

THE REVIEW OF
**BANKING & FINANCIAL
SERVICES**
A PERIODIC REVIEW OF SPECIAL LEGAL DEVELOPMENTS
AFFECTING LENDING AND OTHER FINANCIAL INSTITUTIONS

Vol. 25 No. 10 October 2009

MOBILE BANKING: THE LIABILITY GAP

Banking from mobile phones is on the rise, but the responsibilities for electronic fund transfers are more clearly defined and more extensive for banks than for telecommunication carriers. The author discusses the legal framework for each group, focusing on the issues of liability, security, and customer identification.

By Frederick M. Joyce *

Financial transactions that are conducted using wireless handsets may soon prove to be as pervasive as Internet-based financial applications. Recent surveys indicate that as many as 10 million mobile phone customers already use their handsets for mobile banking, with growth projected at 50% per year.¹ Given the vast number of mobile phone customers in the United States and worldwide, this is a bank application that surely cannot be ignored.

Demographic and technological trends suggest that financial institutions cannot 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 6 to 7% per year;² meanwhile, wireless market share continues to grow at roughly 10 to 15% per year.³ In the United States alone, over 85% of the population now has

at least one wireless phone; and 18% of the population uses only a wireless carrier for their home service.⁴ 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.⁵

At the heart of mobile banking transactions are two entities that are governed under extraordinarily different legal and regulatory frameworks: financial institutions and wireless telecommunications carriers. While paired in their common efforts to make mobile banking transactions for their customers effortless and secure, the fact remains that no third body of law has evolved to address the unique legal issues created by mobile banking transactions. This article compares the legal and regulatory frameworks of financial institutions and communications carriers with respect to mobile banking transactions. That comparative analysis reveals some

¹ TowerGroup: U.S. Mobile Banking Forecast, 2008-13.

² Wireline Competition Bureau, Fed. Comm'n Comm'n § 16-4 tbl.16.2 (2008), available at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-284932A1.pdf.

³ Cellular Telephone Indus. Ass'n, Wireless Quick Facts (2008), available at http://www.ctia.org/media/industry_info/index.cfm/AID/10323.

⁴ *Id.*

⁵ Laura Wood, The Level of Wireless Penetration in Austria is Steadily Increasing, Reuters, Jan. 18, 2008, available at <http://www.reuters.com/article/pressRelease/idUS174710+18-Jan-2008+BW20080118>.

* FREDERICK M. JOYCE is the Chair of the Communications Practice Group at Venable LLP, in Washington, D.C. His e-mail address is rjoyce@venable.com. The author wishes to thank summer associate Matthew R. Farley for his assistance with this article.

IN THIS ISSUE

● MOBILE BANKING: THE LIABILITY GAP

fundamentals gaps in the law today with respect to legal liability arising from these transactions.

MOBILE BANKING PLATFORMS

Mobile banking provides unparalleled convenience. Financial institutions can now use a variety of mobile media channels to deliver their services. These delivery channels include Short Message Service (SMS), Wireless Application Protocol (WAP), and Mobile Client Applications (MCAs). These channels can be reduced to their basic technologies: text messaging (SMS), website navigation using an Internet browser (WAP), and software applications installed directly on the customer's mobile device (MCAs). The type of information and degree of interactivity varies from one platform to another, and each has its strengths and weaknesses. Generally speaking, mobile banking platforms have four objectives: affordability, ubiquity, security, and simplicity.⁶

Short Message Service, or SMS, is supported by most mobile phones; many financial institutions have already implemented SMS-based banking services. SMS is relatively easy to use and affordable. Using SMS, a financial institution can send a short message to customers or respond to a customer request for information, such as the location of a nearby ATM, the customer's account balance, or an unsolicited promotional message. These messages are usually limited to about 200 characters and are essentially text-message banking.

Perhaps the most common platform, Wireless Application Protocol, or WAP, has become fairly standard in the mobile phone market. WAP offers direct access to the Internet from a mobile device. In order to utilize this highly interactive platform, financial institutions must generally deal with a host of compatibility issues that reflect the diversity of access speeds, browsers, and technical capabilities mobile devices currently possess. In short, financial institutions must adapt their Internet-based banking services to allow mobile access via WAP.

Mobile Client Applications, or MCAs, are a rapidly budding segment of the mobile market. MCAs offer powerful and secure functionality. Once installed on a mobile device, consumers can access a multitude of banking services, and they can receive automatic

⁶ For comparison of these three mobile platforms, see Mobile Marketing Ass'n, *Mobile Banking Overview (NA) 1-7* (2009), available at http://www.mmaglobal.com/mbankin_goverview.pdf.

application updates and upgrades from their financial institution. MCAs provide the most secure mobile banking option, as they allow intensive authentication and data encryption capabilities.⁷

BANKING INDUSTRY OBLIGATIONS

From a financial institution's perspective, legal and operational issues surrounding mobile banking transactions fall into three broad categories: liability, security, and customer authentication. In each of these areas, the legal and commercial risks for telecommunications carrier are quite apart from those of financial institutions.

Liability

Regulation E establishes the rights, liabilities, and responsibilities of financial institutions and consumers in electronic fund transfer systems, such as automated teller machine transfers, telephone bill-payment services, and other electronic transfers to or from a financial account.⁸ The term "electronic fund transfer" generally refers to a transaction initiated via an electronic device – whether telephone, computer, or magnetic strip – that instructs a financial institution either to credit or to debit a consumer's asset account.⁹ Mobile banking transactions would appear to be readily covered within the intended scope of the regulation and corresponding statutory rule. Under the law and with few exceptions, a financial institution can be found liable for all damages caused by its "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."¹⁰

Given Regulation E's broad obligations, financial institutions may attempt to limit their liability, at least for matters beyond their reasonable control, by including disclaimers in their account agreements with customers, especially with regard to electronic transfers.

⁷ *Id.*

⁸ 12 C.F.R. § 205 *et seq.* (2009).

⁹ *Id.* § 205.2.

¹⁰ Electronic Fund Transfers Act (EFTA), 15 U.S.C. § 1693h (2006). Notably, the EFTA provides that financial institutions are not liable for technical malfunctions *known to the consumer at the time he attempts to initiate an electronic transfer*. *Id.* § 1693h(b)(2). So if a customer knows that the telecommunications carrier supplying his mobile banking service is faulty or anticipates problems, the bank could be wholly off the hook.

Notwithstanding a financial institution's Regulation E obligations, most banks routinely disclaim liability for completing fund transfers when, for a variety of reasons, it may be beyond the bank's reasonable ability to do so, such as due to problems involving the electronic transmission of financial transactions. But these disclaimers, coupled with a wireless telecommunications carrier's limited liability at law as discussed below, raise fundamental questions as to precisely who is legally liable to the customer in the event that a mobile banking transaction fails.

Security

When a consumer identifies a transaction as an unauthorized electronic fund transfer, there is only nominal consumer liability under Regulation E.¹¹ Yet, unlike the closed ATM and credit and debit card networks, the use of wireless technology may create additional risks that information, not limited to financial transaction information, might be stolen or interrupted. Without the use of encryption technology to prevent third-party data intrusion and losses, there is the possibility that the wireless transmission of sensitive financial data and funds transmissions could be at risk. Unfortunately, existing law and regulations provide little guidance as to who should bear the burden of securing these mobile banking transactions.

We do know that examiners¹² 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 institution, as well as the complexity of the products and services offered.¹³ Moreover, the duty does not end with the download of the security system offered as part of the mobile 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.

No comparable set of requirements has yet to be issued by the Federal Communications Commission, or any other regulatory entity, with regard to specific

network security efforts that telecommunications carriers should employ to safeguard mobile banking transactions. That is by no means to suggest that mobile carriers are not concerned about network security; it is just that they have historically not been regulated based on the content of their transmissions, which in the case of mobile banking happens to be the transfer of large sums of money.

Customer Authentication

One of the most difficult problems facing banks in the mobile banking setting 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, a 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.¹⁴ The 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.¹⁵ 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, clearing house, and internet banking, for instance), money laundering is also a significant concern in mobile banking. The financial institution must integrate mobile banking into its banking security act, anti-money laundering, and foreign assets control

¹¹ Electronic Fund Transfers Act, 15 U.S.C. § 1693g (2006) (limiting consumer liability to the lesser of \$50 or the value of the unauthorized transfer).

¹² FDIC examiners are authorized to conduct examinations or inspections of insured depository institutions on behalf of the FDIC. *See, e.g.*, 12 U.S.C. § 1820(b) (2006).

¹³ *Id.*

¹⁴ Title III of the USA PATRIOT Act, 115 Stat. 272, 301-400, relates to money laundering prevention and deals with identity considerations and bank security in general.

¹⁵ "Know your customer" is the due diligence and regulation that financial institutions must perform to identify their clients and ascertain relevant information pertinent to doing financial business with them. It is typically a policy implemented to conform to a customer identification program mandated under the Bank Secrecy Act and USA PATRIOT Act.

compliance programs.¹⁶ Since 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.

Given that mobile devices are ambulatory, financial institutions must also consider 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.

Fundamentally, a wireless telecommunications carrier's statutory obligations are almost the opposite of a financial institution's obligation with regard to customer authentication. A telecommunications carrier does not have an affirmative obligation to ensure that the party initiating a given call is a "good person"; indeed, the carrier does not even have the obligation to ensure that a party using a particular mobile handset is the same person that paid for that device and monthly airtime charges (if that were true, it would be illegal for friends and family members to share their cellphones). While there are certainly laws and regulations dealing with the criminal use of interstate telecommunications networks,¹⁷ until such time as law enforcement authorities inform a carrier that criminal activities are occurring over their networks (or, if the carrier happens to establish actual knowledge of such activities on its own), the telecommunications carrier's primary statutory obligation is to "furnish communications service" by wire or radio "upon reasonable request."¹⁸

Clearing and Settlement

Financial institutions must have the ability to track each mobile banking 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.¹⁹

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 safely and securely rolled out, they will need to be in compliance with these laws and regulations.

Mobile telecommunications carriers have somewhat similar legal and regulatory obligations, but for a different purpose. Their obligation to verify the origination and termination of a telecommunications call or transmission is mainly for purposes of accurately billing customers for the services rendered. To the extent that a transmission is not completed, regardless of the content of that transmission, the legal liability of telecommunications carriers is extremely limited as a matter of longstanding common law precedents and statutory law.

TELECOMMUNICATIONS CARRIER OBLIGATIONS

For financial institutions, the liability bar is high: once a customer's order is received, an institution is legally obligated to complete each financial transaction initiated by that customer. By contrast, although telecommunications carriers are expected to "furnish communications" services to all interested persons, their legal liability for failing to complete a telecommunications transaction (be it voice or data) is limited as a matter of law.

Telecommunications Carriers and Limited Liability

Title II of the Communications Act of 1934 prescribes the regulation of telecommunications common carriers, which are defined in a somewhat circular manner as "any person engaged as a common carrier for hire."²⁰ The Act limits liability for telecommunications carriers, but, only when they are acting in their capacity as communications carriers providing services to customers.²¹

The notion that communications carriers are limited liability creatures was first established more than a century ago in cases involving the early telegraph service. In *Primrose v. Western Union Telegraph*

¹⁶ The Office of Foreign Assets Control prohibits certain trade transactions with foreign entities as a part of the U.S.'s broader national security regulation. The Office of Foreign Assets Control ("OFAC") derives its power from a variety of federal laws, the most prominent being the Trading with the Enemy Act. 50 U.S.C. § 5 (2006).

¹⁷ See, e.g., 18 U.S.C. § 1343 (2006).

¹⁸ 47 U.S.C. § 201(a) (2006).

¹⁹ 15 U.S.C. § 1693c (2006).

²⁰ 47 USC 153(h) (2006).

²¹ *Id.* § 153(44) ("A telecommunications carrier shall be treated as a common carrier under this chapter only to the extent that it is engaged in providing telecommunications services.")

Company,²² the U.S. Supreme Court likened telegraph companies to railroad companies (also “common carriers”), noting that they are both “instruments of commerce ... bound to serve all customers alike, without discrimination.”²³ The Court noted that the concept of “limited liability” might be particularly apt for telegraph companies, compared to other forms of common carriers, due to the unique nature of the services they offer. Traditional common carriers, the Court observed, have actual possession of the carried goods and can estimate the value of those goods, taking commensurate precautions for highly valued products. By contrast, a communications carrier has no knowledge of a message’s value, the intrinsic value of the message is often time-sensitive and private, and negotiating an appropriate fee based on the message’s value is simply impracticable.²⁴ For these reasons, the Court found that the liability imposed on other types of common carriers (such as shippers) for lost or damaged goods or inadequate services should not apply to communications carriers.

Today, this limitation on liability applies to essentially all forms of telephone, satellite, and mobile telephone services, so long as the services are provided by “common carriers.” Numerous courts have affirmed that it is reasonable to limit a telecommunications carrier’s liability for the interruption of telephone services, whether wireline or wireless, with damages being limited to no more than the fee the customer would have paid had the call or transmission been completed.²⁵

Telecommunications carriers cannot entirely avoid all liability for failed transmissions over their networks. The limitation of liability must be *reasonable*. At law, reasonable limitation means exculpating conduct that does not entail “gross negligence” or “willful” interruption of service – in other words, pardoning simple negligence.²⁶ In practice, there are very few

exceptions to the limited liability rule. For one thing, it is rare for a telecommunications carrier to act in a grossly negligent²⁷ or willful manner when it comes to providing service to its customers. It is obviously in the best interests of telecommunications carriers to provide reliable service; departing from that standard, particularly in a highly competitive marketplace, such as mobile/wireless communications services, would be commercially unwise.

Even in those instances where a telecommunications carrier, to a plaintiff’s eye at least, appears to have met the gross negligence standard, the courts have routinely declined to find the carrier liable.²⁸ Indeed, reported instances of telecommunications carriers being found grossly negligent as a matter of law are so rare as to be essentially non-existent.

Limits on Limited Liability

Even before Congress passed the Communications Act of 1934, the U.S. Supreme Court had held that a common carrier might not act as a common carrier in all of its commercial functions.²⁹ The limited liability that telecommunications carriers enjoy is not blanket immunity; rather, it is limited protection when they are acting as common-carriers.

Telecommunications carriers have been successfully sued for damages for their conduct when it does not entail the provision of telecommunications services. For example, disputes over telecommunications billing practices have resulted in claims against telecom carriers

²² 15 U.S. 1 (1894).

²³ *Id.* at 14.

²⁴ *Id.* at 14-15.

²⁵ See, e.g., *Pilot Indus. v. S. Bell. Tel. & Tel. Co.*, 495 F. Supp. 356, 361-62 (D.S.C. 1979); *Robert Gibb & Sons, Inc. v. Western Union Tel. Co.*, 428 F. Supp. 140 (D.N.D. 1977) (tariff provisions limiting liability are binding on all parties and have the force of law irrespective of their knowledge or notice thereof); *In re Bell Switching Station Litig.*, No. 72999, 1993 Ill. LEXIS 65 (Ill. Aug. 26, 1993).

²⁶ *Coachlight Las Cruces, Ltd. v. Mtn. Bell Tel. Co.*, 664 P.2d 994 (N.M. Ct. App. 1983).

²⁷ Gross negligence has been defined as conduct “show[ing] an entire, utter, complete, or extreme lack of care.” *Mullins v. State Farm Fire and Cas. Co.*, 697 So. 2d 750 (La. Ct. App. 1997).

²⁸ See, e.g., *Burdick v. Southwestern Bell Telephone Co.*, 675 P.2d 922 (Kan. Ct. App. 1984) (no liability where a telephone company failed to forward important business calls to a customer’s new number, even though it previously agreed to forward all calls).

²⁹ See, e.g., *R.R. Co. v. Lockwood*, 17 Wall. 3857, 3877 (1873) (a common carrier may become a private carrier when it undertakes to carry something not its business to carry); *Express Cases*, 117 U.S. 601 (1886) (railroad companies are common carriers with respect to the general public but may determine for themselves, under contract, the terms on which they will deal with express companies that use railroads to deliver packages).

for damages related to deceptive and fraudulent billing.³⁰

With respect to mobile banking transactions, it remains to be seen whether there is something unique or novel about these transactions that warrants that they be treated other than under the traditional “limited liability” model that has been the hallmark of telecommunications services for over a hundred years. For instance, some wireless telecommunications carriers offer banking customers more than just “transmission services;” they provide those customers with downloadable mobile applications that are used to engage in mobile banking transactions. The provision of this type of “information service” or software application is not in any traditional sense the provision of “common carrier” services.

Still, the real risk to the mobile banking consumer is unlikely to be that a particular mobile banking software application does not work (if it did not, then presumably the entire banking transaction could not be initiated); rather, it is that something goes decidedly wrong in the act of transmitting financial information. From that perspective, the core telecommunications transaction, from the telecommunications carrier’s perspective at least, appears to be no different than any other data coursing over that carrier’s network.

BRIDGING THE LIABILITY GAP

Mindful that there is something inherently and quantifiably different about a mobile banking transaction than, say, a misplaced e-mail or a call to a spouse that ends up being a “dropped call,” the wireless industry has taken steps to address these issues. Under the aegis of its leading trade association, the industry has adopted “Best Practices and Guidelines for Mobile Financial Services.”³¹ For example, under its “Guidelines Specific to Mobile Banking and Mobile Payments,” the Cellular Telephone & Internet Association (“CTIA”) recommends that service providers “use methods

consistent with industry best practices to authenticate user identity” (Which industry is referenced is left deliberately unspecified.)

The CTIA guidelines also recommend that 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 fund transfers).”³² Whether relevant regulators view these self-regulatory measures as sufficient, or whether compliance with such industry guidelines even matters given the pervasive legal concept of limited liability, it is too early to say.

From a financial institution’s perspective, however, it ought to be clear from even a brief comparative analysis that there is a significant gap between financial institutions and telecommunication carriers when it comes to their respective liability for the success or failure of mobile banking transactions. That is not to pass judgment on how these respective businesses are regulated today; rather, it is merely to shed some light on the situation.

As mobile banking continues to grow in popularity, it is fair to ask whether the average customer is fully informed about who will be liable to ensure that these transactions are completed, and, who will be liable to the customer when they are not. It is also fair for those who initiate and complete these transactions (financial institutions and wireless carriers) to consider whether the legal and regulatory frameworks that have been bent to fit this nascent service are appropriate to the task. Absent any foreseeable changes in this legal structure (which the interested parties may not wish to see in any event), it may be that mutual collaboration between telecommunications carriers and financial institutions would be the best approach to avoid, minimize, or at least fairly allocate liability risks attendant to mobile banking services. ■

³⁰ See, *e.g.*, *In re Universal Service Fund Telephone Billing Practices Litigation*, No. 02-MD-1468-JWL, 2009 WL 435111 (D. Kan. Feb. 20, 2009).

³¹ Cellular Telephone & Internet Association, “Best Practices and Guidelines for Mobile Financial Services,” January 28, 2009.

³² *Id.* at 2-3.