VENABLE LLP

white paper

NOVEMBER 2008

Mobile Banking

BY VENABLE'S TELECOMMUNICATIONS AND FINANCIAL SERVICES GROUPS

MOBILE BANKING TASK FORCE

Frederick ("Rick") M. Joyce, Esq.
rjoyce@venable.com
202.344.4653

Bruce Jolly, Esq.
bojolly@venable.com
202.344.4818

Ralph Sharpe, Esq.
resharpe@venable.com
202.344.4344

Ed Wilson, Esq.
dewilson@venable.com
202.344.4819

Joseph Lynyak, Esq.
jtlynyak@venable.com
310.229.9660

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.

Venable office locations

BALTIMORE, MD
750 E. PRATT STREET
SUITE 900
BALTIMORE, MD 21201
t 410.244.7400
f 410.244.7742

LOS ANGELES, CA
2049 CENTURY PARK EAST
SUITE 2100
LOS ANGELES, CA 90067
t 310.229.9900
f 310.229.9901

NEW YORK, NY
ROCKEFELLER CENTER
1270 AVENUE OF THE AMERICAS
TWENTY-FIFTH FLOOR
NEW YORK, NY 10020
t 212.307.5500
f 212.307.5598

ROCKVILLE, MD
ONE CHURCH STREET
FIFTH FLOOR
ROCKVILLE, MD 20850
t 301.217.5600
f 301.217.5617

TOWSON, MD
210 ALLEGHENY AVENUE
TOWSON, MD 21204
t 410.494.6200
f 410.821.0147

TYSONS CORNER, VA
8010 TOWERS CRESCENT DRIVE
SUITE 300
VIENNA, VA 22182
t 703.760.1600
f 703.821.8949

WASHINGTON, DC
575 SEVENTH STREET NW
WASHINGTON, DC 20004
t 202.344.4000
f 202.344.8300