

# Mobile Payments: What Happens When the Card Disappears?



By Mark Moore, Esq., Principal,  
Aldrich and Bonnefin

The prepaid card industry always has been at the forefront of developments in payment systems architecture and technology. So, it's no surprise that many in the industry are turning their attention to mobile form factors as a possible new channel for delivering payment services. As with any evolving system, various solutions are in play as the marketplace differentiates between the products that will succeed and those that only will be

remembered. Several legal themes are common to these efforts under federal and state laws: compliance, information security and liability for unauthorized transactions.

Before looking at these legal issues, however, it is useful to more carefully define what "mobile payments" are. Proximity-based (or "contactless") product evolution continues, with each major card brand offering variations on the idea that contactless check-out offers merchants faster processing at the point of sale by eliminating the need to "swipe" a card.<sup>1</sup> Visa offers payWave, MasterCard offers PayPass, Discover offers NetworkZip and American Express offers ExpressPay. Each employs radio-frequency identification (RFID) technology, essentially a silicon chip and antenna embedded in the traditional plastic payment card or in a mini-card or fob. The transaction is initiated by a cardholder holding the card (or other form factor) in close proximity to the merchant's point-of-sale terminal (normally, within 1 or 2 inches).

Magnetic inductive coupling provides a power source to the passive transmitter (the RFID chip). This is sometimes referred to as passive RFID, since the card, mini-card or fob does not contain an independent power supply.

Near field communication (NFC) is a form of active RFID technology—active in the sense that the RFID transmitter has its own power source, enabling it to both receive and send data. Cell phones, PDAs and other hand-held devices may be equipped with passive RFID and used to conduct contactless card transactions in the same way an RFID-equipped plastic payment card, mini-card or fob might. In addition, mobile phones, PDAs and other hand-held devices may be equipped with active NFC technology, allowing a more dynamic passing of information back and forth between the purchaser and the merchant.<sup>2</sup>

A third option—often referred to as "over the air" (or OTA)—offers a branded user interface on a mobile

*Cont'd*

#### FOOTNOTES:

1 Contactless technology offers advantages in addition to faster check-out. For example, merchants incur lower cleaning, servicing and repair costs with contactless readers, since no physical contact is made or needed between reader and the card's magnetic stripe.

2 There is, for example, a lot of interest in using NFC to push targeted discount coupons, advertising or other promotional materials to consumer phones. In theory, real-time information about a consumer's shopping experiences would allow more efficient and effective promotional efforts by merchants and/or suppliers.

## Mobile Payments: What Happens When the Card Disappears?

January 2009, By Mark Moore, Esq., Principal, Aldrich and Bonnefin

Page 2

phone or other device. OTA payment-related software can be loaded before or after a phone is sold. With OTA, payment information may be processed through a card brand (under payWave or PayPass, for example) or may be routed through another payment system such as a money transmitter. For example, Obopay offers mobile phone software coupled with its money transmitter function to accomplish P2P (here, “phone to phone” as much as “person to person”) and supplements that with a MasterCard function to allow transfers to and from cards (as a payment destination or as a funding source).

In some cases, mobile payments involve the use of a mobile network telecommunications carrier or operator. Whether NFC or OTA, with a mobile phone also comes added functionality. Web-application protocol (WAP) may be used with a properly equipped mobile phone to supplement its use as an access device for payment services, allowing fuller integration with, for example, financial tracking and recordkeeping software. Some posit that a “killer application” might consist of a mobile phone that initiates payments at the point of sale, tracks balances and updates personal or business financial software—all in real time.

So what are the compliance, information security and liability issues in this brave new world?

### Compliance

Closed- and open-loop prepaid “card” programs can be moved to mobile delivery systems. As a general matter, the compliance impact on issuers (that is, the banks holding customer accounts or operating subaccount programs for an ISO/TPS program manager) remains much the same even with the transition from a more traditional plastic card to a contactless or other mobile channel. This generally also would be true as to the compliance issues faced by the processors, program managers and merchants that might be involved in a mobile channel.

Looking at network branded prepaid cards as the underlying product, compliance begins with federal and state laws, and includes card brand rules.

### Federal Rules

Regulation E applies to payroll cards but does not apply to other prepaid accounts.<sup>3</sup> Where Regulation E applies, initial and periodic disclosures are mandated. In addition, billing rights notices must be refreshed annually or included with periodic statements in an abbreviated form. Use of a mobile channel would not alter these rules, although the content of one or more of the disclosures might change. For example, initial disclosures of types of transfers and limitations under Regulation E Section 205.7(b)(4) would need to include some description of

the mobile application and its limits (if any), particularly where these might differ from more traditional card programs. General contract law principals lead to the same concern. It would, for example, be advisable to disclose to the customer that the fob or mobile phone would not be usable at traditional ATMs or other terminals where insertion is required.

Most practitioners accept that initial disclosures can be provided by a third party such as an employer. It is less clear how a periodic statement can be delivered as part of a telephone bill, assuming this were a goal and an integrated offering and a servicing agreement could be reached between the bank and the mobile carrier. As an operating principal, disclosures must be “in a clear and readily understandable written form.” Segregating the Regulation E disclosure from other parts of the phone bill should be Regulation E compliant.

Mobile payments via a mobile carrier channel are likely to include fees and charges that are paid to the carrier. Particular attention needs to be paid to these fees and charges, since the bank is required to disclose “any fees imposed by the financial institution for electronic fund transfers or for the right to make transfers.”<sup>4</sup> Periodic statement presentation of bank fees can present operational problems,

*Cont'd*

#### FOOTNOTES:

<sup>3</sup> This is a simplification, of course. See 71 Fed. Reg. 1474 (Jan. 10, 2006). As another example, some bank issuers of open-loop cards open a deposit account for the cardholder. In that case, Regulation E applies to the deposit account associated with the card, as it would to any other consumer demand deposit (checking), savings or other asset account.

<sup>4</sup> Parties also need to remember that contract law requires the customer's agreement to all customer fees and charges, whether or not Regulation E applies.

## Mobile Payments: What Happens When the Card Disappears?

January 2009, By Mark Moore, Esq., Principal, Aldrich and Bonnefin

Page 3

requiring data interfaces between a carrier and the bank or its servicers.

Recently, more and more issuers are seeking to move disclosure fulfillment away from paper and into electronic systems. An Internet-capable phone or other mobile device is an obvious attraction, and—in theory—no legal impediment prevents compliance with E-Sign and use of electronic records in lieu of written disclosures.<sup>5</sup> One untested issue that should be examined, however, is the clarity of disclosures that are delivered over a portable device. Tests should be conducted to ensure that the type size is readable and, if used for periodic statement purposes, the electronic presentation remains clear and intelligible.

### State Law

While mobile payments would generally present the same money transmitter licensing issues as would arise in a comparable card-based prepaid program, parties should never assume that the laws in 50 states are either uniform or consistent. Thus, one compliance responsibility is always to determine if the introduction of a new player (for example, a telecommunications carrier) might alter an otherwise available exemption or introduce a party in need of a license

*While mobile payments would generally present the same money transmitter licensing issues as would arise in a comparable card-based prepaid program, parties should never assume that the laws in 50 states are either uniform or consistent.*

—Mark Moore, Aldrich and Bonnefin

into a program that had previously been free of licensing requirements.<sup>6</sup>

Substantive laws in particular states also may require examination (or reexamination). Sometimes, the results do not change even though a mobile payment channel is used in place of a traditional plastic card. California, for example, limits consumer liability for unauthorized use of an accepted debit card to \$50, with an exception if unauthorized use is not reported within

60 days of transmittal of a periodic statement.<sup>7</sup> PIN-based transactions are not subject to this California rule. Surprisingly, however, mobile phones used in a “signature-based” transaction to access a consumer account would appear to be covered, since a “debit card” is defined to include “other means of access” to a debit card holder’s account. The California limitation, when applicable, affects the Regulation E disclosure of liability for unauthorized use, making any violation a matter for trouble under both state and federal law.

### Card Brands

While the card brands have specific rules to accommodate contactless payments that involve a card, mini-card or fob, there is less clarity on dealing with other form factors. Accordingly, depending on the program contemplated, the parties may need to coordinate with Visa, MasterCard or other card brand.<sup>8</sup> One significant issue would be branding, since historically the card brands have been reluctant to allow transaction data to be processed via their systems if the transaction was not initiated with a branded access device.

From the standpoint of a merchant participant, chargeback rights are likely to be an area of concern.

Cont'd

### FOOTNOTES:

5 See 12 C.F.R. 205.4(a)(1).

6 The caution to review licensing requirements is given in general terms, but one example might be in the money transmitter laws of New York. Generally, parties in stored value (including prepaid) are not required to obtain a money transmitter license in New York if they are not present in the state, either directly or through agents. If a mobile carrier is used, and depending on the specifics of the program, this may introduce a New York physical presence where none had previously existed. In this case, clarifying that the carrier is not an agent of another party may be sufficient to maintain the exemption.

7 See California Civil Code 1748.31(a).

8 For example, see reports regarding Bank of America’s recent initiative with iPhone and AT&T. While at the forefront in many ways, the program (insofar as is publicly reported) offers mobile banking services (balance inquiry, bill pay, transfers) but not mobile payments. See [www.apple.com/webapps/productivity/bankofamericamobilebanking.html](http://www.apple.com/webapps/productivity/bankofamericamobilebanking.html).

## Mobile Payments: What Happens When the Card Disappears?

January 2009, By Mark Moore, Esq., Principal, Aldrich and Bonnefin

Page 4

Contactless transactions are generally handled much like other transactions including expanded rights to charge back when a signature is not obtained (whether due to card-not-present or low-dollar exceptions to the signature requirements). One anticipates that similar rules would apply to transactions initiated via mobile phones.

### Information Security

Given events in 2008, information security is on everyone's mind. Mobile payments offer advantages, but there is a need for safety and data integrity. Each step of the flow of transaction data should be analyzed including the passage of data from the mobile device to the merchant reader. Acquiring banks may, for example, seek to include mobile channels within a merchant's PCI DSS certification.<sup>9</sup> For issuing banks, similar concerns and solutions apply to third-party service providers that handle cardholder data.

One minor, but easily overlooked compliance matter, is to update incident response plans to account for any changes in risk parameters that are presented by the newer devices. Federal law<sup>10</sup> would require this for issuing banks, and some states<sup>11</sup> likewise impose a need for an incident response plan. In that regard, a mobile phone channel would provide an easy

avenue for electronic notification of a security incident in appropriate circumstances. Parties may want to include this as one of the "categories of records" for which an electronic notice may be used in lieu of a paper one.<sup>12</sup>

### Liability for Unauthorized Use


Claims of unauthorized use can create difficult issues in a prepaid environment. Regulation E and state consumer protection laws may or may not apply, depending on the specific type of product involved. Some issuers provide Regulation E-like consumer protections against unauthorized use, even when this would not be mandatory under relevant law.

A fundamental goal is to build strong authentication systems to protect against fraud. Two-factor programs can be built that meet federal guidelines for Internet banking.<sup>13</sup> In some phone-based systems programs, PIN-based access restrictions are supplemented by SMS text confirmation programs that help to confirm authenticity. One concern in this regard is the validity of the mobile phone number itself, since there is a theoretical danger of spoofing.

More traditional risk-mitigation systems also are used. These include transaction amount limits (per transaction and over time periods), velocity limitations, fraud checks and

"know-your-customer" due diligence. Insurance coverage also should be reviewed, especially if a program constitutes a material business segment, since losses may arise due to employee defalcation (or other insider malfeasance), data breach or fraudulent transactions, among other things. A traditional policy designed with a traditional credit or debit card program in mind may have gaps that leave a party unexpectedly uninsured.

### Conclusion

Mobile payments are an exciting and potentially lucrative service for those who understand the prepaid sector. Experience in overseas markets suggests that U.S. consumers will find advantages to having a mobile wallet in their mobile phones. Prepaid programs offer an opportunity to address these needs, as they develop, using tried-and-true compliance, information security and risk-mitigation systems. 

*Mark Moore is a lawyer who practices at the Irvine, Calif., offices of Aldrich & Bonnefin, PLC (mmoore@aldrichandbonnefin.com, +1 949.474.1944). He has focused on banking and payments issues for more than 20 years. More recently his practice includes prepaid cards, mobile payment services and money transmitter licensing and compliance. He advises bank and non-bank issuers, sellers and redeemers of stored value. Moore is a past chair of the Business Law Section of the California State Bar and of its Financial Institutions and Consumer Financial Services Committees. He is a member of the California Bankers Association Legal Affairs Committee and chaired CBA's Bank Counsel Seminars in 2007 and 2008.*

#### FOOTNOTES:

<sup>9</sup> Requirement 4.1 is to encrypt transmission of cardholder data across open public networks and would allow testing of both transmission and storage systems for contactless cards and for mobile phones. See PCI DSS v 1.2 (Oct. 2008) available at [www.pcisecuritystandards.org/security\\_standards/pci\\_dss\\_download.html](http://www.pcisecuritystandards.org/security_standards/pci_dss_download.html).

<sup>10</sup> 70 Fed. Reg. 15736 (March 29, 2005).

<sup>11</sup> For example, see the new Massachusetts requirements for a "comprehensive, written information security program applicable to" personal information about residents of that state. 201 C.M.R. 17.03 (generally effective May 1, 2009).

<sup>12</sup> The E-Sign Act provides a general safe harbor to protect against claims that a record is defective due to its electronic form. 15 U.S.C. 7001(a)(1). Agreement to use electronic records is a prerequisite, and specific information (including the "categories of records" that may be provided in electronic form) must be given to consumers prior to their acceptance of e-disclosures. 15 U.S.C. 7001(c)(1)(B)(ii)(III).

<sup>13</sup> As the FFIEC's Aug. 15, 2006 FAQs on "Authentication in an Internet Banking Environment" make clear, "While the guidance focuses on Internet banking systems, its principles apply to all forms of electronic banking, including telephone banking systems."