For release on delivery
10 a.m. EDT
July 10, 2012

Statement of

Thomas P. Brown

Adjunct Professor, Berkeley Law School, University of California

and

Partner, Paul Hastings LLP

before the

Committee on Banking, Housing, and Urban Affairs

U.S. Senate

Washington, D.C.

July 10, 2012

Chairman Johnson, Ranking Member Shelby, and members of the Committee, thank you for inviting me to appear before you today to discuss mobile payments.[1]

Historically, innovation in the payment industry has not been a subject of public interest. I attribute this relative disinterest to the fact that recent innovation in the payment industry has been invisible to consumers. For more than a quarter of a century, the basic mechanics of engaging in a payment transaction have not changed even for payment cards, the newest of our payment technologies: approach point of sale, select card from wallet or purse, hand card to cashier (or swipe the card yourself), and wait for a message that the transaction has been authorized (or declined). Although industry participants can rightly claim that they have radically transformed the process of authorizing the transaction in the past three decades, most consumers don't see it this way.[2]

The phrase "mobile payments" elicits a different reaction. People are genuinely excited about mobile payments. Some of this excitement stems from the eye-popping valuations that some providers of mobile payments have reported to the technology press. But much of it appears to flow from anticipation that the mash-up of mobile with payments will bring a bit of magic to the point of sale. Waving a phone just seems cooler than swiping a plastic card.

Although I look forward to the day when I no longer have to carry plastic or paper to buy things, we should not, in my view, measure the success of mobile payments by the speed with which waving replaces swiping. Existing payment technologies work very well in traditional

---

[1] I am appearing today in my capacity as an adjunct professor at Berkeley Law School. In my private practice, I have represented and currently represent a number of clients that participate in the mobile payments industry. The opinions expressed in today's testimony are my own and may not represent those of my firm or my clients.

[2] *See* Thomas P. Brown, *Keeping Electronic Money Valuable: The Future of Payments and the Role of Public Authorities, in* MOVING MONEY: THE FUTURE OF CONSUMER PAYMENTS 127, 132-33 (Robert E. Litan and Martin Neil Baily eds., 2009).

retail environments. In fact, one might say that they were made for each other. The retail environments that Americans experience most often—multi-lane retailers, gas stations, quick-service restaurants—were designed to take full advantage of the virtues of existing payment mechanisms (primarily speed at the point of sale). And mobile payment technologies will not soon displace the well entrenched incumbents.

With that said, the bundle of technologies that we generally label "mobile" is rapidly transforming the payment industry. Mobile devices are being turned into Point Of Sale ("POS") systems. This is enabling millions of new merchants to accept electronic payments. It is also rapidly changing how existing merchants engage their customers inside and outside of traditional retail environments. These changes hint at the potentially radical ways in which mobile payments will change how people shop, buy, sell and pay for goods and services. It is possible—though not certain—that mobile payments will further undermine the distinctions between financial services companies, retailers and communications providers. But these really are just hints. At this point, it is impossible to say with any real confidence how mobile payments will affect banks, payment companies, merchants and customers. It is also far too early to pick winners (or losers) among the many mobile payment technologies and companies now emerging.

In my view, lawmakers should be wary of claims that mobile payments need to be further regulated, particularly in the areas of information security and privacy. The payment industry, including the mobile payment piece, is already heavily regulated. New layers of regulation could easily stifle innovation and benefit some providers at the expense of others. And any new laws or regulations directed at the burgeoning mobile payment industry should be developed on the basis of a concrete understanding of the laws and regulations now in place.

With that preface, I will describe the existing regulatory framework for the payment industry, discuss what's truly new about mobile payments, and address potential issues related to consumer privacy and compatibility.

Existing Regulatory Framework

Participants in the mobile payments space already face substantial costs associated with complying with the existing regulatory regime. Firms that want to enter the business typically confront a choice between obtaining licenses on a state-by-state basis or working under the regulatory authority of a chartered financial institution. And once that threshold is crossed, firms in the payment industry shoulder a long list of compliance obligations.

Generally speaking, a firm that wants to enter the payment business faces a stark choice: find a suitable regulated chartered partner (*i.e.* a bank or other depository institution) or obtain licenses from all 50 states as a money services provider. The first option brings the mobile payments provider under the indirect supervision of the state and federal agencies responsible for regulating the chartered partner (*e.g.* FDIC or OCC). This option also carries costs associated with revenue-sharing and compliance, although some compliance costs and responsibilities may be shared with the chartered partner. The second option brings the mobile payments provider under the direct supervision of various state entities. It also brings with it the initial burden of acquiring state licenses—potentially a multi-year process with associated fees and costs that can easily exceed a million dollars. Annual maintenance costs for state licensing can also be significant.

Beyond this choice, firms in the payment industry must comply with a long list of laws and regulations. Regulation of consumer financial services is complicated. Payments companies—mobile payments included—are typically bound by federal law providing

consumers with recourse in the event of a disputed charge.[3] Firms that rely on a stored value purse to support their payment applications may be required to implement Customer Identification Programs and to report suspicious transactions to the federal Financial Crimes Enforcement Network (FinCEN).[4] Firms that support international payments must scrutinize their operations for compliance with the requirements laid down by the Office of Foreign Assets Control (OFAC). Firms that store customer bank account or other payment account data are also subject to state laws governing notification to customers and state entities when that personal information is compromised.[5] Finally, although the full scope is still being fleshed out, the Consumer Financial Protection Bureau has supervisory authority over certain "covered persons," including nonbanks.[6]

One potential way to reduce costs is to eliminate the requirement that an entity must be licensed by all 50 states to operate nationally. There is no apparent benefit, from a prudential standpoint, of such a fragmented regulatory regime. This is not to say that licensing itself has no value—as in the banking industry, some supervision likely helps ensure that mobile payment companies can meet their obligations to consumers. This value becomes diluted, however, when that mobile payments company must contend with the overlapping, but not identical, regulatory

---

[3] For example, for mobile payment transactions involving credit cards, Regulation Z, which implements the federal Truth in Lending Act, limits a cardholder's liability to $50 for unauthorized charges. 12 C.F.R. pt. 226.12(c). Likewise, the federal Electronic Fund Transfer Act provides similar limitations on liability for unauthorized debit card charges. 15 U.S.C. § 1693g(a).

[4] All federally regulated banks are required to have a written CIP pursuant to section 326 of the USA PATRIOT Act.

[5] At this time, forty-six states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted such statutes. The National Conference of State Legislatures publishes a comprehensive list, *available at* http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx.

[6] *See* 12 U.S.C. § 5514(a)(1)(C).

requirements across the 50 states. In other contexts, state-regulated entities are able to "passport" a single state license across all 50 states, so that compliance with that individual state's regulations suffices to allow those entities to do business nationwide.[7]

Potential Benefit: The Mobile Point Of Sale

Although most of the conversation surrounding mobile payments focuses on the possibility of using mobile phones instead of plastic cards to initiate transactions, mobile's initial impact on the payment industry has been felt on the receiving side of the transaction. Existing forms of payment are mobile at least from the perspective of the consumer (*i.e.*, with rare exceptions, our wallets and purses follow us wherever we go). Until recently, however, electronic payment systems were limited to environments that could be reached by fixed line communication systems. Advances on the mobile front are releasing this constraint.

The transformation of mobile devices into Point Of Sale ("POS") systems is taking place on a number of fronts:

- Mobile devices have enabled millions of informal merchants to accept electronic payments. With an app and a small (generally free) device that plugs into the mobile device (known as a "dongle"), artisans, contractors and farmers now accept payment cards from their customers instead of cash.

- Mobile devices are changing how people shop. By equipping sales associates with tablets and smart phones and sending those associates onto the store floor, traditional retailers are turning the entire retail environment into the point of sale. Customers can make purchases in the aisle, rather than waiting to pass through the check-out line.

- Some retailers are using their customers' mobile devices to extend the point of sale outside the store. They are allowing customers to use their mobile devices to make purchases on their mobile phones (and tablets), go to the store, take the item

[7] For example, under the federal Secure and Fair Enforcement for Mortgage Licensing Act ("SAFE Act"), 12 U.S.C. § 5100 *et seq.*, mortgage loan operators enjoy uniform licensing standards nationwide, either through their home states' participation in the Nationwide Mortgage Licensing System and Registry or by those states' establishing individual systems that comply with certain federal standards.

off the shelf, and walk out of the store without ever having to present a payment card to a sales associate.

- Mobile devices are rapidly changing how people purchase information goods like books, music, movies and software. Again, the mobile device is the point of sale. Consumers use their own tablets and smart phones to access digital marketplaces, purchase books, songs, apps, etc., and read, listen to and use those goods.

The transformation of the consumer's mobile device into a primary point of contact between the merchant and the consumer may have a dramatic effect on retail commerce. People tend not to share their mobile devices in the same way that they share laptops and personal computers. This creates the opportunity for merchants to create customized offers for consumers. Most offers currently take the form of discounts, location based offers and fairly basic extensions of traditional loyalty programs (*e.g.*, buy nine coffee drinks and get the tenth free).

This evolution in payment technology may make it possible for restaurants and other small retailers to employ some of the dynamic pricing techniques that have been reserved to large-scale travel businesses. Outside of the travel industry, customers in most retail environments confront a single set of prices. Although different customers may be willing to pay very different prices for essentially the same service, it is difficult for traditional retailers to distinguish one customer from another. As merchants use mobile payment technologies to engage more directly with their customers, they may begin to employ some of the same strategies used by airlines, hotels and car rental companies to maximize traffic in their stores and restaurants, setting lower prices for some customers and higher prices for others. The extension of dynamic pricing strategies from the nation's airlines to the corner store may not be universally hailed.

Mobile Payments And Privacy

In order to customize experiences for particular customers, the merchant (or payment provider) must have access to information about those customers. For example, imagine a restaurant owner trying to craft an offer to attract new customers to her restaurant. Our hypothetical restaurant owner would likely want to reach out to those customers whose spending habits indicate that they like to eat out but who have never eaten at her restaurant. But the restaurateur would likely want to limit the offer to customers who live in the local area, excluding from the scope of the offer tourists and people traveling though the area on businesses. Such distinctions immediately implicate concerns about consumer privacy.

The legal and regulatory framework that governs the collection and use of information regarding consumers is complex and fragmented. Regulatory requirements vary by industry. Financial institutions and affiliated third parties, for example, face one set of requirements under the Gramm-Leach-Bliley Act.[8] Credit reporting companies face another set of requirements under the Fair Credit Reporting Act.[9] Health care providers face another set of requirements under the Health Insurance Portability and Accountability Act's ("HIPAA") Privacy Rule.[10] Federal law also imposes specific restrictions on the sharing of information about certain kinds of purchases.[11] Special rules apply to certain kinds of information, and the rules can vary depending on the manner in which the information is held at the time of disclosure.

[8] 15 U.S.C. § 6801 *et seq.*

[9] 15 U.S.C. § 1681 *et seq.*

[10] *See* HIPAA Privacy Regulations, 45 C.F.R. pt.160.

[11] For example, information regarding video or video game rental or sale records is protected from disclosure pursuant to the Video Privacy Protection Act, 18 U.S.C. § 2710.

Communications in transit receive a different set of protections, for example, than information at rest.[12]

No single agency is responsible for administering federal privacy law. The FTC has shown the most consistent interest in the subject, though the Department of Justice gets involved, too, particularly when a third party obtains information by illegal means. The prudential agencies have historically been responsible for ensuring that the financial institutions that fall within their purview adhere to the requirements of Gramm-Leach-Bliley. Dodd-Frank has further complicated this picture by severing responsibility for supervising adherence with GLB's privacy requirements from responsibility for supervising adherence to its information security and disposal requirements.[13]

State laws add another level of complexity. A number of states purport to limit the information that can be collected from consumers in connection with certain types of transactions. California law, for example, forbids merchants from, as a condition of sale, requiring or requesting personal identification information from consumers who use a credit card at a point of sale,[14] and the California Supreme Court has defined a zip code to be personal identification information.[15] And, as noted above, forty-six states have enacted laws requiring that consumers receive notice if certain information is obtained by a third party.

---

[12] "Electronic communications," meaning any transfer of information through electronic means, are generally protected from disclosure under the federal Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2510 *et seq.* Title I of the ECPA, known as the Wiretap Act, protects electronic communications while in transit. Title II of the ECPA, known as the Stored Communications Act, protects communications held in electronic storage.

[13] The Dodd-Frank Act amended Title V of the Gramm-Leach-Bliley Act to grant rule-making authority under Sections 502-509 of that Act to the Consumer Financial Protection Bureau (CFPB).

[14] Cal. Civ. Code. § 1747.08(a)(1)-(2).

[15] *Pineda v. Williams-Sonoma Stores, Inc.*, 51 Cal. 4th 524 (2011).

Private law also plays an important role in this area. The major card networks restrict the uses to which transaction data can be put. Visa's Operating Regulations prohibit a merchant from disclosing a cardholder account number, personal information, or other Visa Transaction Information to any entity other than a registered third party agent, the acquirer, or the acquirer's agent, and that such disclosure must be made for the sole purpose of (i) assisting the merchant in completing the initial merchant transaction, or (ii) as specifically required by law. The payment card networks, through the PCI Council, also regulate how merchants and other participants in the payment card systems may store information related to payment card transactions.

This complex suite of laws does not advance a single policy objective. Much of federal privacy law is based on the principle that consumers should receive notice and choice with respect to the use of information about them when that information is being used for marketing purposes. As some commentators have observed, it is far from clear that consumers actually want to receive such notices.[16] Other aspects of federal privacy law are directed at protecting consumers against misuse of data that relates to them. The Do Not Call Registry and the liability caps for unauthorized transactions under Regulation Z and Regulation E fall into this category.[17] Moreover, to the extent that privacy laws attempt to enable consumers to shield their identities from mobile payment providers or other financial institutions, they work at cross purposes with federal banking law, which as noted above requires firms to collect enough information about their customers to report suspicious transactions.

---

[16] *See, e.g.*, J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109, 113 (2008) ("Few consumers actually take the time to read [GLB notices], understand them, and make a conscious choice about whether to opt out of information sharing that is not a matter of statutory right for the financial institution.").

[17] *See id.* at 118-20 (explaining that the Do Not Call list addressed the problem of unwanted calls at home by focusing on the consequence—the call—rather than access to the information necessary to produce the call—the consumer's phone number).

This complexity should lead lawmakers and regulators to take particular care before creating new laws under the privacy banner. Most efforts to protect consumer privacy interests simply make it more costly for firms to collect information from consumers and to share that information with other firms. But information sharing is not a concern *per se*, and the focus on sharing tends to distract attention from the problems that give rise to the concern about sharing in the first place—the misuse of sensitive information and the failure to take care against the exposure of sensitive information to malicious third-parties.

Compatibility

This leaves the question of compatibility. Of the issues on today's agenda, this is the most complex and nuanced.

Compatibility (or incompatibility) issues can arise at many different levels. My iPhone is not, for example, compatible with my aunt's Android device. My phone has a different operating system from hers, and it connects to one telecommunication network—Verizon—while hers connects with another—AT&T. My device supports some applications that hers does not. In this sense they are incompatible. But in another sense, they are deeply compatible. Even though the phones are different in many ways, I can use my phone to call or send emails and texts to hers. If we both have accounts with PayPal or Dwolla, I can use my phone to send her money.

As mobile technologies grow in importance as platforms for the exchange of value, compatibility issues are likely to arise. Every mobile payment application may not work in every environment. Starbucks, for example, may choose to keep its mobile payment application separate from that offered by Peet's. But incompatibility issues at that level should not be a

source of concern. Indeed, the decision to offer a closed loop payment product may reflect regulatory distinctions as much as anything.[18]

With that said, concerns about the interoperability of different mobile payment applications cannot be dismissed entirely. Both the telecommunications industry and the payment industry have borne witness to significant battles over network access and compatibility.[19] And those issues may surface again. Antitrust authorities in Europe are currently reviewing a proposed payment joint venture in the UK in part due to such concerns.

But—and this is a perspective informed as much by my background as an antitrust lawyer as a student of the payment industry—these issues are sufficiently nuanced that they are not susceptible to a one-size-fits-all solution. Issues of compatibility and interoperability need to be evaluated on a case-by-case basis. Firms may, as in the Starbucks example above, have good reason for rendering their payment applications incompatible with the applications offered by others. But they may not, and in some instances, incompatibility can be a cause for public concern. Fortunately, antitrust law provides a well-developed framework for analyzing these issues as they arise on a case-by-case basis.

Conclusion

This is an exciting time for the payment industry. Emerging technologies are creating opportunities for financial institutions, merchants and consumers to reinvent commerce. This innovation is taking place against the backdrop of a very complex regulatory regime, and although it is possible to imagine ways in which the regulatory burdens facing firms in the area

[18] *See, e.g.*, 31 C.F.R. pt. 1022 (FinCEN's final rule relating to prepaid access).

[19] *See, e.g.*, *MCI Commc'ns Corp. v. Am. Tel. & Tel.*, 708 F.2d 1081 (7th Cir. 1983); *United States v. Visa U.S.A., Inc.*, 344 F.3d 229 (2d Cir. 2003).

could be reduced (particularly in the area of state-by-state licensing requirements), this emerging industry does not appear to need any new regulation.

Thank you again for inviting me to appear today. I am happy to answer any of the committee's questions.