobile device.

2. Obtaining User Authorization

MFS Providers should obtain user authorization for purchases, consistent with industry best practices.

Examples of industry best practices may include express authorization of transaction, confirmation screen, transaction cancellation option, and opt-in for subscription services.

3. Receipts, Order Status and Account Information

MFS Providers should make receipts or proofs of purchase available for mobile purchases. MFS Providers should also provide systems that allow users to access order status and other information about their accounts. The appropriate methods of presenting such information (e.g., via an SMS message, email, on a website, on the mobile service bill, paper receipt, etc.) and the level of information available will vary depending upon the type of service.

4. Mobile Coupons, Rebates, Loyalty Programs, etc.

MFS Providers should disclose, in a clear and conspicuous manner, the material terms of mobile coupons, rebates, loyalty programs and similar products. Such terms include redemption values, expiration dates, fees, limitations on use and other restrictions.
5. Minors

MFS Providers of age-restricted products, services or applications must include clear and conspicuous warnings and use appropriate methods of age-screening or verification before allowing purchase.

C. General Guidelines

1. Disclosure of Terms; Disclaimers

The identity of the MFS Provider and all material terms relevant to an MFS should be disclosed in a clear and conspicuous manner to users prior to their use of the service. Such disclosures should include applicable disclaimers.

Examples of material terms and disclaimers may include a description of the MFS, terms of use, applicable fees, purchase price, method and frequency of billing, use restrictions and limitations, liability caps, and disclaimers of liability and warranties.

2. Consent to Enrollment in MFS

MFS Providers should obtain affirmative consent from the user for the enrollment of the user in an MFS. Notice should be given to the user that will allow the user to make an informed decision prior to taking any action that will result in the user incurring a charge (e.g., a charge for text message that contains confirmation of a transaction, for data plan usage after enrollment, or to a wireless or payment account).

3. Compliance with Laws and Regulations

It is the responsibility of each MFS Provider to provide the products, services, software, and/or hardware provided by that MFS Provider in accordance with all applicable local, state, and federal laws, payment network rules, and mobile industry best practices guidelines.

Examples of laws, regulations and mobile industry best practices guidelines that may apply to MFS Providers include, but are not limited to: state and federal banking laws, the Electronic Funds Transfer Act, Regulation E, the Bank Secrecy Act, federal Money Services Business laws, state money transmitter laws, the Truth in Lending Act, the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act (GLBA), state gift certificate laws, federal and state debt collection laws, NACHA - The Electronic Payments Association (NACHA) rules, Federal Financial Institution Examination Council (FFIEC)

4. Security of Data Transmissions

MFS Providers should utilize industry best practices when providing security of data during transmission. MFS Providers should not rely solely on GSM, CDMA or other wireless network security.

Examples of industry best practices may include encryption, hashing or compensating controls to create secured sessions.

5. Security on the Mobile Device or in Storage

MFS Providers should use industry best practices to protect against unauthorized access to MFS data on a mobile device or in other storage locations. Such protections may include mechanisms for keeping software applications separate, keeping MFS data and MFS communications secure, and protecting memory from unauthorized access or modification.

Examples of industry best practices may include PIN protection, remote device disabling or wiping, and encryption of sensitive information on the device.

6. Access Controls and Security of Sensitive Information

MFS Providers should offer access control options and tools that enable users to protect their data and to limit unauthorized party access to sensitive information on the device. MFS Providers should educate users on the importance of protecting their personal information, and how to use application security features and capabilities.

Examples of sensitive information include Social Security numbers, bank account numbers, PINs, passwords, and personally identifiable information. Personally identifiable information may include any information that could be used to create a fraudulent identity or transaction.

Examples of tools for protection of personal information may include encryption, hashing or compensating controls, and password protection.
7. **Fraud and Identity Theft Protection**

MFS Providers should incorporate into their MFS fraud-prevention techniques and offer tools to protect users’ information, funds, credit, and identities.

*Examples of fraud-prevention techniques and tools may include proactive user identification, detection and response to transaction/use patterns, practices or specific activities, customer ability to place limitation on spending, etc.*

8. **Collection, Use, and Disclosure of Information**

(a) **Information Use.** MFS Providers should provide clear disclosures about their access, collection, use, storage and disclosure of personally identifiable information. The MFS Provider should not access, collect, use, store or disclose the personally identifiable information for any purpose other than provision of the MFS, unless it provides appropriate notice and obtains consent from users. Such notice should explain, for example, the other intended uses (e.g., the use of the information for advertising) of the information. MFS Providers that use the information collected to create aggregate data should remove or permanently obscure the consumer’s identity and provide clear notice of such aggregation and use.

(b) **Security Incident.** In the event of a security breach, MFS Providers should notify consumers of such breach in accordance with relevant breach notification laws. MFS Providers should respond to the breach as the responsible party. Although wireless carriers are not responsible for providing notice, the MFS Provider should coordinate and collaborate with wireless carriers to ensure the wireless carriers are prepared for inquiries related to the incident. The MFS Provider should be the user’s main point of contact regarding the breach, and the wireless carriers should not be referenced in any breach notice.

9. **Dispute Resolution Processes and Customer Service**

MFS Providers should develop reasonable dispute resolution processes for handling disputed payments and transactions. MFS Providers also should have processes in place to address general customer complaints related to the use of the MFS. MFS Providers should provide customer service via an appropriate method (phone, online, SMS, etc.) and at commercially reasonable times. Responses to inquiries should be made in a reasonably expedient manner and as appropriate for that MFS. MFS Providers should make customer service contact information readily available so that customer service requests can be properly directed.