



# PRIVACY & SECURITY LAW



## REPORT

Reproduced with permission from Privacy & Security Law Report, 10 PVLR 212, 02/07/2011. Copyright © 2011 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

### Mobile Payments: The Challenge of Protecting Consumers and Innovation



BY ELIZABETH ERAKER, COLIN HECTOR AND CHRIS  
HOOFNAGLE

**T**he ubiquity of mobile phones has long promised to spell the success of mobile payment platforms—a world in which the phone is a universal currency and no one needs plastic. While such predictions have proven mostly fruitless in the past, there is increasing evidence that the next few years may bring a fundamental shift towards mobile payment systems. A recent market study predicts that the worldwide mobile payments market will grow to \$633.4 billion and 490 mil-

*Elizabeth Eraker and Colin Hector are graduating students at Berkeley Law, University of California. Chris Hoofnagle is an attorney with the Samuelson Law, Technology & Public Policy Clinic and the Berkeley Center for Law & Technology at Berkeley Law.*

lion users by 2014, up from \$68.7 billion and 81.3 million users in 2009.<sup>1</sup> Over the last several months, a diverse group of companies have generated news about their plans in the mobile payments market: Verizon, AT&T and T-Mobile announced their coordination on a new mobile payments network, Google is reportedly working on a mobile payment service, and PayPal is increasing its focus on the mobile platform, among other developments.<sup>2</sup>

Along with the hype accompanying this trend, some caution may be warranted. The shift to mobile payments has enormous implications for privacy, as unregulated entities, or businesses traditionally regulated under some other sectoral scheme, such as telecommu-

<sup>1</sup> Liz Gannes, *Mobile Payments to Reach \$633B by 2014*, GIGAOM, May 13, 2010.

<sup>2</sup> See, e.g. Peter Pachal, *Google to Launch Mobile Payment Service*, PC MAGAZINE, Jan. 4, 2011; *PayPal Dives into Mobile Payments*, CNNMONEY.COM, Oct. 26, 2010.

nications, will have access to increasing amounts of financial and transactional data once only held by banks and transaction processors. Just a few years ago, mobile carriers were using telephone numbers as both identifier and authenticator for access to voicemail. Obviously, a different level of care will have to be applied to reduce opportunities for fraud that can endanger the solvency and trust in a payment system. Recent concerns that iPhone and iPad applications are leaking users' personal information to advertisers without consumer consent<sup>3</sup> suggests that mobile payment systems transferring sensitive payment data might be similarly susceptible to privacy breaches. The lack of industry standards and the rapid pace of technological change in mobile payment services also present consumer protection issues.<sup>4</sup> In addition, regulators charged with overseeing mobile payment platforms face the challenge of identifying a framework that effectively regulates non-bank entities—ones without the culture or deep experience with security found in other sectors—that are nevertheless offering financial services bordering on those provided by traditional banking institutions.

Despite these issues, the emergence of mobile payments promises substantial benefits for consumers. In the developed world, where the market for mobile telephony is mature, mobile payment systems have the potential to upset the existing balance between merchants and payment companies and provide new conveniences to consumers. For instance, m-payments may give merchants more ability to interact directly with the consumer, through in-store promotions and rewards that are delivered directly to the mobile device. Existing credit card rules disintermediate the consumer and merchant, causing merchants to have to engage in awkward contrivances in order to identify their own consumers.<sup>5</sup> In developing countries, the explosive growth of mobile payment systems demonstrates the potential for such systems to transition unbanked and poor communities into mainstream financial services. M-PESA, the mobile payments platform operated by Kenya's largest mobile network operator, has attracted over 13 million customers since its launch in 2007, almost fifty percent of the country's adult population.<sup>6</sup>

The central policy challenge: ensuring an adequate level of consumer safeguards while allowing for experimentation and innovation in a burgeoning industry. This was the topic of a recent conference that we helped organized with colleagues from the University of Washington School of Law entitled, "Mobile Payments: Global Markets, Empowered Consumers and New Rules?"<sup>7</sup>

<sup>3</sup> See Joel Rosenblatt, *Apple Sued Over Applications Giving Information to Advertisers*, BUSINESS WEEK, Dec. 28, 2010, <http://www.businessweek.com/news/2011-01-05/apple-sued-over-applications-giving-information-to-advertisers.html>.

<sup>4</sup> Kate Fitzgerald, *Data Breach Risks Rise with Social Networking, Mobile-Payment App Use*, AMERICAN BANKER, May 12, 2010, <http://www.americanbanker.com/news/data-breach-risks-1019079-1.html>.

<sup>5</sup> See, e.g., *Pineda v. Williams-Sonoma Stores, Inc.*, 100 Cal.Rptr.3d 458, 460 (Cal. App. 2009) (describing the store's effort to match a customer's name and zip code to her home address through a reverse-lookup in a third-party database).

<sup>6</sup> NPR, *Mobile Money Revolution Aids Kenya's Poor*, IDEASTREAM, Jan. 5, 2011, <http://www.ideastream.org/news/npr/132679772>.

<sup>7</sup> <https://www.law.washington.edu/cle/seminars/mobilepay/>

## M-payment Platforms

The term "mobile payments" is used to describe a range of different platforms that enable consumers to use their mobile phones to conduct transactions. One means of using the phone for payments relies on a phone's SMS or mobile broadband capability to make payments for goods or services, which are then charged to the customer's phone bill or deducted from prepaid airtime for prepaid subscribers. The next generation of mobile payments relies on an entirely different set of "contactless" technologies that enable proximity payments without contact between a payment device and an interfacing reader—allowing consumers to "swipe and pay." Near Field Communications (NFC), an extension of radio-frequency identification (RFID) that uses short-range, high frequency communication between a chip embedded in a mobile phone and terminals at the point of sale, is the leading technology in this area.

At our conference, Georgetown Law Professor Adam Levitin suggested that there are three primary business models for m-payment systems that vary in their independence from traditional payment networks, which are helpful in understanding the market. In the most orthodox model, m-payments operate as an extension of existing payment networks. Here, a m-payments solution is built on top of an existing payment structure, providing another means for transmitting payment authorization information between merchants and consumers.<sup>8</sup> For example, Square, an m-payment system recently recognized by *Time* magazine as one of the 50 Best Inventions of 2010,<sup>9</sup> allows merchants to directly accept credit card payments through a small device attached to a cell phone, essentially transforming a smart phone into a credit card machine.<sup>10</sup>

Second, mobile payment systems could integrate existing payment models with other incentive systems such as merchant advertising or rewards programs. For example, Shopkick is a location-based mobile application designed to enhance the offline shopping experience by providing consumers with loyalty rewards from merchants when they visit physical stores.<sup>11</sup>

Finally, mobile payment systems could function as completely independent payment platforms. This third possibility is the "game-changer," in which transactions are processed through a channel separate from existing payment systems. Carol Coye Benson, founder of the payments consulting firm Glenbrook Partners, has noted that m-payment systems have the potential to streamline and "decouple" the existing payment model by more directly connecting merchants to consumers. This could create a fundamental shift in the existing power balance between merchants and credit card companies by giving merchants a larger "piece of the pie" in consumer transactions. The M-PESA model dis-

<sup>8</sup> See Amelia H. Boss, *Convergence in Electronic Banking: Technological Convergence, Systems Convergence, Legal Convergence*, 2 DREXEL L. REV. 63, 91.

<sup>9</sup> Dan Fletcher, *The 50 Best Inventions of 2010*, TIME, Nov. 11, 2010, [http://www.time.com/time/specials/packages/article/0,28804,2029497\\_2030652\\_2029712,00.html](http://www.time.com/time/specials/packages/article/0,28804,2029497_2030652_2029712,00.html).

<sup>10</sup> L.A. TIMES, *Square, Twitter Founder Jack Dorsey's Mobile Payments Start-up, May Be Worth \$200 Million in New Funding Round*, Jan. 3, 2011.

<sup>11</sup> See Courtney Bank, *Top 10 Apps of '10*, WSJ Blog Digits, Dec. 31, 2010, <http://blogs.wsj.com/digits/2010/12/31/the-top-ten-iphone-and-android-apps-of-2010/>.

cussed above is an example of such a decoupled platform. Safaricom, the mobile carrier operating the wildly successful service, issues electronic value which customers can transfer to other customers, redeem for cash, or use to make payments to merchants, while it holds matching-value assets in a pooled account at a regulated bank.<sup>12</sup>

These different models have varying prospects for consumer adoption, which depend in part on the targeted user base. For example, in the United States, given the powerful position of financial institutions and the widespread use of credit cards, m-payment systems compete with traditional ways to process credit card payments. By contrast, in developing countries where many people lack access to traditional financial systems, m-payments have been introduced as a completely separate platform. Thus, in turning to the promises and challenges of m-payment systems, it is important to consider the interaction between the technology being introduced and the incumbent payment structure.

### **Promises and Challenges of M-payment Systems**

In developed countries, m-payment systems promise several advantages over the traditional credit card acceptance process. Primarily, m-payment systems offer convenience for both consumers and merchants. With m-payment devices such as Square, more merchants will allow consumers to pay with credit cards. Contactless payment systems promise to enable customers to use their phones to pay at the point of sale, which could be widespread if NFC technology is included in handsets and mobile operating systems, and rolled out in merchant terminals. Furthermore, the growth of mobile payment systems may signal a shift towards a more comprehensive “mobile wallet” that eliminates the need for customers to carry cash, credit and debit cards, rewards cards, and coupons. Instead, mobile phones may act as an all-in-one device that consumers can use to pay merchants, receive discounts, and track expenditures.

For merchants, m-payments promise a more affordable means of completing sales. M-payment systems may streamline the payment process, although the gains in efficiency depend largely on the form of m-payment system that is used. M-payment services that act as a way to accept credit cards—such as Square and Verifone’s competing PAYware system—offer a simpler and cheaper way to process payments by eliminating start-up costs and minimizing fees. This benefit is especially important for small businesses, which may have not acquired the traditional terminal required to process credit cards and don’t have the volume to endure monthly minimums for transactions.<sup>13</sup> For example, Square co-founder Jack Dorsey estimates that of the roughly 30 million U.S. merchants who have less than 100,000 in revenue, only six million are processing

<sup>12</sup> Michael Tarazi and Paul Breloff, *Nonbank E-Money Issues: Regulatory Approaches to Protecting Customer Funds*, CGAP Focus Note, July 2010, No., 63, at 2.

<sup>13</sup> Leena Rao, *Square Now Processing Millions of Dollars in Mobile Transactions Every Week*, TechCrunch, Nov. 9, 2010, <http://techcrunch.com/2010/11/09/square-now-processing-millions-of-dollars-in-mobile-transactions-every-week/> (last visited Jan. 7, 2010).

credit cards.<sup>14</sup> Thus, for the remaining twenty four million merchants, m-payment technologies may offer a low-cost solution to processing plastic.

If m-payment systems move away from credit cards and start to provide an entirely separate platform, the payment process will become even more efficient. By removing credit cards altogether, m-payment systems will allow consumers to make direct purchases from merchants, without the transaction costs involved in processing cards. Although such an independent m-payments system promises additional benefits, getting merchants and consumers to adopt such a model faces serious obstacles in the United States. Mobile carriers and financial services companies have historically taken significant steps to “lock-in” customers to their particular services. Given the powerful position of financial institutions, it will be especially difficult for m-payments to take hold as a separate payment system in the United States.<sup>15</sup>

Even for less ambitious systems, there are additional challenges to launching any m-payment system. For example, those systems that rely on contactless technology face the initial obstacle of achieving widespread adoption of the underlying technology. While NFC-enabled devices are common in Japan and Europe, the technology is largely theoretical among consumers, card issuers, and merchants in the United States. To date, only 150,000 to 200,000 U.S. merchants have installed NFC readers to accept contactless payments from consumers.<sup>16</sup>

More generally, successful introduction of any m-payments platform will require coordination between many different actors and a split of revenue from new fees that sufficiently incentivizes those actors. Needed cooperation and a “meeting of the minds” has been lacking to date. For example, carriers have historically charged exorbitant fees to process third party payments through consumers’ mobile phone bills. Analysts predict that the forty to fifty percent fees currently imposed for adding transactions to consumer bills would need to dramatically decrease if that particular mobile payment service is going to take off.<sup>17</sup>

There are equally challenging obstacles on the demand side of the equation. Generally speaking, U.S. consumers are satisfied with their current payment options and seem perfectly content reaching for plastic to make payments.<sup>18</sup> (A recent study shows that the younger “millennial generation” of 18-to-35 year olds are the age group most likely to drive mobile payment demand, which bodes well for the industry.<sup>19</sup>) Ameri-

<sup>14</sup> Leena Rao, *Square Now Processing Millions of Dollars in Mobile Transactions Every Week*, TechCrunch, Nov. 9, 2010, <http://techcrunch.com/2010/11/09/square-now-processing-millions-of-dollars-in-mobile-transactions-every-week/> (last visited Jan. 7, 2010).

<sup>15</sup> Mobile Service Innovation and Business Models 202-203 (Harry Bouwman, et. al., eds., 2008).

<sup>16</sup> James Temple, *3 Questions for Bill Gajda, Visa Innovator to Tap Mobile Payment Market*, San FRANCISCO CHRONICLE, Sept 19, 2010.

<sup>17</sup> See Liz Gannes, *Mobile Payments to Reach \$633B by 2014*, GIGAOM, May 13, 2010.

<sup>18</sup> Claire Cain Miller and Nick Bilton, *Now Accepting Cash, Checks or Cellphones*, N.Y. TIMES, Apr. 29, 2010, at B1.

<sup>19</sup> Kevin C. Tofel, *Who’s Driving Mobile Payments? (Hint: Some Are Barely Old Enough to Drive)*, GigaOM, Oct. 22, 2010.

can consumers, paradoxically, expect high levels of service and rewards from their banks, and at the same time, dislike their banks. M-payments would have to surmount this inertia, perhaps by leveraging consumer distrust of banks, by offering a much better value proposition, or by a leap in convenience.<sup>20</sup> Consumer adoption of contactless mobile payments will also require the roll-out of mobile devices equipped with NFC technology. That could happen relatively quickly given that the average consumer replaces his or her phone every eighteen months.<sup>21</sup>

The barriers to implementing m-payment systems in developing countries appear to be less daunting. In countries with a significant population of consumers with no access to financial institutions and widespread mobile phone penetration, m-payments can provide a critical financial tool for consumers. Safaricom, the mobile carrier operating M-PESA, estimates that at least 50% of current M-PESA users are unbanked. Moreover, by building an m-payment system on top of a ubiquitous and affordable technology—short message service (SMS) that allows texting—M-PESA has enjoyed meteoric success.

For users in developing countries, mobile payment systems offer several benefits over the alternative of hard currency. M-payment systems allow consumers to send small amounts of currency over long distances, without the risks of loss or theft that attend hard currency. Thomas Friedman has described how a payment system run by EKO India Financial Services is allowing low-wage Indian migrant workers living in rural areas with few bank branches to use their mobile phones and village kiosks to transfer funds between family members.<sup>22</sup> Moreover, in countries where widely-used denominations of currency have a very low value, physically storing currency may be impractical. M-payments offer consumers a means of saving small amounts of cash.

Thus, while we may see some growth of the m-payment market in developed nations, its incubation and adolescence may very well occur in developing nations, which are underserved, but also not burdened by the cultural and technological infrastructures laid by existing payment technology.

### **Consumer Protection Issues: Privacy and Security**

In addition to these obstacles to adoption, mobile payment systems raise privacy and security challenges that warrant serious consideration. As a rapidly growing technology, mobile payment services pose a particularly high risk of leaking users' personal information because the technology is evolving quickly and security risks are not fully understood. For example, the launch of Square was delayed in part because the underlying infrastructure needed to be strengthened in order to handle the risk of charge-backs and fraud.<sup>23</sup>

<sup>20</sup> UW Conference Transcript, Carol Coye Benson.

<sup>21</sup> See Matt Gunn, *The End of Plastic?*, 1/1/11 *BANK SYS. & TECH* 1.

<sup>22</sup> Thomas L. Friedman, *Do Believe the Hype*, *The New York Times*, Nov. 2, 2010.

<sup>23</sup> Ross Densley, *Payments Start-Up Square Delayed Over Security Concerns*, *Financial Services Technology*, June 6, 2010, <http://www.usfst.com/news/payments-startup-square-delayed-over-security-concerns/>

While there are widely-accepted security standards for processing credit cards and transferring funds electronically, there is no specific security standard that governs the specific issues raised by m-payments. When the Payment Card Industry (PCI) Security Standards Council, which issues widely-followed security standards in the payments industry, recently released the second version of its PCI Data Security Standard (DSS), it gave no specific guidance on mobile payments.<sup>24</sup> Shortly after the second PCI DSS was released, the Council released a statement noting that m-payment technology will be a “key focus” for 2011 and indicating that the Council will work towards a comprehensive examination of the mobile communication device and mobile payment application landscape in the near future.<sup>25</sup> The lack of industry standards and rules for mobile payments presents a particular risk for merchants operating on thin margins. Mobile payments running on the credit card network might be processed as “card not present” (CNP) transactions, which would shift the liability of loss in more situations to the merchant.

Arguably, the lack of a uniform security standard may benefit consumers in the long run. With several actors competing for market share, companies are pushing to be seen as the industry leader on security. For example, VeriFone has suggested that the end-to-end encryption employed in its PAYware mobile payment system is more secure than the common SSL encryption standard used by other mobile payment systems such as Square.<sup>26</sup> However, although competition on security may push larger players towards more stringent protections, without a uniform standard, some companies may rush products to the market with scant attention to security.<sup>27</sup>

In addition to the security of consumer information, these technologies also raise privacy concerns. Some new payment systems, such as PayPal and Google checkout, receive “Track 3” data (that is, an accounting of your actual purchase). In the mobile payments space, the issue of what data service providers should receive similarly merits attention in light of the lack of uniform standards governing the tracking of data beyond the purchase price and recipient of payment.

This concern is especially important given the evolving state of mobile disclosures and privacy policies. The small viewing screen of mobile devices poses a challenge in communicating a meaningful disclosure to consumers. For this reason, some commentators and industry groups have advocated shifting towards a model of “multilayered” disclosures on mobile phones that would provide a short initial notice that lays out the ba-

<sup>24</sup> Ellen Messmer, *Upgraded Retail Security Standard Ignores Mobile Payments*, *Network World*, Oct. 28, 2010, <http://www.networkworld.com/news/2010/102810-pci-data-security-standard.html>.

<sup>25</sup> PCI Security Standards Council statement on PA-DSS and mobile payment applications, Nov. 29, 2010, [https://www.pcisecuritystandards.org/documents/statement\\_101129\\_pcissc.pdf](https://www.pcisecuritystandards.org/documents/statement_101129_pcissc.pdf) (last visited Jan. 6, 2011).

<sup>26</sup> PayWare Mobile Q&A, <http://www.paywaremobile.com/q-and-a.aspx> (last visited Jan. 6, 2010).

<sup>27</sup> Kate Fitzgerald, *Data Breach Risks Rise with Social Networking, Mobile-Payment App Use*, *American Banker*, May 12, 2010, <http://www.americanbanker.com/news/data-breach-risks-1019079-1.html>.

sic privacy standard.<sup>28</sup> For example, TRUSTe, which operates the well-established online privacy seal program, has launched a mobile privacy certification program that utilizes a layered policy.<sup>29</sup>

### **Regulatory Frameworks: Striking the Right Balance**

Determining the appropriate response to the consumer protection issues raised by m-payments requires a consideration of the risks involved. In some cases, security and privacy issues may be adequately addressed by industry self-regulation and consumer education, while other concerns may warrant regulatory attention.

An initial challenge lies in determining how mobile platforms fit into the existing patchwork of U.S. laws and regulations governing the payments industry. Depending on the services offered by an m-payment provider, laws such as the Truth in Lending Act and the Electronic Fund Transfer Act (Regulation E) may apply. This question also raises the broader issue of what sort of regulatory framework properly addresses the financial risks to consumers posed by m-payments.

One possibility is to take a “hands-off” approach in order to allow the m-payments industry to blossom and experiment. Particularly in areas where adoption will be difficult, the threat of regulatory burdens may slow or even stop the launch of m-payment services. For example, Kenya has taken a light-touch regulatory framework, permitting nonbanks to operate m-payment platforms on an ad hoc basis through “no objection” letters and conditional approvals.<sup>30</sup> By contrast, Scott Morris, General Counsel and Senior Vice President of Trilogy International, has reported that the imposition of some regulations in Haiti, such as the requirement that m-payment providers maintain a 100 percent reserve to secure funds in their system, has posed a serious challenge to implementing an alternative payment system.<sup>31</sup>

However, putting responsibility for safeguards solely in the hands of industry self-regulation may mean that consumer risks go unaddressed. For example, basic is-

such as transaction disputes and under-secured credit may be best handled by regulations that have the force of law. In addition, there may be some issues that private companies lack expertise in, such as money laundering and terrorist funding.<sup>32</sup>

Implementing some consumer protection rules does not mean those regulations need to be inflexible. The European Union’s recent revision of the initial capital and ongoing funds required for m-payment companies highlight the need to closely monitor the m-payment landscape in order to ensure that regulations do not become an unacceptable barrier to entry for small companies.<sup>33</sup> Given the dynamic nature of the industry, it would be prudent to regulate in a manner that is flexible, and can change with the evolving state of the m-payments market. In any case, ensuring robust cooperation between the public and private sector will be essential to striking the right regulatory balance.

### **Concluding Thoughts**

In order to succeed, consumers will have to be convinced that m-payment systems are both sufficiently trustworthy and economically worthwhile.<sup>34</sup> In developing countries, where the benefits of m-payment systems are obvious and security concerns minimized by the small amounts that are sent across the technology, m-payments have experienced enormous growth. For many consumers in the United States, however, the benefits over traditional payment systems are less visible at this point and the security concerns are more daunting. In particular, the current lack of a uniform security standard and the low rate of integration of contactless technologies by merchants pose major obstacles for m-payment systems.

Despite these challenges, the potential impact of m-payment systems on the U.S. market is clear. The same characteristics that raise concerns over m-payments also make the technology an exciting, promising venture, with the potential to change the landscape of consumer spending habits. Whether m-payments fulfill their considerable hype ultimately will depend in large part on the ability for government and industry participants to create a framework that appropriately aligns regulations with risk.

<sup>28</sup> See, e.g., Nancy J. King, *Direct Marketing, Mobile Phones, and Consumer Privacy: Ensuring Adequate Disclosure and Consent Mechanisms for Emerging Mobile Advertising Practices*, 60 Fed. Communications L.J. 239, 330-32 (2008).

<sup>29</sup> Mobile Certification by TRUSTe, [http://www.truste.com/privacy\\_seals\\_and\\_services/enterprise\\_privacy/mobile\\_certification.html](http://www.truste.com/privacy_seals_and_services/enterprise_privacy/mobile_certification.html) (last visited Jan. 7, 2010).

<sup>30</sup> Michael Tarazi and Paul Breloff, *Nonbank E-Money Issuers: Regulatory Approaches to Protecting Customer Funds*, CGAP Focus Note, July 2010, No., 63, at 1.

<sup>31</sup> UW Conference Transcript, Scott Morris

<sup>32</sup> See U.S. Dep’t of State, *Mobile Payments—A Growing Threat*, March 2008, <http://www.state.gov/p/inl/rls/nrcrpt/2008/vol2/html/101346.htm>.

<sup>33</sup> UW Conference Transcript, Thaer Sabri

<sup>34</sup> Niina Mallat, *Exploring Consumer Adoption of Mobile Payments – A Qualitative Study*, 16 J. OF STRATEGIC INFORMATION SYSTEMS 413, 417 (2007).