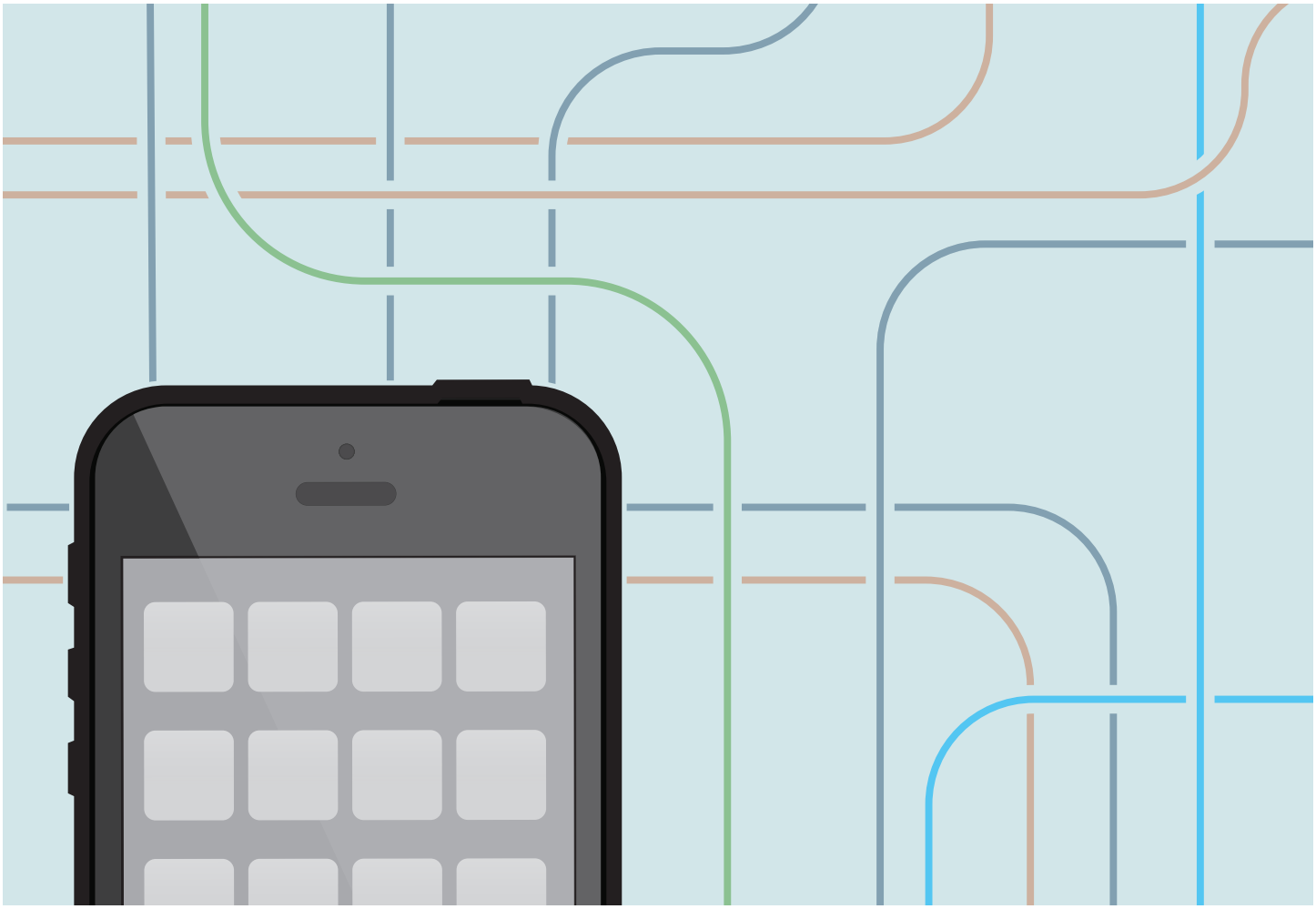
A brief from THE PEW CHARITABLE TRUSTS | Feb 2016



Mobile Payments

Regulatory gaps, ambiguities, and overlap

Overview

Mobile payments enable consumers to make financial transactions using their smartphones via a website, by sending a text message, or through an app. This technology, in turn, relies on many other consumer products and services, including credit, debit, and prepaid cards; wireless carriers; and nonbank providers such as Apple, Samsung, Google Wallet, and PayPal.

Research predicts that mobile payments in the U.S. will grow at an overall 22 percent compound annual rate through 2019.[1] These products and services have the potential to provide consumers with greater convenience and lower costs when managing their money. Mobile payments may be especially useful to those without a bank

account (the "unbanked"), one-third of whom have a smartphone, by offering these customers savings, money management, and transaction services that are not otherwise available to them.[2]

As mobile payments grow in popularity, policymakers need to understand the legal framework in which these transactions take place. A multitude of uncoordinated state and federal statutes, regulations, agency "guidance," and court decisions covers mobile payments providers and their products and services, which results in an incomplete and uncertain regulatory environment.

This analysis examines the legal framework as it applies to three stages of mobile payment transactions: when consumers use mobile devices to contract for payment services; when they use mobile devices to make payments; and after they make mobile payments. This study considers gaps where no law applies; ambiguities as to whether or how a law applies; and overlap in which two or more laws apply to the same situation, more than one agency has legal authority over the same type of conduct, or both.

Consumers face significant risks at each stage of the payment process. For example, service agreements on websites or apps are often unclear, leaving customers unsure about what they have agreed to and what terms they are bound by. When making payments, a lack of comprehensive consumer protections—especially for prepaid cards, nonbanks, and mobile transactions—leaves some customers vulnerable to problems such as financial liability or fraud. And after making mobile payments, consumers face inadequate federal protections, putting them at risk of security breaches and privacy invasions by providers or third parties.

This brief summarizes the findings of a white paper commissioned by The Pew Charitable Trusts and written by Mark E. Budnitz, professor of law emeritus at Georgia State University. The white paper is available at http://bit.ly/20ri6t0.

Laws Governing Mobile Payments

Myriad federal laws cover some part of the mobile payments marketplace. These include:

- Children's Online Privacy Protection Act—regulates collection of data from children younger than 13.
- Communications Act—restricts phone company use of customer proprietary network information, which is data that local, long-distance, and wireless telecommunications companies acquire about their subscribers, including services used and amount and type of usage.
- Credit Card Accountability Responsibility and Disclosure Act—provides consumer protections for credit cards.
- Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank)—Title X of the act established the Consumer Financial Protection Bureau (CFPB) and grants it authority over consumer financial protection laws.

Continued on the next page

- Electronic Fund Transfer Act (EFTA) —provides consumer protections for transactions conducted via ATMs, point-of-sale terminals, and the Automated Clearing House (ACH), which is a network through which electronic transactions are sent between accounts.
- Electronic Signature Act—regulates the timing and delivery of electronic disclosures.
- Expedited Funds Availability Act—requires banks to make funds from a deposited check available within specified time frames.
- Fair Credit Reporting Act (FCRA)—regulates the collection, dissemination, and use of consumer credit information.
- Fair and Accurate Credit Transaction Act—governs some consumer rights under the FCRA, including in cases of identity theft.
- Federal Trade Commission (FTC) Act—prohibits unfair and deceptive practices.
- Financial Services Modernization Act (also known as the Gramm-Leach-Bliley Act)—requires companies that offer consumer financial products or services such as loans, financial or investment advice, and insurance to explain their information-sharing practices to customers and to safeguard sensitive data.
- Truth in Lending Act (TILA)—provides rules institutions must follow, including disclosure of key loan terms and conditions, when offering credit.
- Truth in Savings Act—requires financial institutions to make disclosures, including of fees, interest rates, and minimum balance requirements.
- Uniform Commercial Code (UCC)—laws to govern business and commercial transactions that have been largely adopted by the states.
- Uniform Electronic Transactions Act—suggests uniform state rules to govern electronic transactions, including records and signatures, that have been adopted by most states.

Stage 1: Using mobile devices to contract for mobile payments services

When setting up a smartphone to make mobile payments, consumers can choose to load their credit, debit, or prepaid cards onto their mobile devices or to rely on a nonbank account such as PayPal or Google Wallet. And these choices have significant implications, particularly because the applicable consumer protections against fraud, loss of funds, and other risks vary based on the type of account used, differences that consumers may not fully understand.

In addition, before using a smartphone to make a payment, consumers may be required to agree to an app or site's terms and conditions. But a lack of transparency can cause consumers to unknowingly be bound to terms and conditions of a particular website. For example, the consumer might take on obligations and restrictions merely by clicking on various website buttons or boxes without ever seeing the terms—which are on a different part of the website—or having an opportunity to explicitly decline them. Likewise, if the website's owner updates the terms, customers could unknowingly be bound to additional requirements.

Problems with current laws include:

Gaps

- No law dictates whether a mobile device should be treated as legally equivalent to a credit card or, instead, as an "access device" (such as a debit card), which carry different consumer protections.
- Consumers have no guarantee that they will receive clear and noticeable disclosures for mobile payments terms and conditions. When they charge mobile payments to credit cards or other open-ended credit accounts, TILA Regulation Z requires "conspicuous" disclosure of rates, fees, and other cost information but does not define "conspicuous" or explain how to apply the standard to payments made using mobile phones.
- Consumers increasingly use general purpose reloadable prepaid cards, which can also be used when making mobile payments, but no law regulates these cards. The lack of regulations requiring card issuers to provide uniform, clear, and conspicuous disclosures means consumers may not be aware that they are not covered by the same protections that apply to credit and debit cards. The CFPB required new disclosures in its proposed rules, but these regulations are not expected to go into effect until at least 2016.
- Software licenses such as those used for mobile apps are not explicitly included under the UCC. Mobile payments users often implicitly agree to these agreements merely through use of the app, unaware that key consumer protection provisions of the UCC do not apply to these licenses.

Ambiguities

- Dodd–Frank does not clearly articulate which federal agencies have authority to enforce the FTC Act, which includes provisions regulating unfair and deceptive acts and practices and could apply to providers of mobile payments. The CFPB has no authority to enforce the act, but Dodd-Frank did grant the bureau explicit authority to issue rules and bring enforcement actions against businesses under its jurisdiction that engage in unfair, deceptive, or abusive acts or practices.[3] Nonbanks are subject to FTC enforcement actions, but debit cards and many credit cards are issued by banks regulated by federal agencies such as the Office of the Comptroller of the Currency, National Credit Union Administration, and Federal Deposit Insurance Corp. Dodd-Frank created ambiguity by throwing into doubt whether those agencies can enforce the FTC Act, although it appears that each agency retains the authority to bring actions against financial institutions under its jurisdiction.[4] The uncertainty around responsibility for enforcement could leave mobile payments customers largely unprotected.
- The courts have not developed clear rules or standards for determining when consumers are bound to contracts that purport to obtain the customer's consent by a mere click of a mouse or the opportunity to browse on a website and read the terms, including mobile websites and apps. This leaves consumers without a clear understanding of what terms and conditions they may have agreed to when they read through content on a website.
- The validity of "rolling contracts"—legal agreements in which some terms are disclosed initially and more terms are disclosed later—is not clear. Ongoing changes to the terms of a contract could create uncertainty for consumers about their obligations and rights and what they have agreed to.
- The law governing "browsewrap agreements"—in which companies contend that consumers consent to the provider's contract terms simply by purchasing goods or services from or continuing to use a website—is ambiguous and lacks transparency. For example, a consumer who browses on a seller's website and clicks on various boxes and buttons could unknowingly be entering into an agreement and be bound to terms that are on other pages of the website or that go into effect later.

Overlap

- The CFPB and FTC both have legal jurisdiction over unfair and deceptive acts and practices. Both have rule-making and enforcement authority in regard to some of the same companies when those companies engage in unfair or deceptive acts or practices. The two agencies have entered into a memorandum of understanding that establishes a procedure for coordinating their activities.[5] Dodd-Frank added "abusive" acts or practices to the CFPB's jurisdiction but not the FTC's.
- The CFPB has the authority to supervise some companies ("larger participants") within the mobile payments market but has not yet indicated whether it will do so. This jurisdiction may overlap with other federal regulators' authority, potentially creating inconsistency for consumers should these agencies differ in their supervision and enforcement of current laws and rules.

Stage 2: Using mobile devices to make payments

Once consumers enable their devices to make mobile payments, they face a new set of risks, including lack of error resolution or limitations on liability rights and appropriate fraud-detection services. Financial regulation has many gaps with respect to mobile payments transactions. Several reflect the failure of the law and other rules to keep pace with new technology and products, such as Google Wallet and Apple Pay, and virtual currencies such as bitcoin, leaving consumers unprotected. Additionally, inadequate regulation places customers at risk of harm associated with denial of service attacks, in which hackers block online access to a company and which may substantially impede the ability of users to make timely mobile payments.

Gaps

- The Electronic Fund Transfer Act requires financial institutions to provide disclosures regarding consumers' liability for unauthorized transfers, the types of transfers customers may make, and the amount of the fees. The institution must also include notices regarding the right to receipts, periodic statements, stop payment, preauthorized payments, and error resolution and permits them to be sent electronically.[6] But the statute does not offer any guidance on what courts should do when a financial institution says it sent an electronic disclosure but the consumer denies receiving it, leaving consumers unaware of their legal rights and protections, some of which are time-limited.
- The Electronic Payments Association, representing over 10,000 financial institutions, develops rules for the Automated Clearing House network (ACH), known as the NACHA Rules. These rules require that financial institutions maintain fraud detection systems, but they do not apply to transactions made via text message, so consumers who make such transactions are not covered by the detection systems.
- Regulation E, which implements the Electronic Fund Transfer Act, exempts transactions done by telephone from the requirement that customers receive a receipt for electronic transactions. However, whether this exemption applies to mobile payments conducted using a wearable device, such as a watch, is not outlined in the law.
- No comprehensive federal or state law regulates transaction services from nonbank providers such as PayPal. In addition, nonbank mobile payment providers are not supervised by any federal agency. Because these providers are important participants in the mobile payments marketplace, these gaps in the law may leave consumers subject to provider practices that are not in accordance with the law and without error resolution rights or limitations on liability, among other substantial risks.

- Generally, in the event of insolvency, nonbanks such as Google Wallet and PayPal may be subject only to state money transmitter laws rather than FDIC insurance coverage. In most states, these laws provide inadequate protection for consumer transaction account funds and could leave the funds of mobile payments customers at risk.
- If a consumer makes a mistake, such as a typing error when sending a mobile payment, the Uniform Electronic Transactions Act provides limited relief under certain circumstances, such as when no opportunity to correct an error was provided at the time of entry, but the law does not require payment providers to notify consumers of their right to correct a mistake, so consumers are unlikely to be aware that they can do so. Many customers may be unaware of this opportunity, leading to needless loss of consumers' funds.
- A denial of service attack, in which access to a provider's website is shut down, may substantially impede a consumer's ability to make timely mobile payments. No law directly protects consumers who are unable to make payments before the due dates and must pay additional charges as a result of such attacks.

Ambiguities

- The applicability of TILA protections to mobile payments in which a consumer authorizes a nonbank payment provider to charge a credit card account is unclear.
- Until the CFPB enacts a final rule governing prepaid cards, limitations on liability for lost or stolen prepaid cards (including those connected to mobile payment transactions) are available only at the discretion of the prepaid provider.

Stage 3: After a mobile payment is made

Issues can also arise after consumers make mobile payments, and protections are largely absent. For example, customers may need to stop or revoke authorization of electronic payments, but that ability is not ensured. Consumers also confront risks to their account balances with regard to the lack of legal restrictions on overdraft fees, privacy, and security when using remote deposit capture—sending a picture of a check via a mobile device in order to place funds in an account for use in making mobile payments. And the absence of a guaranteed ability to disable lost or stolen phones creates additional vulnerabilities.

Gaps

- Excessive overdraft fees can drain a consumer's bank account. Although a recent rule requires that consumers affirmatively agree ("opt in") to be charged for debit card overdraft transactions, it is limited in scope. It does not apply to payments made with a mobile device except one-time debit card purchases and restricts only the assessment of debit overdraft fees while still allowing an institution to assess a fee for checks, ACH electronic transactions, or other types of transactions. As a result, mobile payments customers are at risk of incurring significant overdraft fees.
- Consumers can deposit checks using their smartphones, but gaps in the law leave several questions unanswered. For example, the law does not define who pays for funds lost due to fraud. In addition, whether banks are required to make mobile deposit funds available promptly, as they are for money deposited through other means, is ambiguous.

- No comprehensive federal or state law protects consumers from security breaches or privacy invasions, and existing law offers only limited protections. Consumers have no right to sue if a financial institution violates the law and must rely on federal enforcement actions. State laws vary greatly, typically requiring only that consumers be notified after a breach.
- Laws requiring that consumers be able to remotely disable lost or stolen smartphones in order to protect financial and other information stored on the device have been enacted only in California and Minnesota; there is no federal statute.
- If a bank fails, deposit insurance protects consumer funds on prepaid cards only when the consumer has registered the card and the bank has placed the funds in "pass-through" accounts.
- If a nonbank seller of prepaid cards fails, state insolvency and federal bankruptcy law promises little if any relief for those who bought the cards.
- No comprehensive federal law provides consumers relief for privacy invasions. A federal statute does require financial institutions to disclose their privacy policies and practices, but that law is ambiguous because, although the FTC has brought enforcement cases alleging unfair and deceptive conduct, the decisions have been grounded in the unique facts of each case. As a result, consumers have only limited privacy protections. State privacy laws are not tailored to the electronic environment, and the courts have established rules that make it difficult for consumers to prove injury.
- There is a major gap in the law because it does not clearly provide for the stop payment or revocation of transfers that are not recurring payments. The Electronic Fund Transfer Act delineates authorization requirements for recurring transfers but not for single electronic fund transfers. Consumers can put a stop payment on a preauthorized debit but not on a single payment.

Ambiguities

- Although the law grants consumers the right to stop payment of preauthorized electronic payments, it does not clearly provide that right when consumers make other types of electronic payments, such as one-time mobile payments. In addition, the law is ambiguous as to the effect of a consumer's order to stop payment on future instances of a preauthorized transfer. Precisely how the Uniform Commercial Code applies to problems such as the alteration of checks deposited via smartphone is unclear. The code allocates liability for alterations of checks, but because it was drafted long before mobile technology was developed, it is ambiguous as to whether and how its provisions apply to such transactions.

Overlap

- Consumers can charge purchases to their wireless carrier bills, but some third parties have engaged in "cramming," in which they charge unauthorized purchases to consumers' bills. Both the FTC and Federal Communications Commission have authority to take action against companies that engage in this practice. The FCC has not used this power to regulate cramming, and although the FTC has brought enforcement actions against crammers its resources are limited. Further, no statute or regulation explicitly allows consumers to sue for damages caused by this scam.
- Federal and state breach notification laws, which require a company to inform customers if their data have been compromised, overlap, making it unclear what protections may apply.

Conclusion

Although many laws are applicable to mobile payments and cover a variety of issues, the overall legal framework is neither comprehensive nor consistent. Unfortunately, state and federal laws have not kept pace with technological developments that have enabled new products and services. Rather, current laws are filled with gaps, ambiguities, and overlap that undermine important consumer protections.

Endnotes

1 Forrester Research Inc., "Forrester Research Mobile Payments Forecast, 2014 to 2019" (Oct. 20, 2014), https://www.forrester.com/US+Mobile+Payments+Forecast+2014+To+2019/fulltext/-/E-RES115498.

2 Federal Deposit Insurance Corp., *2013 FDIC National Survey of Unbanked and Underbanked Households* (October 2014), 50, https://www.fdic.gov/householdsurvey/2013report.pdf.

3 Dodd-Frank Wall Street Reform and Consumer Protection Act, 12 U.S.C. §§ 5481(14), 5531.

4 "The FDIC has affirmed its authority to prevent unfair and deceptive acts and practices generally under §8 of the FDI Act." Catherine M. Sharkey, "Agency Coordination in Consumer Protection," University of Chicago Legal Forum (October 2013), 337, note 38, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2443572.

5 "Memorandum of Understanding Between the Consumer Financial Protection Bureau and the Federal Trade Commission" (March 6, 2015), https://www.ftc.gov/policy/cooperation-agreements/ftc-cfpb-interagency-cooperation-agreement. "The CFPB and the FTC share regulatory enforcement over non-depository consumer financial product providers. The CFPB must consult with the FTC in defining respective jurisdictions. The statute thus contemplates that the two agencies can agree on a division of enforcement authority." Sharkey, "Agency Coordination," 337, note 36. "The CFPB has no authority to enforce the FTC Act. … The set of entities included in [the definition of "covered persons" in Dodd-Frank] is substantially broader than the set of bank entities excluded from direct FTC enforcement authority in §5 of the FTC Act. … Thus, a substantial source of overlap is the set of covered persons under Dodd-Frank who can also face direct FTC enforcement."

6 Electronic Fund Transfer Act (Regulation E), 12 CFR § 1005.7(b).

For further information, please visit:

pewtrusts.org/banking

Contact: Sultana Ali, officer, communications
Email: sali@pewtrusts.org
Phone: 202-540-6188
Project website: pewtrusts.org/banking