Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Insights From The FTC's Mobile Payments Workshop

Law360, New York (May 04, 2012, 3:03 PM ET) -- On April 26, 2012, the Federal Trade Commission held a public workshop titled "Paper, Plastic ... or Mobile?" to examine the use of mobile payments in the marketplace and the impact of emerging technologies on consumers. Three consumer issues surrounding mobile payments were highlighted: (1) the lack of clear consumer redress and dispute resolution processes, (2) data security and (3) consumer privacy.

This article summarizes the FTC's workshop and the discussion on these three issues. For industry participants that are involved in the mobile payments ecosystem — or wish to be — having a clear understanding of these components and emerging best practices makes good business sense, and can help keep a company from becoming an enforcement or litigation target.

Mobile Payments Defined

Carol Coye Benson, managing partner of Glenbrook Partners, keynoted the fundamental concepts behind mobile payments. Traditional financial payments such as credit and debit cards are easily understood, easy to use and highly regulated — with relatively little innovation. Now enter mobile payments. The official definition from the Federal Reserve is "purchases, bill payments, charitable donations, payments to another person, or any other payments made using a mobile phone."[1] Benson also provided the following background:

Where Is Payment Data Held

There are three models currently at play. One model puts the financial data on a chip contained in the smartphone, called "Secure Element." The second model essentially points the smartphone to the payment data saved on an external server. The third model has the financial data encrypted in a file contained in the phone's memory.

Near Field Communication ("NFC")

ComputerWeekly.com defines NFC as "allow[ing] data to be exchanged between devices via short-range, high-frequency wireless communication technology by combining the interface of a smartcard and reader into a single device."[2] Panelists colloquially referred to NFC as the enabling mechanism behind the "smart tap."

Other Mobile Payment Options Than NFC

- single merchant applications employed in retail locations;
- multiple merchant peer-to-peer bar code scans;
- mobile carrier channel prepaid accounts with multiple funding methods;
- multiple merchant "card of file"; and
- account to account transfers with PIN security.

Benefits of Mobile Payment

According to Benson, the consumer benefits of mobile payments include a cool user experience, integrated coupons and utility like a regular credit or debit card. In addition to the convenience and coolness factor, speakers cited benefits such as receiving instantaneous digitized receipts to confirm purchases, more comprehensive loyalty programs, and real-time communication of dynamic pricing.

This is particularly important, panelists noted, for small businesses. For example, mobile payment options can enable a family-run ice cream business to advertise in real time its fluctuating pricing scheme due to changes in temperature. Likewise, one panelist commented that mobile payments enable millions of small-business merchants to enter the financial services market when they otherwise would have been unable to get a merchant account.

Further, mobile payments also serve the underbanked and nonbank communities. A significant number of Americans do not have a bank account of any kind, and many make regular use of alternative financial services such as payday loans, check chasers, rent-to-own services, money orders or pawn shops.[3]

According to the Federal Reserve, the underbanked make comparatively heavy use of both mobile banking and mobile payments, with 29 percent having used mobile banking and 17 percent having used mobile payments in the past 12 months.[4] Sixty-two percent of the underbanked who use mobile payments have used it to pay bills.[5] Panelists noted other services potentially appealing to this community, including real-time information of financial information to monitor budgets and prevent overdraft.

Issue No. 1: Lack of Clear Redress/Dispute Resolution

Panelists frequently cited the adage that there will now be "more mouths at the trough." In addition to the financial institutions involved in the traditional credit card payment scheme, enter now an "ecosystem" of players: the original equipment manufacturer of the mobile device; operating systems; new hardware; applications/service providers; carriers; coupon/loyalty program distributors; and other companies yet to enter the market. Problematically, the current financial scheme does not adequately contemplate this new ecology.

What happens when mobile payment transactions go awry? For traditional credit card transactions, the avenues for consumer redress are well established. Consumers seeking to dispute a charge file a complaint with the card issuer and/or the financial institution. With mobile payments, the path is less certain given divergent money flows, conflicting and nonharmonized regulatory schemes, and the lack of consumer education.

Panelists described the money flow issue as essentially a problem of too many mouths to feed: Carriers want consumers to make payments directly through their phones; other mobile payment options either want that amount to be directly withdrawn from the consumers' bank account or charged to their credit cards. Panelists also commented that the divergent regulatory schemes associated with these types of payment can exacerbate the money flow issues.

Panelists conceded the confusion of potentially applicable laws, though they differed on whether and to what extent more regulation was needed. For example, one panelist suggested that consumers are already protected by laws to the extent that mobile payments are used as credit cards, and no evidence exists that consumers are particularly concerned by the lack of clear redress. In fact, he emphasized that given the pro-consumer nature of existing laws, merchants — not consumers — usually bear the consequences of fraud.

When asked to give recommendations to both consumers and industry, panelists suggested that consumers conduct due diligence prior to adopting new payment methods, educate themselves on the financial data flows and consider the downside risks of mobile payments. Regarding industry, panelists advised that companies seeking to enter this market be fully educated on the regulatory framework of the financial services industry. Companies need to offer uniform consumer redress processes, provide better disclosures and more transparency to consumers, and devise specific industry best practices.

Issue No. 2: Data Security

Data security issues were addressed throughout the workshop. The Federal Reserve found that, among survey respondents, concerns about the security of the technology were the primary reason for not using mobile payments (42 percent), and the second most common reason for not using mobile banking (48 percent).[6] Some speakers were more optimistic than others in the security of mobile payments. On one end of the spectrum, one panelist stated that mobile payment acceptance devices currently lack consistent standards in what he called "the wild wild west" of fraud and security, of which "bad actor" companies have taken advantage.

Other panelists countered this view by suggesting that mobile payments may in fact be more secure than traditional credit cards. In emphasizing this point, panelists addressed the inherent insecurity of conventional payment methods like credit and debit cards. The majority of credit card transactions pass through networks and systems in unencrypted format in some way. As a result, panelists noted the infeasibility in ensuring 100-percent integrity of the conventional payment system.

In contrast, mobile payments conduct real-time "fraud scoring analysis" and have at least three additional layers of security: required payment credentials, dynamic authorization and password protection on mobile devices. These security measures are particularly compelling in the event of loss or theft, where applications such as Google Wallet could instantaneously disable access to multiple payment options with one phone call.

Even in light of these heightened security measures, panelists emphasized that mobile payments will only be more secure when done correctly. New companies that trivialize data security and insufficiently protect themselves risk breach. In addition to password-protecting smartphones, panelists recommended that security-focused consumers conduct due diligence on the data being transmitted by mobile payments.

Issue No. 3: Privacy

Panelists provided a comprehensive laundry list of new privacy concerns. Because mobile payments can deliver more consumer information than can traditional credit cards, panelists emphasized the need for mobile payment service companies to build in strong consumer privacy controls. Sharing this information will likely increase online behavioral advertising and allow detailed profiling of consumers. To curb the need for more restrictive regulations, panelists encouraged players in the mobile payment ecosystem to work together to secure transactions and prohibit unnecessary data sharing.

When asked what information was "necessary" for a mobile payment transaction and what companies were doing with this data, one panelist suggested that this data was being used to understand consumer shopping preferences in a manner similar to the personalized "mom-and-pop" store experience. When asked what privacy by design in mobile payments would look like, panelists suggested the following:

- opt-in ability to loyalty programs, targeted advertising, and second/third party data sharing;
- transparency for consumers to make informed decisions;
- control of privacy settings to restrict disclosure;
- "do not track" as either a superseding application or by industry agreement;
- paradigm shift that begins with respect and consumer privacy as a fundamental right;
- consistency in industry value propositions;
- clear definition of "first party" data use, in which many parties could potentially be involved; and
- privacy as the differentiator in products.

Conclusion

In concluding the workshop, Jessica Rich, associate director of the FTC's Division of Financial Practices, reiterated the trinity of consumer issues surrounding mobile payments: the lack of clear consumer redress, data security and consumer privacy. Given the complex and uncertain legal landscape, education will be key to ensure that consumers understand their rights and the avenues for redress. In addition to providing unique benefits, such as real-time data analysis and dynamic pricing, mobile payments may in fact be more secure than their traditional payment counterparts.

However, with the harvesting of this highly sensitive financial data comes the attendant rise in privacy-related issues. To counter this risk, the FTC strongly encourages current and new companies to adopt the following privacy framework as set forth in the FTC's final privacy report released earlier this year: privacy by design, simplified choice for businesses and consumers, and greater transparency.

--By Dana B. Rosenfeld, Alysa Zeltzer Hutnik and Sharon Kim Schiavetti, Kelley Drye & Warren LLP

Dana Rosenfeld is a partner in Kelley Drye's Washington, D.C., office, where she chairs the firm's privacy and information security practice. Alysa Hutnik is a partner, and Sharon Schiavetti is an associate, in the firm's Washington office.

[1] See Consumers and Mobile Financial Services, Bd. of Governors of the Federal Reserve System, pp. 11 (March 2012), available at http://www.federalreserve.gov/econresdata/mobile-devices/files/mobile-device-report-201203.pdf (“Fed. Reserve Study”).

[2] ComputerWeekly.com, What is Near Field Communication (NFC)?, available at http://www.computerweekly.com/feature/What-is-Near-Field-Communication-NFC.

[3] Fed. Reserve Study, pp. 4.

[4] Id.

[5] Id.

[6] Fed. Reserve Study, pp. 1.