The Legal Framework of Mobile Payments

Gaps, ambiguities, and overlap

By
Professor Mark E. Budnitz

Feb 10, 2016

Contents

Overview 5

Stage 1: Using mobile devices to enter into contracts for mobile payment services 7

I. Introduction 7

II. The regulatory framework 8

III. Is a mobile device a credit card? 9

IV. Is a mobile device an 'access device' under the EFTA? 10

V. Disclosure of mobile payments contract terms online 11

A. Credit cards 11

B. Debit cards and other electronic fund transfers 13

C. General purpose reloadable prepaid cards 14

VI. What constitutes the consumer's acceptance of an online agreement? 17

A. Clickwrap agreements 17

B. Browsewrap agreements 18

C. Rolling contracts 19

D. Pre-dispute mandatory arbitration agreements 21

E. The law applicable to software licenses compared with other types of contracts 22

VII. Add-on services 23

VIII. Online modification of original contract terms 23

IX. Advertisements for financial services displayed on mobile device screens 24

X. Phishing scams 24

XI. Conclusion 25

Stage 2: Use of mobile device to make payments 26

I. Introduction 26

II. Mobile payment by credit card 27

III. Mobile payment by debit card 30

IV. Mobile payment by prepaid accounts and cards 33

V. Regulation of nonbanks 34

VI. Regulation of payments charged to accounts with wireless carriers 35

VII. Authentication 36
VIII. Consumer mistakes 37
IX. Virtual currency 38
X. Children making online payments without parental consent 39
XI. Denial of service attacks 39
XII. Natural disasters 40
XIII. Payment processors 40
XIV. Third-party service providers 41
XV. Conclusion 42
Stage 3: Consumer problems after payment is made 42
I. Introduction 42
II. Consumers' ability to stop electronic payments 43
III. Overdrafts 47
IV. Remote deposit capture 49
V. Security 54
VI. Privacy 58
VII. 'Kill switch' laws 63
VIII. Unauthorized payments charged to consumers' accounts with wireless carriers 64
IX. Children making mobile payments without parental consent 66
X. Insolvency and bankruptcy 66
XI. Remedies 70
A. Unauthorized use of credit and debit card accounts 70
B. Other federal and state remedies 71
C. Requiring arbitration and restricting class actions impede consumer remedies 71
XII. Conclusion 73
Options for lawmakers 75
Appendix A: Credit cards: Withholding and billing error rights under TILA 77
Appendix B: Liability for violations of TILA 79
Appendix C: Debit cards: Error resolution procedures under the EFTA 80

Appendix D: Liability for violations of EFTA 82
Appendix E: Liability for violations of the NACHA rules 84
Appendix F: Federal laws prohibiting unfair, deceptive, and abusive acts or practices 84
Appendix G: State unfair and deceptive acts or practices statutes 86
Endnotes 87

Overview

As the popularity of mobile payments grows, it becomes increasingly important to understand the legal framework in which these transactions take place. Consumers need to know their rights and responsibilities. They need to be alert to the financial risks they are exposed to and the legal remedies available when transactions go awry. Financial institutions and other companies that facilitate mobile payments need clear rules describing their obligations, rights, and liability as they develop new mobile payment products and contract with consumers for mobile payment services. Finally, policymakers need to understand the impact of applicable laws and rules on consumers and mobile payment providers so they can evaluate whether they are adequate, and if not, what new provisions are needed.

This report describes and analyzes the legal framework of mobile payments. That framework consists of a wide variety of state and federal statutes, regulations, agency "guidance," and court decisions. Determining which laws apply to mobile payments is complicated by several factors. For example, many federal agencies have regulatory, supervisory, or enforcement authority over various aspects of mobile payments services when offered by financial institutions under their jurisdiction. These include the "prudential regulators," the Office of Comptroller of the Currency, the Federal Reserve, the Federal Deposit Insurance Corp., and the National Credit Union Administration. Companies not within legal definitions of financial institutions, such as PayPal and other nonbanks, are subject to the authority of the Consumer Financial Protection Bureau and the Federal Trade Commission. Telecommunications companies are regulated by the Federal Communications Commission. State agencies, such as bank commissioners and attorneys general, enforce their laws applicable to mobile payments.

A final factor making it difficult to determine which laws apply is the flood of new products and services that the industry offers, as well as the different types of situations in which consumers make mobile payments. For example, most consumers charge their mobile payments for goods and services to credit cards, debit cards linked to a checking account, or prepaid card accounts. Others agree to charges being placed on their wireless carrier's monthly bills along with the communications charges for using their cellphones. Entirely different laws apply depending on which type of account the consumer uses. Issues that arise vary significantly, from the circumstances under which online contract provisions are enforceable to a company's liability for data security breaches and privacy invasions.[1] Applicable laws range from centuries-old contract law and tort theories to new federal and state statutes. In some instances, no law at all applies.

What emerges is a patchwork of laws that is characterized to a large extent by three features: gaps (situations in which no law applies); ambiguities (where it is not clear whether a law applies); and overlap (where two or more laws apply to the same situation and more than one agency has legal authority over the same type of conduct).

This report describes the legal framework of mobile payments as it applies to three stages of mobile payment transactions. The first stage is when consumers use mobile devices to enter into contracts for mobile payment services. The second stage describes the law that applies when consumers use mobile devices to make payments. The final stage focuses on problems consumers may confront after they make mobile payments. They are referred to, respectively, as Stage 1, Stage 2, and Stage 3.

After discussion of each of the stages, the report includes a conclusion section that identifies those gaps and ambiguities that are likely to have the greatest impact on consumers who make mobile payments because they result in mobile payment transactions being less transparent and safe.

The report ends with a section that examines various policy options in light of the gaps, ambiguities, and overlap identified in the report. Each alternative has its benefits and drawbacks. The report does not advocate any position but instead provides a legal framework that may aid policymakers in making a decision on future action.

Stage 1: Using mobile devices to enter into contracts for mobile payment services

I. Introduction

This portion of the report describes and analyzes the regulatory framework in which mobile payments occur. It then discusses discrete legal issues that arise when consumers enter into contracts for mobile payment services. Topics include the legal status of the mobile device itself when consumers charge their purchases to their credit or debit card accounts. The report also analyzes the legal status of prepaid cards and the circumstances under which consumers agree to legally enforceable terms in online agreements. In addition, the report examines arbitration agreements, add-on services, advertisements on mobile device screens, and phishing scams.

As described in greater detail below, there are gaps where no law applies to mobile payments, ambiguities where it is not clear how or whether current law applies, and overlap where two or more laws may apply to the same situation or more than one government agency has authority over a transaction.

There are many gaps where no law explicitly applies to mobile payments. Examples include issues such as whether a mobile device should be treated as legally equivalent to a credit card or as an "access device" when a mobile payment is charged to a debit card account. When consumers charge mobile payments to their credit card accounts, the federal Truth in Lending Act requires disclosures to be "conspicuous," but that law does not explain how to apply the conspicuous standard to payments made using a mobile phone. Consumers increasingly use general purpose reloadable prepaid cards when making mobile payments, but no law currently regulates those cards, although this may be remedied if a proposed regulation becomes law. Finally, there is a gap in the law governing software licenses. Software is not explicitly included under the Uniform Commercial Code (UCC), and key provisions of the UCC do not apply to licenses.

The law also is ambiguous in several respects. For example, with passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank), it is no longer clear whether some federal agencies can enforce the Federal Trade Commission Act. Consumers who agree to engage in mobile payment transactions typically enter into contracts that they consent to via an online medium. The courts have not developed clear rules or standards for determining the circumstances under which consumers are bound to contracts that purport to obtain the consumer's consent by a mere click of a mouse or the opportunity to browse on a website and

read contract terms. The law also is ambiguous in regard to the validity of "rolling contracts," in which some terms are disclosed initially and more terms are disclosed later.

There is some overlap in the authority of the Consumer Financial Protection Bureau (CFPB) and the Federal Trade Commission (FTC). Moreover, it is uncertain how far the CFPB's supervision will reach. It has the legal jurisdiction to subject some companies within the mobile payments market to supervision but has not yet indicated whether it will use this authority.

II. The regulatory framework

Several federal agencies have authority over companies that participate in the mobile payments environment. The agencies exercising this authority engage in one or more of the following activities:

> (1) The agencies supervise institutions under their authority. This authority permits the agencies to demand books and records and send examiners to inspect the institutions by visiting their offices.
> (2) The agencies can engage in rule-making and issue regulations. However, they can issue only regulations that a federal statute grants them the power to issue. The statutes most pertinent to mobile payments include the Truth in Lending Act (TILA), the Electronic Fund Transfer Act (EFTA), Dodd-Frank, and the Federal Trade Commission Act. The regulations accompanying TILA are known collectively as Regulation Z (Reg. Z), and those accompanying the EFTA make up Regulation E (Reg. E).
> (3) The agencies can bring lawsuits to enforce the statutes and regulations. In this instance, the regulators have two options: First, they can bring an administrative proceeding, a lawsuit heard within the agency and decided by an administrative law judge.[2] (A company can appeal an adverse decision to a federal court.) Alternatively, the regulators can bring a lawsuit in a federal District Court.

Before Dodd-Frank went into effect beginning in 2010, many of the supervision, regulation, and enforcement activities that govern mobile payments were done by "prudential" regulatory agencies (focused primarily on the safety and soundness of banks and credit unions) that no longer have that authority.[3] Much of it is now being done by the CFPB, but exactly which functions are now subject to the CFPB's authority varies among types of institutions.[4] Banks with more than $10 billion in assets are subject to CFPB supervision, enforcement, and rule-making in regard to their consumer financial services, including mobile payments. Banks with fewer assets are subject to the CFPB's regulations. The prudential regulators still supervise

them and enforce CFPB regulations.[5] The CFPB also has enforcement authority over the banks' third-party service providers.[6] And nonbanks are subject to the CFPB's regulations and its enforcement actions. In addition, payday lenders, mortgage lenders, and brokers, as well as nonbank private education lenders, are subject to CFPB supervision. Finally, the CFPB can designate companies with revenue exceeding specified amounts in certain markets as "larger participants" and subject them to supervision by the CFPB. So far, debt collection, consumer reporting, student loan servicing, nonbank auto finance, and international money transfers have been identified as "larger participants."

Dodd-Frank creates an overlap in the authority of the CFPB and FTC. Both have supervisory, rule-making and enforcement authority in regard to some of the same companies when the 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.[7] Dodd-Frank added "abusive" acts or practices to the CFPB's arsenal but not the FTC's.

III. Is a mobile device a credit card?

When consumers pay by waving their mobile device (linked to a credit card) in front of a card reader at the point of purchase, the device transmits the credit card's "credentials," the payment card account number and other information about the account, to the reader. The question arises as to whether that makes the device the legal equivalent of a credit card because it includes the information contained in the physical card's magnetic stripe or computer chip. The law is ambiguous, since it does not mention mobile devices, but the definition of a credit card seems broad enough to include the devices.

Reg. Z defines "credit card" to mean "any card, plate, or other single credit device that may be used from time to time to obtain credit."[8] The official interpretation of Reg. Z provides:

> An account number that accesses a credit account, unless the account number can access an open-end line of credit to purchase goods or services, [is not a credit card]. For example, if a creditor provides a consumer with an open-end line of credit that can be accessed by an account number in order to transfer funds into another account, … the account number is not a credit card. … However, <u>if the account number can also access the line of credit to purchase goods or services (such as an account number that can be used to purchase goods or services on the Internet),</u> the account number is a credit card.[9]

In other words, the crucial requirement for constituting a credit card is not a physical card at all. The 4th U.S. Circuit Court of Appeals stated it this way: The "core element of a 'credit card' is the account number, not the piece of plastic."[10]

This definition of credit card has implications for mobile payments. When a consumer uses a mobile phone to purchase goods by waving the card in front of a reader at the point of sale, the mobile phone itself could well be considered a credit card for purposes of TILA. Some wireless carriers provide a service through which a mobile phone can be used to make a purchase that will be billed to the consumer's cellphone account. "If the consumer is permitted to defer payment for these goods until the cellphone bill arrives, the cellphone could constitute a credit card."[11]

Based on the broad and general definition of credit card in Reg. Z, the official interpretation, and case law, it appears that a mobile device falls within the definition of a credit card.[12] If that analysis is correct, consumers who use mobile phones to charge purchases to their credit card accounts may not obtain the full benefit of TILA's liability cap when there is unauthorized use of that account. To limit liability to no more than $50, Reg. Z requires consumers to notify the card issuer of any unauthorized use.[13] When consumers' credit cards are stolen, most probably understand that they have to promptly notify the card issuer in order to limit their liability to less than $50. In contrast, when consumers' mobile phones are stolen, they may not immediately realize that the thief could charge purchases to their credit card accounts since mobile phones increasingly are used for multiple important everyday functions besides credit card payments. Consequently, they may not notify the card issuer until more than $50 is charged by the thief. While many consumers will not be seriously harmed by incurring a $50 loss, if the mobile phone contains credentials for several credit card accounts the consumer's total loss could create a significant hardship.

IV. Is a mobile device an 'access device' under the EFTA?

When consumers pay by waving their mobile device (linked to a debit card) in front of a card reader at the point of purchase, the device transmits to the reader the debit card's "credentials," the payment card account number, and other information about the account. The question arises as to whether that makes the device the legal equivalent of an access device such as a debit card, since it includes the information contained in the physical card. As in the case of credit cards, the law is ambiguous because it does not mention mobile devices, but the definition of "access device" appears to include such devices.

Reg. E defines "access device" to mean "a card, code, or other means of access to a consumer's account, or any combination thereof, that may be used by the consumer to initiate electronic fund transfers."[14] The official staff interpretation of access device in Reg. E provides the following example. "The term 'access device' includes debit cards, personal identification numbers (PINs), telephone transfer and telephone bill payment codes, and other means that may be used by a consumer to initiate an electronic fund transfer."[15] It appears from the Reg. E definition and the staff interpretation example that a mobile device falls within the definition of an access device.[16] If that is a correct analysis, financial institutions that provide mobile payment services must comply with Reg. E's prohibition of the unsolicited issuance of access devices.[17] Precisely how this provision will be applied to mobile devices is uncertain since mobile payments are relatively new.

V. Disclosure of mobile payments contract terms online

Federal law requires the company that issues a credit card or a debit card or provides other electronic fund transfer services such as mobile bill paying to disclose certain information when consumers first apply for the card or service and at certain other times after that. Without those disclosures, consumers cannot know essential information about their use of the payment instruments, including their rights and responsibilities. Credit card issuers and financial institutions providing debit cards and other mobile financial services often make the required disclosures online.[18] If the card issuer does not comply with federal disclosure requirements, it may be liable for damages to the consumer.[19] The following describes the legal framework for disclosing that information online.

A. Credit cards

Credit extended by means of credit cards, in which credit is offered on a continuous basis, is what TILA and Regulation Z call "open-end credit." TILA and Reg. Z require certain disclosures to be made when the card issuer solicits credit card applications and when the consumer applies for the card.[20] They require the disclosures to be "clear and conspicuous."[21] Furthermore, some disclosures must be more conspicuous than others.[22] TILA and Reg. Z require the uniform disclosure of rates, fees, and other cost information.[23]

There is a gap in the law, however, because neither TILA nor Reg. Z defines "conspicuous," although the regulation does include some formatting rules for solicitations and account-opening disclosures.[24] Lacking sufficient guidance in Reg. Z, some courts apply the definition of "conspicuous" provided in the Uniform Commercial Code.[25] Under the UCC, a term is conspicuous if "it is so written, displayed, or presented that a reasonable person against which

it is to operate ought to have noticed it."[26] The provision includes examples such as larger type than surrounding text, contrasting color, or a different font.

The Credit Card Accountability Responsibility and Disclosure Act of 2009 (Credit CARD Act) imposed several new requirements on the marketing, application, and issuance of credit cards. Card issuers are not permitted to open a credit card account or increase the credit limit unless the issuer considers the consumer's ability to make the required minimum periodic payments under the terms of the account.[27] The issuer's determination of the consumer's ability to pay must be based on the consumer's income or assets and the consumer's current financial obligations. The issuer must establish and maintain reasonable written policies and procedures to consider the consumer's ability to pay.[28] Reg. Z describes various factors that the issuer must consider.

The CARD Act also has provisions intended to protect young consumers, defined as those less than 21 years old, from accruing debt that they cannot repay.[29] The law prohibits issuing a card to a young person unless the transaction fits under one of two exceptions. First, a young consumer may be issued a credit card if the application contains the signature of a person 21 years or older who acts as a co-signer and has the means to repay all credit card debts incurred by the consumer. [30] The second exception is when the young consumer submits financial information "indicating independent means of repaying any obligations" arising from using the credit card.[31]

Credit card issuers often identify the consumers they want to target by purchasing prescreened lists from consumer reporting agencies. The CARD Act amends the Fair Credit Reporting Act to prohibit these agencies from including consumers under the age of 21 on prescreened lists if a consumer's report includes a date showing that he or she is under 21.[32] An exception is made for young consumers who consent to be included in these lists.

Finally, the CARD Act includes provisions intended to protect consumers who are students of institutions of higher education. All of the above protections for consumers under 21 apply. In addition, a card issuer may not offer a student under 21 any "tangible item" to induce the student to apply for an open-end credit plan if the offer is made on or near the student's campus or at an event sponsored by or related to the institution.[33] In addition, the institution must publicly disclose any agreement it has made with a card issuer in regard to marketing the issuer's credit card.[34]

Reg. Z specifically permits disclosures for open-end credit to be made electronically.[35] Consequently, companies can make the disclosures available on desktops, laptops, tablets, or

mobile devices. “Disclosures provided in electronic form must be accurate as of the time they are sent, in the case of disclosures sent to a consumer’s email address, or as of the time they are viewed by the public, in the case of disclosures made available at a location such as a card issuer’s website.”[36]

Under certain circumstances, disclosures must be made in electronic form, such as if the consumer accesses a credit card application or solicitation electronically.[37] This follows from the Reg. Z requirement that disclosures be made in a timely manner on or with the application or solicitation. To illustrate what is meant by electronic access, the official interpretation provides the example of access online at a home computer.[38] To illustrate what is meant by disclosures in electronic form, the official interpretation gives the example of disclosures provided on the issuer’s website with the application or solicitation.

In addition to TILA and Reg. Z, another federal law applies to the disclosures required by TILA and Reg. Z. The Electronic Signatures in Global and National Commerce Act, popularly known as E-Sign, permits legally required disclosures to be made electronically.[39] However, the disclosures can be made electronically only if the consumer consents, and the statute contains very specific requirements for how that consent may be obtained.

B. Debit cards and other electronic fund transfers

The EFTA requires the disclosure of certain information consumers need when they apply for a debit card and other electronic fund transfer services. Reg. E provides that the disclosures be “clear and readily understandable, in writing, and in a form the consumer may keep, except as otherwise provided in this part.”[40] The disclosures may be made in electronic form. But the financial institution must comply with the requirements of E-Sign, including the consumer consent rules. Reg. E requires the financial institution to make initial disclosures “at the time a consumer contracts for an electronic fund transfer service or before the first electronic fund transfer is made.”[41] The disclosures include the consumer’s liability for unauthorized transfers, the types of transfers the consumer can make, and fees. The institution must include notices regarding the right to receipts, periodic statements, stop payment, preauthorized payments, and error resolution.[42]

C. General purpose reloadable prepaid cards

Consumer use of general purpose reloadable prepaid cards has grown tremendously in recent years. There has been a serious gap in consumer protections because no federal laws or regulations impose online disclosure requirements for general use prepaid cards, but this will likely change when proposed CFPB rules take effect. Illinois law requires general use reloadable prepaid cards to contain certain disclosures at the time of purchase.[43] For cards sold online, the disclosures "must be clearly and conspicuously accessible on the issuer's Internet website prior to purchase."[44] The statute also requires that the disclosures themselves be "clear and conspicuous."[45]

Most states have money transmitter laws.[46] According to the CFPB, many of these laws may apply to prepaid product providers, requiring them to be licensed and to post a surety bond to cover consumer losses. However, the CFPB also understands that state oversight varies from state to state and that many states "may not have streamlined processes" to pay consumers when a provider files for bankruptcy.[47] However, the extent to which these laws regulate the industry varies considerably. None of these laws requires disclosure of important information when the consumer enters into a contract for mobile payment services.[48]

The CFPB has issued a proposed prepaid account regulation that is expected to be finalized soon. It is motivated by the concern "that because prepaid cards can be so similar to credit and debit cards … consumers may not realize that their prepaid cards lack the same benefits and protections as those other cards."[49] The proposed rule is relevant to mobile payments because prepaid card users increasingly use this product to make mobile payments.[50] Therefore, the prepaid card rule directly addresses mobile payments. In addition, the rule deals with issues that arise in all Web-based environments. The rule reflects the CFPB's approach to this medium.

The CFPB's proposed rule subjects payroll and general purpose reloadable prepaid cards to most of the requirements of Reg. E.[51] In regard to mobile payments, the definition of "prepaid account" covers only those products that can store funds. To the extent that a digital wallet, for example, merely stores payment credentials (for example, a consumer's bank account or payment card information) rather than storing the funds themselves, the digital wallet would not be considered a prepaid account under the proposed rule. (Digital wallets include smartphones that store the consumer's payment credentials for credit, debit, and prepaid card accounts. With those credentials, consumers can make payments using their smartphones.[52]) For example, as currently structured, Apple Pay would not be subject to the rule. "If, however, a

digital wallet allows a consumer to store funds in it directly, then the digital wallet would be a prepaid account if the other criteria of the proposed definition are also met."[53]

Under the proposal, prepaid accounts would be subject to the Truth in Lending requirements of Reg. Z if they have an overdraft capability.[54] The rationale is that an overdraft is credit, and a prepaid card account with overdraft capability is considered a credit card.

The proposed rule requires businesses to provide both a short-form disclosure and a long-form disclosure. Both forms must be given to the consumer prior to account or card acquisition. Consumers who acquire a prepaid card via the Internet must be given electronic disclosures.[55] This includes acquisitions via mobile applications. However, the card issuer would not have to comply with the consumer notice and consent requirements of the federal E-Sign law.[56] The CFPB proposed rules contain very specific formatting requirements for the forms, including font or pixel size. Disclosures also must be made in a foreign language under certain circumstances.[57]

The top portion of the short-form disclosure must disclose the monthly fee (if any), ATM withdrawal fees, purchase fees, and cash reload fees. The bottom portion must disclose ATM balance inquiry fees, customer service fees, inactivity fees (if any), "mandatory statements," and "incidence-based" fees.

Mandatory statements include disclosing that credit-related fees may apply and the number of fees other than those listed on the form that the consumer may incur. For example, the form would state, "We charge six other fees not listed here." The form also would be required to include a phone number and URL the consumer can use to access the long-form disclosure or an FDIC or National Credit Union Share Insurance Fund (NCUSIF) insurance statement if funds are not insured, and the URL for the CFPB.

The incidence-based fee disclosure requires informing the consumer of the three fees most often incurred for the product in the previous 12 months, not including the fees disclosed in the top portion of the form.

The long-form disclosure must disclose all the fees that may be imposed, including the amount as well as when the fees are imposed, waived, or reduced. If the card has overdraft capability, appropriate Reg. Z disclosures must be included. The disclosure form is required to include a phone number, URL, and mailing address where consumers can obtain more information, the CFPB's URL, and a URL and phone number for consumers to use if they have complaints. Finally, if funds are not insured, the form has to contain an FDIC or NCUSIF insurance statement.

D. Other potential legal guidance

The Federal Trade Commission Act prohibits unfair and deceptive acts or practices. The FTC can issue rules and can enforce those rules as well as the general prohibition of unfair and deceptive acts or practices. However, Dodd-Frank substantially restricted the FTC's rule-making authority. In regard to consumer financial products or services such as mobile payments, the CFPB now has exclusive authority to engage in rule-making.[58] The CFPB has no authority to enforce the FTC Act, but under Dodd-Frank the agency has explicit authority to issue rules and bring enforcement actions against those under its jurisdiction who engage in unfair, deceptive, or abusive acts or practices.[59] 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 Comptroller of the Currency, National Credit Union Association, and Federal Deposit Insurance Corp. Dodd-Frank created ambiguity by throwing into doubt whether those agencies can enforce the FTC Act. It appears that they retain the authority to bring actions against financial institutions under their jurisdiction that engage in unfair or deceptive acts or practices (UDAP).[60]

Regardless of whether an agency has explicit authority to bring enforcement actions under the FTC Act, when it brings UDAP actions, courts will be influenced by the FTC's enforcement actions, rules, and guidance in deciding whether disclosures meet the requirements for credit and debit cards.

The FTC has issued a guidance on digital advertising that explains how information should be presented in online ads to ensure they are not unfair or deceptive.[61] Some of the discussion and specific illustrations address representations made on mobile devices. That guidance appears to be directly relevant to disclosures in online card agreements as well. For example, "The same consumer protection laws that apply to commercial activities in other media apply … [to] activities in the mobile marketplace." "If a disclosure is too small to send on a mobile device and the text of the disclosure cannot be enlarged, it is not a clear and conspicuous disclosure." The guidance includes examples. The FTC notes that an ad appearing on a mobile device may require zooming in or scrolling horizontally, raising questions as to whether necessary representations are clear and conspicuous because it is unlikely a consumer will zoom or scroll.

The Federal Reserve's views on text messages may be relevant to required disclosures: "The font size, screen size, and character limitations inherent in SMS text messaging raises significant

doubts about the ability of SMS text messages to satisfy the Regulation E disclosure requirements."[62]

VI. What constitutes the consumer's acceptance of an online agreement?

A. Clickwrap agreements

Clickwrap agreements allow consumers to agree to the terms of online credit and debit card agreements. Companies that offer alternative payment methods, such as PayPal, also allow consumers to enter into contracts online. One form of making the contract available is the clickwrap agreement, also known as a "clickthrough" agreement. The consumer agrees to the online terms, typically by clicking on a button that says "I agree." "The 'I agree' button commonly appears below a scroll-down window that contains the standard terms. … In some cases, the 'I agree' button appears next to a link that would take the consumer to another page with the standard terms. … In some cases, the clickwrap text refers to additional terms, available on a different website."[63] Yet, even if the clickwrap contract obtained a consumer's consent in a valid fashion, courts have held that specific terms are unconscionable or otherwise unenforceable.[64]

Moreover, some firms operating online have deceived consumers into clicking on an "I agree" button without realizing they were agreeing to purchase goods or services. The FTC successfully sued a company engaging in that practice.[65]

Courts have held that, in general, clickwrap agreements are valid and that consumers are bound by their terms. However, the case law does not validate these agreements unquestioningly; many of these courts reached that conclusion only after careful examination of the manner in which consumer consent was obtained on the website.[66] Moreover, some courts insist they are not applying new legal requirements when determining the validity of clickwrap agreements:

> "An agreement where the terms are presented in an electronic form, or one that is signed electronically, is therefore interpreted and applied using the same common law rules that have been applied for hundreds of years to oral and written agreements."[67]

In conclusion, courts have upheld the enforceability of the typical clickwrap agreement as a valid way to obtain a consumer's consent. However, they have not ruled that these agreements

are automatically valid; they may be invalid if not carefully presented, and specific terms of the agreements may be successfully challenged.

B. Browsewrap agreements

Many companies obtain consumer consent online through what is known as browsewrap agreements. These agreements differ from clickwrap agreements in that they do not give the consumer the opportunity to affirmatively indicate consent by clicking on an "I agree" button. Instead, the online page includes a hyperlink to another page that includes the agreement. Companies contend the consumer consents to the contract by purchasing the goods or services offered or by simply continuing to use the site. Agreements may state that such conduct constitutes consent. "The defining feature of browsewrap agreements is that the user can continue to use the website or its services without visiting the page hosting the browsewrap agreement or even knowing that such a Web page exists."[68]

In face-to-face transactions, consumers write their unique signatures on a piece of paper. Unless the seller engages in fraudulent conduct, courts assume the consumer's signature indicates actual agreement to be bound by the terms printed on the paper. In clickwrap agreements, courts, in effect, substitute clicking on the "I agree" button for writing a signature. A browsewrap agreement is one step removed from a clickwrap agreement. That is, the consumer does nothing to explicitly indicate consent.

The case law on the validity of browsewrap contracts is ambiguous because courts have been less willing to validate browsewrap agreements. Sometimes courts insist they are applying traditional principles of contract law that require the "mutual manifestation of assent, whether by written or spoken word or by conduct."[69] Applying those principles, courts require evidence that the consumer had actual or at least "constructive" knowledge of the seller's terms and conditions.[70] To satisfy the constructive notice requirement, the seller must put the consumer on "inquiry notice." Courts examine both the design and content of the website and the Web page containing the agreement to determine whether the requisite notice was given.

Examples of this type of online agreement approved by the courts include requiring users to check a box confirming they had both read and agreed to the website's terms and conditions and posting a notice below the "sign up" button: "By clicking Sign Up, you are indicating that you have read and agree to the Terms of Service."[71]

Courts have held that the inquiry notice requirement has not been satisfied when the link to the agreement "is buried at the bottom of the page or tucked away in obscure corners of the website where users are unlikely to see it."[72] Courts have invalidated agreements where links are not obvious or the agreement is not easily accessible because it requires several steps.[73] Even a conspicuous link on every page of the website, including a link close to buttons the user has to click on to complete a purchase, was found to be insufficient.[74] Users are not bound by contract terms that are hidden or difficult to reach.[75]

Courts have acknowledged that the level of experience and sophistication varies greatly among different consumers.[76] Consequently, although courts consider the sufficiency of a website's inquiry notice according to a "reasonably prudent" user standard, it can be difficult to apply that standard because of the wide range of consumers' familiarity with how websites notify and provide access to browsewrap contracts.[77] The 2nd U.S. Circuit Court of Appeals even refused to consider the user's past experience with websites containing browsewrap contracts beyond the website involved in the case before it.[78]

In conclusion, consensus has not yet emerged on the legal validity of browsewrap agreements. Websites make browsewrap contracts available to consumers in many different ways. Courts have closely examined the design and content of the websites, upholding many of the browsewrap agreements but also invalidating many others.

C. Rolling contracts

A rolling contract is one in which the consumer is provided the contract terms in two or more stages. These are known as "money now, terms later" contracts. As applied to mobile payments, one example is when the consumer uses a mobile device to pay for goods, charging the purchase to a credit card account. At the point of sale the consumer knows a few of the contract terms, such as the price. But inside the package containing the goods, there may be a written contract with many additional terms, such as a mandatory arbitration clause. Another example is the purchase of software. The consumer may pay for this before the End User License Agreement appears on an online screen.[79]

The case law on the enforceability of the additional terms in rolling contracts is not uniform, resulting in ambiguity. Most, but not all, courts follow two 7th U.S. Circuit Court of Appeals decisions (ProCD v. Zeidenberg and Hill v. Gateway) that uphold the validity of rolling contracts if the consumer can terminate the transaction after having the opportunity to read the contact terms that are provided after purchase.[80] Under those opinions, if the consumer does not terminate the transaction, a contract is formed at the expiration of the termination period. The

contract consists of all the terms provided prior to the expiration of the termination period. However, a few decisions have directly rejected the holdings and the reasoning of the 7th Circuit decisions. The most prominent is Klocek v. Gateway. In those jurisdictions that reject the 7th Circuit's reasoning, the courts believe a contract is formed when the consumer offers to purchase the goods and the seller accepts the offer by completing the transaction, agreeing to ship the goods, or actually shipping them. Under these decisions, any terms provided by the seller later are merely proposals and do not bind the consumer unless the consumer expressly agrees to them.[81]

The two lines of cases engage in fundamentally different analyses. In ProCD, the court declares that it is the seller who is making the offer; the consumer has the option whether or not to accept. In Klocek, the court regards the consumer as the party making the offer. The contract includes only the terms at the time the consumer offers to purchase the goods or services. The seller has the option whether or not to accept. In ProCD, no contract is formed unless and until the consumer accepts the offer or the termination period expires. The agreement includes the terms provided prior to acceptance of the contract or expiration of the termination period. In Klocek, a contract is formed when the seller accepts, which may be well before the later terms are provided to the consumer.

The 7th Circuit decisions left many questions unanswered, and subsequent cases have not produced definitive answers. The court ruled that all the contract terms bound the consumer because the seller structured the transaction so that the consumer had the opportunity to read the terms provided after purchase. But the court did not indicate how much time the seller has to give the consumer. The ProCD opinion states that under the Uniform Commercial Code, the buyer has the opportunity "to make a final decision after a detailed review."[82] In Hill v. Gateway, the consumer had 30 days to return the goods. The court did not specifically discuss whether 30 days was sufficient time, but that is the obvious implication from the court's holding. In the Klocek case, the consumer was given only five days to return the product. The court never reached the issue of whether that was sufficient time because it held that the consumer was not bound by the terms provided after purchase. From the cases, we know that 30 days is sufficient time, but we do not know what may constitute too little time.

Another issue is whether consumers can use the product during the time they are given to read the terms that are disclosed after purchase and decide whether to terminate the transaction. The ProCD court approved a contract in which "ProCD proposed a contract that a buyer would accept by *using* the software after having the opportunity to read the license at leisure."[83] But what if the consumer began to use the product before noticing that there were terms disclosed after purchase?[84] A court that closely analyzed the reasoning and holdings of the ProCD and Hill

cases found that consumers could use the goods during the 30-day return period and still retain the right to terminate the transaction and return the goods within 30 days.[85]

However, the consumer who returns the goods may incur costs in doing so. These may include the expense of shipping as well as restocking or other fees imposed by the seller. Would a court hold that the consumer is not bound by the later disclosed terms if the inconvenience or cost is so great that a reasonable consumer would not take advantage of the right of return? The Hill court found the question "interesting" but said the consumers were bound by whatever the expenses might be because they knew before purchasing the goods that some important terms would come later.[86]

Most of the cases have involved "shrinkwrap" rolling contracts, in which the consumer purchases the product in a store and additional terms are in the box containing the goods. Because there are so few cases involving rolling contracts for electronic services, it is impossible to know how the courts will treat them in the future.[87]

In conclusion, it appears that most courts enforce rolling contracts. However, there is no definitive case law addressing important issues related to enforcement of those contracts in the mobile payment context. Moreover, courts in several jurisdictions do not enforce those contracts at all.

D. Pre-dispute mandatory arbitration agreements

The contract requirement in Internet transactions that has been challenged most often is the pre-dispute mandatory arbitration clause. This provision states that the consumer has no right to sue the company in a court should a dispute arise. Instead, the consumer can bring a case to be heard before an arbitration forum. The companies that include these requirements contend that arbitration is fair and is as fast as or faster than judicial proceedings, and that it can be less expensive.[88] A number of legal objections to mandatory arbitration have been raised, most fundamentally that it prevents consumers from choosing whether to pursue a dispute in court.[89] More specific objections include that the arbitrator is not required to follow the law, the arbitrator can severely limit discovery, there is no jury, the hearing may be held far from where the consumer lives, the company chooses the arbitration service or services that can be used, and arbitration can be more expensive than litigating in court.[90] Courts uphold arbitration clauses in which consumers waive their right to participate in class actions in court as well as class-wide arbitration.[91] While these agreements typically require the consumer to use arbitration as the exclusive dispute resolution forum, in many agreements the company has the option of suing in either an arbitration or judicial forum.

Arbitration clauses have been presented as part of both browsewrap agreements and rolling contracts.[92] The courts carefully examine the design and presentation of the arbitration clause, applying the same standards as for other terms in browsewrap and rolling contracts.

Per a provision in Dodd-Frank, the CFPB has conducted studies of consumer arbitration clauses in financial services contracts in order to decide whether to regulate them, but has made no determination as of this writing. [93]

E. The law applicable to software licenses compared with other types of contracts

Software such as mobile apps is an important component in mobile payments. Often it is provided to consumers through licensing agreements that consumers consent to implicitly or explicitly, but the law that applies to these licenses is somewhat ambiguous. (Legal differences between software licenses and other types of contracts are discussed in greater detail in the third stage because they are especially relevant in examining consumer problems after a payment has been made.) Courts hold that UCC Article 2, the basis of most of the law on the sale of goods, applies to software.[94] However, many software transactions also involve services, and the UCC does not apply to the sale of services. When a transaction involves both goods and services, however, courts apply a "predominant purpose" test: If the main reason for the transaction involved goods rather than services, the UCC applies to the transaction.[95] However, even if the UCC applies, many of the key provisions of Article 2 apply only to sales of goods, not licenses.[96] If the transaction is not subject to the UCC, contract law applies unless a specific state law governs licenses.

In regard to consumer acceptance, the courts make no distinction between software licenses and other types of contracts. Therefore, legal differences are not relevant to this aspect of mobile payment transactions.

There are legal differences between software licenses and other types of contracts. But in regard to consumer acceptance, the courts make no distinction between software licenses and other types of contracts. (Legal differences between software licenses and other types of contracts are discussed in greater detail in the third stage because they are especially relevant in examining consumer problems after a payment has been made.)

VII. Add-on services

Companies attract customers by offering goods or services that they want. Once having gained consumers' attention, some firms then try to persuade them to make additional purchases by offering "add-on" products. Courts have found that in order for consumers to purchase the product they want online, some mobile payments providers have forced consumers to maneuver through confusing sites that deceive them into contractual obligations for services they do not want and never realized they were purchasing.[97]

The Federal Trade Commission Act prohibits unfair and deceptive acts and practices. When a seller's conduct in regard to add-on services violates those standards, the FTC, CFPB, and bank regulators have brought enforcement actions to stop that conduct.[98] Based on its experience supervising credit card issuers, the CFPB found that some issuers engaged in deceptive promotional practices and enrolled consumers in programs without their affirmative consent.[99] In certain instances, consumers did not even realize they were enrolled or that they were required to pay extra for the programs. The CFPB has stated that it "will continue to closely review the sale of add-on products by card issuers and their service providers to determine whether additional consumer protections are warranted."[100]

Most states also have enacted consumer protection laws prohibiting unfair and deceptive acts and practices. State attorneys general and other state government agencies can bring enforcement actions to stop this sort of conduct. Those statutes also include a private right of action, enabling consumers to sue. Consequently, consumers may be able to successfully sue companies that engage in unfair or deceptive acts or practices while offering add-on products. However, there is a gap in the law because the UDAP statutes and court decisions in many states significantly restrict consumers' ability to successfully enforce these laws.[101]

VIII. Online modification of original contract terms

Companies often modify their consumer contracts to add new provisions. In particular, banks modify credit card and demand deposit account agreements typically through the addition of an arbitration clause. They also make modifications when new features are added, such as remote deposit capture. This is significant for consumers who make mobile payments using their credit or debit cards.

Courts permit companies to modify their contracts as long as the company provides consumers with proper notice and the opportunity to terminate the contract.[102] The case law is

ambiguous, however, because courts look at the circumstances surrounding each modification. For example, courts examine the presentation and design of the notice to determine if it was sufficient. As a result, courts sometimes have held that the notice was improper when, for instance, the hyperlink to the modification was inconspicuous.[103]

IX. Advertisements for financial services displayed on mobile device screens

Like other commercial enterprises, financial institutions display advertisements for financial services on mobile device screens. The FTC has issued a guidance explaining how companies can present online ads without violating the FTC Act's prohibition of deceptive representations.[104] According to the guidance, "the same consumer protection laws that apply to commercial activities in other media apply … [to] activities in the mobile marketplace." Sometimes to prevent an ad from being misleading, the seller has to disclose limitations and qualifications. That disclosure must be prominent, clear, and conspicuous, close to the claim in the ad, and in understandable language.

Portions of the guidance apply directly to mobile payments. "If a disclosure is too small to send on a mobile device and the text of the disclosure cannot be enlarged, it is not a clear and conspicuous disclosure." The guidance includes examples of disclosures on mobile devices. The guidance also points out that the design of the page on a mobile device may make it unlikely that the consumer will see the disclosure. For example, the small screen may make the disclosure too small to read without zooming in.[105] If the display contains columns and the required disclosure is in the left column rather than the center column, the consumer may not scroll over horizontally to see the disclosure. The guidance recommends that the advertisement be optimized for mobile devices. For example, optimization could be achieved by eliminating columns so the consumer can view required disclosures simply by scrolling vertically.

X. Phishing scams

Phishing involves attempting to deceive consumers into believing that an impostor website is really that of a legitimate company. This can result in unauthorized transfers of the consumer's funds, unauthorized credit card charges, security breaches, and privacy invasions.

It is unlikely that most consumers would be able to identify and successfully sue the perpetrator of a phishing scam. However, credit card and debit card law provide some protection by limiting the consumer's liability. This protection is explained in the Stage 3 part of this report.

The FTC has successfully sued companies to stop phishing. In one case, the FTC brought an enforcement action against a notorious rogue Internet service provider alleging unfair practices for, among other things, hosting phishing websites. The court issued an injunction and asset freeze, shutting down the company.[106]

XI. Conclusion

Stage 1 focuses on the circumstances under which consumers enter into contracts for mobile services. A lack of transparency at this stage can have a significant impact on consumers. It is vital that consumers understand when their browsing on a seller's website and clicking on various boxes and buttons constitutes an agreement to be bound to terms they may not be aware of but are on other pages of the website. Likewise, they need to know that, in addition to the terms and conditions on the website, they may be subject to additional terms later on. The ambiguity of the law governing these browsewrap and rolling contracts is a serious problem when it results in unexpected consumer obligations and restrictions. An example is a contract that requires consumers to bring all disputes to arbitration instead of courts.

The most important gap in the law at this stage is the lack of law requiring disclosure of terms and conditions when consumers use prepaid cards to fund their mobile payments. Prepaid cards are increasingly popular, and consumers need transparency. The failure of prepaid card issuers to provide clear and conspicuous disclosure of important rights and responsibilities can have a negative impact on consumers who find the cards do not have the features and protections they expect, based on their experience with credit and debit cards. The CFPB is working on final rules requiring prepaid card disclosures. In the meantime, many consumers will be spending a great deal of money buying cards whose terms may not be at all transparent. Moreover, until final rules are issued, it is unknown whether the CFPB will require disclosures that ensure sufficient transparency.

Stage 2: Use of mobile device to make payments

I. Introduction

This portion of the report describes the regulatory framework that applies when consumers use their mobile devices to make payments. It describes the legal issues that apply to consumers when they use credit, debit, and prepaid cards to make mobile payments. Payments charged to accounts with wireless carriers are also considered. The legal rights of consumers who make mistakes, such as typing a wrong number, and of parents whose children agree to pay for products without parental permission are examined. Mobile payments involve many parties, including nonbanks, payment processors, sellers of virtual currency, and third-party service providers, and the report explores applicable law affecting these entities.

There are many gaps in the laws that apply when consumers make mobile payments. Some of these gaps reflect the failure of the law and other rules to keep pace with new technology and products. For example, the EFTA requires financial institutions to make many disclosures and permits them to be sent electronically. But the statute does not provide any guidance on what courts should do when the institution alleges it sent an electronic disclosure but the consumer denies receiving it. The Electronic Payments Association, which represents more than 10,000 financial institutions, develops rules for the Automated Clearing House network (ACH), known as the NACHA Operating Rules.[107] These rules mandate that financial institutions maintain fraud transaction detection systems, but the rules do not apply to transactions made by text message. Reg. E apparently provides that mobile payments made via cellphone do not have to comply with receipt requirements, but mobile payments made using a wearable mobile device, such as a watch, arguably are not treated the same. Until proposed prepaid card rules are adopted, a huge regulation gap will persist.

In addition, nonbanks such as Google Wallet and Apple Pay are actively involved in mobile payments. For the most part, they are subject only to state money transmitter laws, which provide little protection for consumers. If a consumer makes a mistake, such as a typing error that results in transferring the wrong amount or sending a mobile payment to the wrong account, the Uniform Electronic Transactions Act provides limited relief by allowing the consumer to avoid liability under a narrow set of circumstances. But the law does not require notice to consumers of the ability to correct a mistake, so few are likely to be aware of it. Virtual currency such as bitcoin is used to make some mobile payments. Consumers face many risks when using virtual currency, but there is almost no law to protect them. Finally, a denial of service attack, in which hackers block online access to a company, may substantially impede a

consumer's ability to make timely mobile payments. No law directly addresses how these attacks may harm consumers.

In addition to gaps in the law, the law is ambiguous in some respects. For instance, it is not clear whether consumers have some of TILA's protections, such as chargeback rights, when they have a dispute with a merchant, make a mobile payment, or permit a nonbank payment provider to charge their credit card account.

II. Mobile payment by credit card

When consumers use a mobile device and charge the purchase to their credit card accounts, generally the TILA and Reg. Z apply, as they do to all credit card transactions. Special considerations related to mobile payments are noted below.

TILA and Reg. Z require certain disclosures to consumers who make payments using their credit card account. The first set of disclosures is called the "account opening disclosures."[108] The creditor must make these disclosures before the consumer engages in the first transaction charged to the credit card account. The disclosures include information the consumer needs to use the account and how to avoid charges. TILA requires creditors to make seven account opening disclosures available to the extent they are applicable.[109] These include when a finance charge may be imposed, how the amount is determined, the periodic rate, other charges, and error procedures such as billing error rights and the right to assert claims and defenses.

TILA permits creditors to make account opening disclosures electronically, but the creditor must comply with the consumer consent requirements of the E-Sign Act.[110] Reg. Z's formatting requirements may present a challenge for creditors wanting to make the disclosures on the small screen of a mobile device. These include requiring 10-point type, grouping together certain disclosures on periodic statements, and providing others in tabular format.[111] TILA, Reg. Z, and the E-Sign Act do not provide any guidance on how courts and agencies should deal with a situation in which the institution proves it sent disclosures electronically but the consumer denies receiving them and the institution cannot prove the consumer received them. [112]

TILA and Reg. Z, in effect, incorporate authentication requirements by holding that a consumer is not liable for unauthorized use of a credit card unless the issuer provides "a means to identify the cardholder on the account or the authorized user of the card."[113] The official staff interpretations provide guidance relevant to mobile payments. The means to identify can include, "for example, a signature, photograph, or fingerprint on the card *or other electronic or*

mechanical confirmation."[114] A magnetic stripe or other device not readable without physical aids does not satisfy this requirement unless the stripe is used in conjunction with a "secret code or the like."[115] The consumer's PIN is an example of a secret code.

Yet when the consumer uses a mobile device to pay, the credit card is not presented to the merchant. The official CFPB staff interpretations deal with this situation in addressing transactions over the phone and on the Internet. "For example, when merchandise is ordered … [over] the Internet by a person without authority to do so, using a credit card account number by itself or with other information that appears on the card (for example, the card's expiration date and three- or four-digit cardholder identification number), no liability may be imposed on the cardholder."[116] But unless the card issuer discovers the charge is unauthorized, it will appear on the consumer's periodic statement. To have it removed, the consumer will have to discover the unauthorized charge and notify the card issuer. TILA and Reg. Z provide withholding and billing error procedures the consumer can follow.[117]

Mobile payments include another party in addition to the card issuer and cardholder, and another step in the process of enabling the consumer to make mobile payments. When a consumer wants to add a credit card account to a mobile payment service, the service engages in a verification procedure with the card issuer. For example, Apple Pay sends personal information about the consumer to the card issuer.[118] The card issuer then decides whether it will approve the consumer using that credit card account to participate in Apple Pay. The law regulating credit card transactions was drafted long before mobile payments. Consequently, it does not address the mobile payment services' verification procedures. This may present a problem for parties to mobile payment transactions. Recently, a payments expert asserted that banks use inadequate verification procedures and that wrongdoers have exploited this flaw to engage in fraudulent transactions.[119]

If the consumer receives an electronic receipt at the point of sale, the Fair Credit Reporting Act prohibits printing more than the last five digits of the card number or the card's expiration date.[120] This provision likely will not apply to most mobile payment transactions. Typically, when a consumer uses a mobile device to pay for goods and services, the merchant sends a receipt via email or text message. Most courts have held that the Fair Credit Reporting Act provision applies only to receipts printed on paper using point-of-sale devices such as electronic cash registers.[121] However, not all courts agree. Several have held that the provision applies to an electronic medium as well. They have ruled that a receipt displayed on a consumer's computer screen qualifies as an electronic receipt.[122]

TILA and Reg. Z also require certain disclosures on consumers' periodic statements, including important information such as the finance charge, when payment is due, and the address for registering a dispute.[123] These disclosures can be made electronically.[124] The Credit Card Accountability, Responsibility and Disclosures Act of 2009 requires additional disclosures.[125] The CFPB has expressed a concern that applies to mobile payments. "Consumers who pay their credit card bills electronically may not access their monthly statement and instead may use online portals which are not required to contain these disclosures."[126] If consumers do not access their monthly statements because they use online portals, they will not have the information they need to make informed decisions about how much to pay each month and how to take advantage of the law's error resolution procedures. The CARD Act requires that the periodic statement be mailed or delivered 21 days before payment is due.[127] The CARD Act also contains several substantive protections. For example, it requires prompt crediting of consumer payments. It also says payment requirements must be reasonable and the cutoff time for payment cannot be before 5 p.m. on the due date.[128] There are limits on fees related to the consumer's method of payment and the order in which payments are allocated.[129] Finally, there are limits on the fees charged for subprime credit cards.[130]

Creditors also must make three types of subsequent disclosures. One is a statement of the consumer's billing error rights.[131] The creditor can make this either annually or in a summary form if it is included with each periodic statement. Second, creditors must disclose additional credit features or devices.[132] Examples of additional credit features are adding an overdraft feature to a checking account or a cash advance to a credit card account. An example of an additional device is adding blank checks. Third, creditors must disclose changes in terms. The CARD Act requires the creditor to provide 45 days' notice for increases in the annual percentage rate and any other significant changes.[133] If any changes in the credit card account terms or imposition of a penalty rate are included in or accompanying the periodic statement, creditors are required to include a summary of the changes on the front of the periodic statement.[134]

Obviously, TILA imposes a great many requirements. Most, however, are requirements for creditors to make disclosures rather than to provide substantive protections to consumers. Perhaps most importantly, TILA contains no restrictions on the amount of the finance charge and resulting annual percentage rate. These are determined by state law, including usury statutes. Some states have allowed either very high rates or none at all.[135] The Supreme Court has made interest rate regulation even more complicated by favoring some states' laws over others. The court held that a credit card issuer can "export" the rate of the issuer's "home" state, imposing that rate on consumers in other states regardless of limits the consumers' states may have established.[136]

The TILA and Reg. Z disclosure and substantive protection provisions may be increasingly important in the mobile payments environment, especially provisions relevant to consumers who are granted subprime credit. Industry participants have said they intend to target unbanked and underbanked consumers for mobile financial services.[137]

III. Mobile payment by debit card

When consumers use a mobile device and charge the purchase to their debit card accounts, generally the EFTA and Reg. E apply, as they do to all debit card transactions. Reg. E defines an electronic fund transfer as "any transfer of funds that is initiated through an electronic terminal, telephone, [or] computer … for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer's account. The term includes, but is not limited to: … (iv) transfers initiated by telephone; and (v) transfers resulting from debit card transactions, whether or not initiated through an electronic terminal."[138]

However, certain telephone-initiated transfers are excluded from coverage. These are defined as:

> Any transfer of funds that:
>
> (i) Is initiated by a telephone communication between a consumer and a financial institution making the transfer; and
>
> (ii) Does not take place under a telephone bill payment or other written plan in which periodic or recurring transfers are contemplated.[139]

The typical mobile payment transaction would not come under the exclusion because the transfer of funds is not initiated by a phone communication, which appears to refer to a phone call to the institution.[140] "A telephone call does not involve an access device within the scope of the EFTA. However, a transfer initiated using a mobile phone in some other capacity, other than one involving a telephone call, does involve an access device."[141]

Special considerations related to mobile payments are noted below.

Under Reg. E, disclosures must be "clear and readily understandable, in writing, and in a form the consumer may keep. … The disclosures … may be provided to the consumer in electronic form," subject to compliance with E-Sign.[142] Unlike TILA and Reg. Z, "no particular rules govern type size, number of pages, or the relative conspicuousness of various terms."[143]

The EFTA and Reg. E require certain disclosures when consumers make payments using their debit card accounts. A set of initial disclosures must be made "at the time a consumer contracts for an electronic fund transfer service or before the first electronic transfer is made involving the consumer's account."[144] The disclosures must include the following, as applicable: consumer liability for unauthorized transfers; the telephone number and address of the person consumers can contact if they believe there has been an unauthorized transfer; the types of electronic fund transfer the consumer may make; fees; the right to documentation; the right to stop payment of preauthorized electronic fund transfers; and the institution's error resolution procedures.[145] In addition, the institution must disclose any limits on the frequency and amount of transfers. Finally, the institution must explain its liability for failure to make transfers and stop payment of preauthorized transfers when properly instructed to do so by the consumer.

The financial institution also must provide subsequent disclosure of changes to terms or conditions if the change would result in increased fees or consumer liability, fewer types of electronic fund transfers, or stricter limitations on the frequency or amount of electronic fund transfers.[146]

The EFTA requires financial institutions to mail or deliver periodic notices of the law's error resolution procedures.[147] The institution can either provide an annual notice or include an abbreviated notice with each periodic statement.

If a consumer has engaged in any electronic fund transfer during a monthly cycle, the institution must provide a periodic statement.[148] If there are no electronic fund transfers, the institution nevertheless must send a statement at least quarterly. The statement must include transaction information, the account number, fees, account balances, an address and phone number for inquiries, and a phone number for preauthorized transfers.[149]

Reg. E permits creditors to make disclosures electronically, but the creditor must comply with the consumer consent requirements of the E-Sign Act.[150] As is true with TILA and Reg. Z, which apply when the consumer uses a credit card, there is a gap in the law regarding electronic disclosures. The EFTA, Reg. E, the E-Sign Act, and case law do not provide any guidance on how courts and agencies should deal with a situation in which the institution proves it sent disclosures electronically but the consumer denies receiving them and the institution cannot prove the consumer received them.[151]

Financial institutions making debit card account transfers processed by an automated clearinghouse subject to the operating rules of the Electronic Payments Association (the NACHA

rules) must comply with those rules. Under the rules, documents that must be signed or similarly authenticated may be signed with an electronic signature that complies with E-Sign. In addition, if a state has enacted the Uniform Electronic Transactions Act, the institution must comply with that law to the extent it is not pre-empted by E-Sign.[152] The NACHA rules provide that an electronic signature must be made "in a manner that evidences the identity of the Person who signed and that Person's assent to the terms of the Record."[153] Upon request, an institution must provide a copy of transfers made by the consumer.[154] Information that is required by the rules "to be in writing may be created or retained in an Electronic form that (a) accurately reflects the information in the Record, and (b) is capable of being accurately reproduced for later reference."[155]

Reg. E does not include any authorization requirements for one-time electronic transfers over the Internet. However, the NACHA rules do contain authorization requirements, and these apply to transfers over the Web, including debits made through wireless networks.[156] Transfers made through wireless networks are subject to the same rules as all transfers made via a Web browser. As a result, a company has to comply with the fraudulent transaction detection system mandated by those rules and must verify the identity of the consumer and the validity of routing numbers. However, there is a gap in the rules because the scope of the rule is somewhat narrow: It does not apply to transactions that are not made through a Web browser, such as a transaction made using a text messaging system.[157] In addition, the rules state that they are not intended to give any legal or equitable right, remedy, or claim to individuals sending or receiving payments through the ACH system.[158]

Generally, the EFTA and Reg. E require financial institutions to provide consumers with receipts when the consumer initiates an electronic fund transfer at an "electronic terminal."[159] "Electronic terminal" is defined to include point-of-sale terminals, ATMs, and cash dispensing machines but exclude "a telephone operated by a consumer."[160] Unfortunately, there is an ambiguity in the law because it does not specify how wearable devices fit into this scheme. Arguably, a mobile payment initiated by the consumer via a wearable such as a watch would not be excluded since a wearable is not a telephone. If that view prevailed, institutions would be required to provide a receipt if the consumer made a mobile payment using a wearable but not if the consumer used a smartphone. It would be unwise for courts and regulators to treat wearables and smartphones differently since they have comparable mobile payment capabilities. Applying different legal requirements unduly complicates marketing these products. Furthermore, it would confuse consumers since they will reasonably expect the law to apply the same provisions to smartphones and wearables when they make mobile payments. To prevent any confusion, the CFPB could implement a new rule or guidance to make it clear that the receipt requirement exclusion applies to wearables. In fact, the official interpretation

already states that the exclusion applies to "a transfer by means analogous in function to a telephone, such as by home banking equipment or a facsimile machine."[161]

The provisions on receipts have caused confusion among those in the mobile payments industry. Assuming receipts must be provided, industry representatives have asked the CFPB whether they can make receipts available through mobile or electronic mail rather than only through paper receipts. The CFPB has said it is considering this issue.[162]

As discussed above in regard to mobile payments charged to a credit card account, if the consumer receives an electronic receipt at the point of sale, the Fair Credit Reporting Act prohibits printing more than the last five digits of the debit or credit card number or the card's expiration date.[163] Courts disagree as to whether this provision applies only to receipts printed on paper, or whether it also applies to electronic receipts.[164]

IV. Mobile payment by prepaid accounts and cards

Many companies permit consumers to establish prepaid accounts from which to make mobile payments.[165] They may be explicitly labeled prepaid accounts and subject to whatever contract terms the consumer agrees to. Alternatively, they may operate as prepaid accounts even if they are not called as such by the company offering the service. Arguably, a consumer transferring funds to PayPal is establishing a prepaid account, whether or not PayPal calls it that.[166]

Federal law does not currently regulate prepaid accounts and prepaid cards, though the CFPB has proposed a rule to do so. As explained in the Stage 1 portion of this report, a mobile device that stores funds would be subject to the proposed rule but a device that stores merely credentials would not.[167]

If the CFPB issues a final rule that includes the provisions of its proposed prepaid rule, consumers who register their prepaid accounts to make mobile payments would gain the right to Reg. E's error resolution procedure and its limits on liability for unauthorized use.

In addition, consumers would have the protections of the CARD Act when they use the credit features that mobile payment services may offer as part of their prepaid accounts.[168] These include requiring the financial institution to consider the consumer's ability to repay, imposing limits on first-year fees and late fees, requiring the institution to mail or deliver statements at least 21 days before the payment due date disclosed on the statement, and providing advance notice of increases in the interest rate.

V. Regulation of nonbanks

The CFPB defines a "nonbank" as "a company that offers consumer financial products or services, but does not have a bank, thrift, or credit union charter and does not take deposits."[169] Some companies that process mobile payments offer limited financial services and therefore are not regulated as banks. PayPal is an example of that type of "nonbank" payment provider. It processes transactions that are paid through a consumer's credit card, debit card, or prepaid account.[170] Consumers may lose rights that they otherwise would have when making payments using funds held by these nonbanks.

For example, in the typical credit card transaction where a credit card is loaded onto a mobile phone, consumers use their mobile devices to pay for goods by charging their credit card account. If the consumer has a dispute with the merchant, the consumer can take advantage of TILA's chargeback rights and withhold payment. There is a gap in the law, however, in which the consumer uses the mobile device but allows one of these nonbank payment providers to charge the credit card account. In that situation, it is uncertain whether the consumer is covered by TILA.[171] This is because TILA and Reg. Z were written long before these nonbank payment providers existed, and the law has not been updated to take them into account.

Instead of using their credit card account, consumers may pay for goods using a debit card account that accesses funds held in a checking account at a bank. In the typical transaction, the consumer has the benefit of the protections afforded by the EFTA and Reg. E, including caps on unauthorized transfers and a required error resolution procedure. However, there is a gap in the law when the consumer uses a nonbank payment provider; it is not clear whether the protections cover that transaction.[172] Finally, if the consumer pays for goods using a prepaid account that is processed by a nonbank payment provider, no current law would apply to protect that consumer.

Nonbank payment providers are subject to federal law such as the Bank Secrecy Act and its anti-money laundering provisions. But there are major gaps in that law because it does not contain consumer protections, such as those found in the EFTA. Nonbanks offering consumer financial services and products also are subject to regulation and enforcement by the CFPB.[173] These nonbanks also are subject to state money transmitter laws.[174] At least one state, California, has updated its money transmitter laws to include mobile payments.[175] The laws of other states include electronic transmissions that are defined broadly enough to likely include mobile payments.[176] However, most of these state money transmitter laws have substantial

gaps because they do not contain significant consumer protections such as required disclosures and error resolution procedures. Instead, they require the nonbank to obtain a state license and post a surety bond. Regulators have the authority to examine the books and records of the companies. Most states also require the companies to hold specific types of investments against at least a portion of outstanding debts. However, these laws provide inadequate protection against a company's insolvency or wrongdoing. It is often difficult for consumers to recover their funds when problems arise.[177] Montana, New Mexico, and South Carolina, do not impose even minimal requirements on money transmitters.[178]

VI. Regulation of payments charged to accounts with wireless carriers

Instead of paying for their purchases through credit card, debit card, or prepaid accounts, many consumers use text messaging services to have their obligations included on their wireless carrier bills. Wireless carriers are regulated by the Federal Communications Commission. The FCC has imposed truth-in-billing requirements upon these carriers to ensure that a consumer's bill contains necessary information in a fashion that consumers can understand.[179]

Thousands of consumers have discovered unauthorized charges on their wireless carrier bills. These charges do not relate to the communications services provided by the wireless carrier but, rather, are obligations claimed by other companies such as telemarketers. This deceptive practice, known as "cramming," in which consumers say that they have been billed by companies they never heard of or that they were contacted by the companies but never agreed to purchase anything from them, is a frequent subject of complaint and legal action.[180] When the FCC was considering what to do about cramming, the FTC urged it to issue strong rules to protect consumers against unauthorized charges on cellphone as well as landline bills.[181]

In 2012, the FCC issued cramming regulations, but they did not cover unauthorized charges on cellphone bills. Instead of developing cellphone regulations, the FCC has brought enforcement actions against T-Mobile, AT&T Mobility, and others, alleging that they permitted cramming by third parties on cellphone bills.[182] The CFPB, in conjunction with state attorneys general and the FCC, brought enforcement actions against Sprint and Verizon for allowing third parties to illegally charge consumers, automatically billing consumers for illegitimate charges without their consent, ignoring consumer complaints about unauthorized charges, and disregarding red flags about third-party vendors.[183] The FTC has also brought several enforcement actions against companies accused of cramming under its authority to prohibit unfair and deceptive acts and practices. These actions are discussed in the Stage 3 portion of this report.[184]

VII. Authentication

Mobile payment systems need strong authentication procedures to ensure that the person engaging in a transaction that may result in access to information about a customer and a charge to the customer's account is in fact an authorized customer. Stakeholders have commented to the FTC on methods to achieve better authentication of mobile payments.[185] Nevertheless, the FCC has yet to impose authentication standards on wireless carriers.[186]

In contrast, regulators have at least recommended, but not required, authentication procedures for financial institutions. In 2005, the Federal Financial Institutions Examination Council (FFIEC) issued a guidance that informs regulated financial institutions of the regulators' supervisory expectations in regard to the institutions' authentication procedures when they provide services in an Internet banking environment.[187] The guidance provides that the institutions should use effective methods to authenticate the identity of customers using Internet-based products and services. It warns that single-factor authentication methodologies that require a username and password before granting access may not offer sufficient protection. It regards such authentication as inadequate for high-risk transactions involving access to customer information or the movement of funds to other parties. It warns that single-factor authentication is often exploited and results in account fraud and identity theft. In addition, it cautions financial institutions that inadequate authentication leading to unauthorized transactions can result in electronic agreements and transactions that are not legally enforceable.[188] The guidance does not suggest any particular technology or methodology for authentication, but it lists several that are available, including biometrics, one-time passwords, and PINs. It does state that federal financial regulators expect institutions to engage in risk assessments and consumer education about online theft of assets and information.

In 2011, the FFIEC issued a supplement to that guidance in which it characterized Internet banking as "an increasingly hostile online environment."[189] The guidance informed institutions they were expected to upgrade their controls for high-risk online transactions through yearly risk assessments, layered security controls for consumer accounts, and more active consumer awareness and education efforts. Layered security controls should include processes to detect and respond to suspicious or anomalous activity.[190] Finally, the FFIEC determined that certain types of device identification and challenge questions should no longer be considered effective controls and should be replaced by more sophisticated measures.[191] These upgrades and other changes are undoubtedly expensive. In addition, as institutions build new security barriers to implement the recommendations in the guidance, fraudsters will likely discover ways to breach them.[192]

VIII. Consumer mistakes

When consumers engage in transactions involving mobile payments, they could make a typo or another kind of mistake. To deal with this situation, most states have adopted the Uniform Electronic Transactions Act.[193] Under this law, the consumer has the right to "avoid the effect of an electronic record that resulted from an error … if the electronic agent did not provide an opportunity for the prevention or correction of the error." An explanation of this awkward language is necessary to understand its meaning. The "record that resulted from an error" is information the company has stored that reflects its transaction with the consumer and information that includes the consumer's error. Under certain circumstances, the consumer can "avoid the effect" of this information. The "effect" of the record is that the consumer is liable for the transaction, including the erroneous information. To "avoid the effect" means the consumer can prevent being held liable for the transaction to the extent it includes the erroneous information.

Consumers are not liable for the error as long as they promptly notify the company of the error and take reasonable steps to conform to the company's reasonable instructions. An electronic agent is a computer program or other automated means that the company uses to interact with the consumer during an electronic transaction. The consumer loses the ability to escape liability if the company, through its electronic agent, provides the consumer an opportunity to prevent or correct the error but the consumer fails to take advantage of that opportunity.

In adopting a comment to this provision, the Uniform Law Commission, the sponsor of this law, explains that the company can give the consumer an opportunity to correct the error by providing a confirmation screen. For example, assume the consumer mistakenly types "$1000" instead of "$100." The electronic agent displays a screen that shows what the consumer typed and asks the consumer to confirm the information on the screen. The consumer confirms the information and continues onto subsequent screens to complete the transaction. Under those circumstances—that is, having had the opportunity to correct or prevent the error by refusing to continue with the transaction, but going ahead anyway—the consumer would be liable for $1,000.

However, this provision has serious gaps because the company is not required to notify consumers of their right to correct errors, so consumers are unlikely to be aware that they can do so. In addition, the statute contains no explicit right to sue a company that fails to comply

with its requirements even though the consumer has fully satisfied the requirements of the statute.[194]

IX. Virtual currency

Virtual currency such as bitcoin is increasingly popular for those making mobile payments.[195] A growing number of merchants are accepting payment with virtual currency. It is touted as offering advantages to the unbanked and underbanked.[196] A comprehensive examination of laws relevant to virtual currency is beyond the scope of this report, but a brief summary of major issues and recent developments follows.

There are many major gaps in the laws applicable to virtual currency, which is not legal tender.[197] Therefore, unlike money issued by the United States Treasury, when a consumer tenders payment in virtual currency, the merchant is not obligated to accept it, and tender does not discharge the consumer's obligation.[198] Its value is extremely volatile; the value of bitcoins rises and falls substantially within short periods of time.

The Internal Revenue Service issued a guidance stating that because virtual currency is not legal tender, the IRS will treat it as property, not currency.[199] Therefore, it is subject to the same reporting requirements as any other payment made in property, including treating exchanges as capital gains or losses. FDIC insurance does not protect virtual currency the consumer has stored with an exchange.[200] Virtual currency also is not subject to requirements under the Gramm-Leach-Bliley Financial Services Modernization Act of 1999 to ensure the security of funds deposited with banks or that law's data breach notification requirements. According to Federal Reserve Board Chair Janet Yellen, the Fed "does not have authority to supervise or regulate bitcoin in any way." Because of the substantial risks associated with virtual currencies, the CFPB has issued a consumer advisory warning about the risks of bitcoin.[201] The Financial Crimes Enforcement Network, a unit of the U.S. Treasury, has issued an advisory guidance for administrators and exchanges.[202] It treats virtual currencies as money transmitters and subjects them to Bank Secrecy Act regulations. The Justice and Treasury departments have exercised their authority to apply money-laundering and registration rules.[203]

There also has been action on the state level. The New York Department of Financial Services has issued regulations governing virtual currency companies operating in New York or doing business with New York residents.[204] The Texas banking commissioner has issued regulatory guidelines for ATMs that provide virtual currency. California, Connecticut, Indiana, Nevada, and New Mexico have issued statements or guidance regarding virtual currency.[205] The Conference

of State Bank Supervisors has published a Draft Model Regulatory Framework. State law is unclear as to the rights of a deceased consumer's estate when it tries to recover digital assets, including virtual currency. To clarify the law, a Uniform Fiduciary Access to Digital Assets Act has been proposed by the Uniform Law Commission for enactment by each state.[206]

X. Children making online payments without parental consent

The Children's Online Privacy Protection Act of 1998 and accompanying FTC regulations are an attempt to counter the conduct of sellers who use websites targeting children in order to obtain personal information from them.[207] The law was amended in 2013 to include smartphones and tablets. The personal information covered by the law includes location data, photographs, and videos. The information collected by sellers can be used for a variety of purposes, including charging a parent's credit or debit card account for purchases made by the child. Before collecting information from a child under the age of 13, website operators must obtain "verifiable consent" from a parent. The operator must send a notice telling the parent that it wants to collect information from the child and that the parent's consent is required. The operator must make reasonable efforts in light of currently available technology to ensure that the child's parent has actually been notified and has given consent. The website targeted at children must post a link to a privacy notice on the home page of the website and on each page from which it collects personal information from children. Parents must be given a way to review any personal information collected from a child. Private individuals have no right of action to sue for violation of this law. Enforcement is left to the FTC and state attorneys general.

XI. Denial of service attacks

One of the benefits of mobile payment services such as paying bills online is the consumer's prompt access to funds in the account. But increasingly, banks are subject to what are known as distributed denial of service attacks in which the banks' online access is blocked for an extended period of time. Consequently, consumers who wait until late on the day a payment is due to make the payment online may not be able to do so if their bank's online access is under attack and it is too late to make other arrangements. Their delay in paying may result in consequences such as late payment fees, repossession, eviction, foreclosure, or adverse credit reports. Denial of service attacks have targeted both bank Web pages and bank apps. Fraudsters also use denial of service attacks to distract bank staff while they access customers' accounts.[208] Customers may find they cannot make mobile payments because the funds in their accounts have been stolen in connection with a denial of service attack.

There is a total gap in the law related to denial of service attacks. No statutes or regulations specifically address this type of attack. However, an alert from the Office of the Comptroller of the Currency (OCC) recommends that the national banks under its authority provide timely and accurate information to customers about the risk of denial of service attacks, problems they may encounter, precautions they can take, and alternative delivery channels.[209] The OCC also describes several risk management programs and procedures banks should adopt.

Consumers whose banks are subject to a denial of service attack may not be able to use their mobile devices to make a payment from their demand deposit account when it is due, resulting in fees and other consequences. A late payment also may result in damaging information on the consumer's credit report and a lower credit score. The EFTA provides: "If a system malfunction prevents the effectuation of an electronic fund transfer initiated by a consumer to another person, and such other person has agreed to accept payment by such means, the consumer's obligation to the other person shall be suspended."[210] The suspension continues "until the malfunction is corrected and the electronic fund transfer may be completed." However, if the person or business the consumer is trying to pay makes a written request demanding payment by a means other than electronic fund transfer, the suspension ends and the consumer must make the payment some other way. Suspension of the consumer's obligation under the EFTA could provide substantial protection to consumers. However, a gap in the law substantially undermines this protection. Since companies are not required to disclose to consumers that they have this right, few consumers are likely to take advantage of it.[211]

XII. Natural disasters

Consumers are unable to take advantage of mobile online payment services when natural disasters destroy the electronic infrastructure, as happened with Hurricane Katrina and Superstorm Sandy.[212] Consequently, it may be impossible for consumers to make payments on time, causing the same problems that result from a denial of service attack. The difference is that the disruption of electronic services due to a natural disaster may last far longer than the typical denial of service attack.

As described above in the section on denial of service attacks, the EFTA provides some relief.

XIII. Payment processors

Some sellers accepting mobile payments use third-party payment processors. However, some processors facilitate payments made to sellers suspected of engaging in fraudulent transactions. The FDIC has issued a guidance on payment processor relationships.[213] Under the guidance, a financial institution must manage payment processor and merchant relationships or be held liable for their unlawful activity. Of particular concern to the FDIC are telemarketers and online merchants who may engage in activities that should alert processors to possible illegal conduct. Specific activities include the use of multiple financial institutions, many consumer complaints, and many returns or chargebacks. The FDIC guidance urged financial institutions to conduct due diligence before establishing a relationship and to engage in continual monitoring. The OCC has provided similar advice and warnings to financial institutions under its authority, and the CFPB has brought enforcement actions against payment processors.[214]

XIV. Third-party service providers

Companies offering mobile financial services often use other companies, known as third-party service providers, to provide many of the components of those services.[215] The CFPB has issued a bulletin for both banks and nonbanks.[216] The guidance alerts financial institutions that the providers with which they work are subject to the CFPB's supervisory and enforcement authority, which includes both specific consumer laws and the prohibition of unfair, deceptive, and abusive acts and practices. Furthermore, a financial institution may be liable for the actions of its providers when they violate those laws. The CFPB requires the institution to have a process to manage risks. This includes a due diligence responsibility for its providers. The institution must review policies and procedures of the providers to ensure compliance. Finally, the institution should engage in ongoing monitoring of its providers. The OCC, FFIEC, FDIC, and the Fed have also issued guidance on third-party service providers.[217] The guidance published by those agencies is similar to that of the CFPB.

XV. Conclusion

Stage 2 examines issues related to consumers' use of mobile devices to make payments. There are gaps in the law in three areas that pose the greatest risks to consumers. The absence of any federal law regulating prepaid cards may make mobile payments funded by such cards unsafe. Until the CFPB issues a final rule governing those cards and that rule takes effect, consumers lack important rights such as a limit on liability for unauthorized use of the cards. And unless the final rule provides substantial protection, consumers will still be at risk.

In addition, there is no comprehensive federal or state consumer protection law regulating nonbanks, such as PayPal. Because nonbanks are important participants in the mobile payment marketplace, this gap in the law may have a substantial impact on consumers.

Lastly, no federal or state law protects consumers from serious potential risk when using virtual currency like bitcoin. Such currency operates outside the boundaries that provide a safety net for traditional currency. Using virtual currency to pay obligations does not necessarily discharge the consumer's debt, those operating the market are not supervised by the government, and FDIC insurance does not protect the consumer's funds from the insolvency of entities holding the funds.

Stage 3: Consumer problems after payment is made

I. Introduction

This section of the report describes and analyzes the law applicable to problems consumers may experience after they make mobile payments. Included are consumers' ability to stop and revoke authorization of electronic payments, legal restrictions on overdraft fees, the risks consumers take when they use remote deposit capture (by sending a picture of a check via a computer or mobile device, instead of depositing it in person), and the dangers of security breaches and privacy invasions. The report discusses the need for laws enabling consumers to disable lost or stolen phones. Mobile payments are discussed in the context of unauthorized charges to consumers' accounts with wireless carriers as well as unauthorized charges made by children without parental permission. The report also briefly considers consumer rights when a party to a mobile payment transaction becomes insolvent, as well as the imposition of mandatory arbitration requirements and restrictions on class actions.

In many respects, because of substantial gaps in the law, it fails to protect consumers when they have problems after making mobile payments. If all else fails, consumers can stop unauthorized electronic transfers out of their bank accounts by closing their accounts. But gaps in the law make closing an account difficult even when the bank does not have a legitimate reason for doing so. Excessive overdraft fees can drain consumers' bank accounts, resulting in a negative balance so there is no money left to make mobile payments. Although a recent law provides safeguards, it is limited in scope. Consumers can deposit checks using their smartphones, but gaps in the law leave several questions unanswered, such as when the deposited funds become available to the depositor, what protections depositors have if they deposit funds from a prepaid card, and who bears the loss if the depositor's phone takes a blurred picture of the check. Security breaches and privacy invasions are major consumer concerns, but there is no comprehensive federal or state law to protect consumers. What law exists is limited. Only California and Minnesota have enacted laws requiring smartphones to permit consumers to disable them if they are lost or stolen; there is no federal statute. If a bank fails, deposit insurance protects funds that consumers placed on prepaid cards only under certain circumstances. If a nonbank seller of prepaid cards fails, state insolvency and federal bankruptcy laws promise little if any relief for those who bought the cards.

There also is ambiguity in some of the applicable laws. 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 a one-time mobile payment from the consumer's debit card account. There is uncertainty over how the Uniform Commercial Code may apply to remote deposit capture in regard to the electronic presentment of the digitized check to the bank on which the check is drawn. The Bankruptcy Code provides a procedure intended to protect private consumer information held by a bankrupt company, but its vague language may frustrate that goal.

There also is overlap in the jurisdiction of some agencies. For example, both the FTC and FCC have authority to take action against companies that cause unauthorized charges to be put on consumers' wireless carrier bills. In addition, there is overlap between federal breach notification law and state law.

II. Consumers' ability to stop electronic payments

Consumers using mobile payment services authorize companies to withdraw funds from their accounts to pay for goods and services. This may be a one-time authorization or an

authorization to withdraw funds on a periodic basis until the debt is paid. But problems and conflicts can arise: Some businesses falsely claim they have authorization to withdraw funds electronically from the consumers' accounts. Sometimes consumers give their authorization but then wish to revoke that authority. The goods may have never been delivered or their quality was not as promised. The services may not have been fully performed. Consumers may believe the debt was paid in full, yet the withdrawals continue. Sometimes consumers lose their jobs or for whatever reason can no longer afford to make payments.

Several specific definitional differences exist in current regulation of electronic payments and help to clarify the significance of the gaps, overlaps, and redundancies that affect mobile payment consumers. One is the distinction between authorized and unauthorized electronic fund transfers. Reg. E defines an unauthorized electronic fund transfer as "an electronic fund transfer from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit."[218] By using the term "actual authority," Reg. E ties the definition to the law of agency that covers the relationship between an individual and a person (or agent) acting on his or her behalf.[219] In contrast to the definition of unauthorized electronic fund transfers, neither the EFTA nor Reg. E defines an "authorized" electronic fund transfer.[220]

A second distinction is between authorization of one-time payments and authorization of multiple preauthorized payments. "'Preauthorized electronic fund transfer' means an electronic fund transfer authorized in advance to recur at substantially regular intervals."[221] An entire provision in Reg. E is devoted to preauthorized payments, including a section on the consumer's right to stop payment of these types of transfers.[222] Neither one-time payments nor preauthorized payments that do not come within Reg. E's definition are specifically mentioned as distinct categories. An example of the latter is a preauthorized payment that does not recur at substantially regular intervals. As a result of this gap, it is not clear that consumers have a right to stop payment of these transfers.

Another distinction is between an effort to stop payment and to revoke payment authority. A consumer could instruct the bank to "stop payment" of a specific transfer. But that does not necessarily mean the consumer intended to revoke the business's authority to receive subsequent electronic fund transfers.[223] For example, after paying a business by check one month only, a consumer may intend to resume paying by electronic transfer in subsequent months.

Consumers typically will first contact the business and tell them to stop future withdrawals. However, some businesses may refuse to stop the withdrawals.[224] When consumers go to the

bank to stop payment of the next transfer or to revoke their authorization of all future transfers, some banks may refuse to do so.[225] In fact, some banks direct consumers to persuade the business to stop sending the bank orders for electronic withdrawals bearing the consumer's account information.[226] Another reason for a bank's refusal may be that the consumer's request does not comply with the requirements of Reg. E, as described below.

Alternatively, thieves may unlawfully obtain information about consumers that enables them to make unauthorized withdrawals by using tactics such as producing counterfeit cards or transferring funds from consumers' bank accounts using online banking services. The bank may require the consumer to produce proof that it was a thief who engaged in fraudulent practices resulting in the withdrawals and not someone the consumer authorized to withdraw funds. This is often difficult for consumers to do, as they can rarely discover the thief's identity. Also, the bank usually will require the consumer to make a police report.[227] Until the consumer satisfies the bank's requirements, the bank may put a hold on the account. That prevents further fraudulent withdrawals but also makes it impossible for the consumer to use the account to make mobile and other types of payments.

Reg. E grants consumers the right to stop payment of preauthorized electronic fund transfers from their accounts.[228] "Preauthorized electronic transfer" is defined as "an electronic fund transfer authorized in advance to recur at substantially regular intervals."[229] Sellers can obtain the consumer's authorization to make preauthorized transfers electronically as long as the seller complies with E-Sign requirements.[230] Consequently, consumers can authorize the transfers via their mobile devices. Reg. E contains detailed requirements that sellers must follow in order to obtain the consumer's authorization for preauthorized transfers.[231]

To stop payment on a preauthorized transfer, the consumer must notify the financial institution either orally or in writing at least three business days before the scheduled date of the transfer.[232] The financial institution is permitted to require the consumer to give written confirmation of the stop-payment order within 14 days of oral notification. If the institution requires written confirmation, it has to inform the consumer of that requirement and provide the address where the confirmation must be sent. The financial institution is no longer bound by the consumer's oral stop-payment order if the consumer fails to provide the required written confirmation within the 14-day period.

If a financial institution complies with a consumer's order to stop payment on a preauthorized transfer, the issue then becomes whether that request prevents a seller from obtaining that particular transfer of funds or all future transfers.

The law is ambiguous on this issue. The EFTA and Reg. E does not specifically address the fate of future payments after the consumer issues a stop-payment order of a scheduled debit, but according to an official Federal Reserve Board staff interpretation:

> The financial institution must honor an oral stop-payment order made at least three business days before a scheduled debit. If the debit item is resubmitted, the institution *must continue to honor the stop-payment order* (for example, by suspending all subsequent payments to the payee-originator until the consumer notifies the institution that payments should resume).[233]

Another issue on which the law is ambiguous is whether the stop-payment provisions for preauthorized transfers apply only to financial institutions or also to payees.[234] There are court decisions supporting each of these positions.[235] In those jurisdictions where courts rule that the stop-payment provisions do not apply to payees, consumers are unable to obtain a remedy even though the payee has engaged in conduct that undermines the consumer's right under the EFTA to stop payment. For example, in one case the business sent the consumer a communication requiring the consumer who wanted to stop payment of a preauthorized transfer to do so only by sending a written request.[236] As discussed above, this is contrary to the EFTA, which permits consumers to provide oral notification. The court held that the provision permitting oral notice referred only to financial institutions. Consequently, the business was not liable for telling the consumer that written notice was required even though that was contrary to the EFTA. In another case, as a condition of obtaining a loan, the payee required the consumer to sign a waiver of the right to stop payment of preauthorized electronic fund transfers.[237] The EFTA's provision granting consumers the right to stop payment of preauthorized transfers is thwarted if payees are not liable for seeking to completely deprive consumers of that right.

Due to a gap in the law, Reg. E is silent on whether a consumer can stop payment of electronic fund transfers that are not preauthorized. An example is a one-time mobile payment charged to the consumer's debit card account. An argument can be made, however, that if a consumer has told the financial institution to stop payment on one of these other types of electronic fund transfers, any payment by the institution should be considered unauthorized.[238]

Instead of ordering the bank to stop payment, consumers may revoke their authorization for a seller or creditor to make future preauthorized transfers. According to an official Federal Reserve Board staff interpretation, "Once a financial institution has been notified that the consumer's authorization is no longer valid, it must block all *future payments* for the particular debit transmitted by the designated payee-originator. … The institution may not wait for the

payee-originator to terminate the automatic debits."[239] However, the financial institution can confirm that the consumer has properly informed the payee-originator of the revocation.

Consumers who are unable to persuade their bank to stop payments and honor their revocation of authorization can instruct their banks to close their accounts as a last resort. However, due to gaps in the law, some banks are able to place various obstacles in consumers' paths that can make closing their accounts a difficult and lengthy process. A bank may have a legitimate reason for temporarily delaying closing the account, such as the need to wait until pending transactions are completed. But a bank that unduly delays closing an account or places obstacles to closing without legitimate reason, can substantially undermine a consumer's ability to halt automatic electronic debits.[240]

Financial institutions and nonbanks that transfer funds electronically through automated clearinghouses agree to comply with the rules of the Electronic Payments Association, known as the NACHA rules.[241] Those rules permit consumers to stop payment of electronic fund transfers for all types of consumer electronic fund transfers, not just those that are preauthorized. However, the consumer must stop payment at a time and in a manner that allows the consumer's bank a reasonable opportunity to act on the stop-payment order before it debits the consumer's account.[242] Because these transfers can occur very quickly, the consumer will have to notify the bank promptly.

The NACHA rules specifically provide for the consumer to revoke authorization of transfers made over the Internet or a wireless network and apply to transfers that are scheduled in advance.[243] The consumer must notify the institution by following the notification requirements in the agreement between the consumer and the institution. The ability to revoke covers one-time transfers as well as recurring ones.[244]

III. Overdrafts

One of the major benefits of mobile payments is the ease with which consumers can pay for funds that are automatically withdrawn from their bank accounts. However, if there are not sufficient funds in the account, substantial overdraft fees may result. Unless the consumer confirms how much remains in the account before making each purchase, the consumer may wrongly believe there is enough to cover the purchase. Consumers who write checks, for example, cannot know for sure when the holder of the check may deposit it and the consumer's bank will honor it and debit the consumer's account.

Reg. E provides consumers limited protection from overdraft fees. A financial institution is prohibited from imposing an overdraft fee for ATM or one-time debit card transactions unless the consumer has agreed to those fees (known as a consumer "opt-in").[245] The institution first has to provide the consumer with notice describing the overdraft service. The notice must be in writing for the consumer's opt-in to be valid. Consumers can provide the notice electronically if they have agreed to electronic notice. As a result, the notice can be given through the consumer's mobile device.

If the consumer agrees to the overdraft service, the institution must confirm that consent in writing, or, with the consumer's consent, the institution can send a confirmation electronically.[246] The confirmation must include a statement informing the consumer of the right to revoke consent.

Reg. E includes some safeguards intended to prevent financial institutions from pressuring consumers to opt in.[247] The institution may not condition the payment of overdrafts for checks, automated clearinghouse transactions, or other types of transactions on the consumer's consent to overdraft fees. In addition, the institution cannot refuse to pay checks, automated clearinghouse transactions, and other types of transactions that overdraw the account just because the consumer has not consented.

It is important to note the gaps that limit the scope of this regulation. It does not apply to any payment transactions a consumer may make with a mobile device except one-time debit card transactions. It restricts the assessment of only overdraft fees, as opposed to the underlying transaction. The institution can honor a one-time debit card transaction if it causes an account to become overdrawn, even if the consumer has not opted in, as long as the institution does not impose a fee.

Although Reg. E rules on overdraft fees apply only to ATM and one-time debit card transactions, other laws related to overdrafts may apply to other types of mobile payment transactions. Reg. DD, which implements the Truth in Savings Act, requires financial institutions to make various disclosures related to overdraft fees.[248] However, a major enforcement gap was created when Congress repealed the section providing consumers the right to sue financial institutions that violate the Truth in Savings Act and Reg. DD. (The right of individuals to sue for violations of statutes and regulations is often referred to as a private right of action.) Consequently, only government agencies can sue banks for violations of Reg. DD.

Federal agencies have published guidance and other materials on overdraft practices.[249] Although guidance does not have the force of law, it expresses the views of agencies that

supervise financial institutions. Consequently, institutions have an incentive to comply with the recommendations. In addition, guidance may influence a court where the law is not clear or has not caught up with current technology and practices, such as mobile payments.

A joint guidance from prudential regulators issued in 2005 suggested obtaining the consumer's consent to overdraft services, having daily limits on fees, and monitoring excessive use.[250] An FDIC guidance that took effect in 2011 made several strong recommendations to regulated banks, including the following: Monitor overdraft programs for excessive and chronic use, impose daily limits on fees, charge fees that are reasonable in relation to the amount of the original transaction, and do not process checks in a manner that maximizes fees.[251] Federal agencies also have brought actions alleging unfair and deceptive acts or practices in relation to overdraft programs.[252]

In addition, litigation by consumers has focused on the order in which banks choose to pay checks, as well as debit card and other transactions. If banks process transactions of the largest amounts before those in smaller amounts, for example, consumers can incur additional overdraft fees. Some banks follow that practice, while others pay in the order in which the bank receives the transactions. Consumers have based their lawsuits on claims of unfair and deceptive acts or practices, breach of the covenant of good faith, and conversion. ("Conversion" is a legal term for the wrongful possession or disposition of another person's property.) Consumers have won some of these cases and lost others. Several banks have settled for many millions of dollars each.[253]

IV. Remote deposit capture

One of the most popular mobile payment applications is remote deposit capture. RDC allows a person who wants to deposit a check to simply take a picture of the front and back with the camera on a mobile device and transmit the image to the depositor's bank.[254] That bank then credits the depositor's account and electronically sends the image to the bank of the person who wrote the check, called the "drawer" in the UCC.[255] The drawer's bank decides whether to "honor" the check by paying it. If it honors the check, it debits the drawer's account based on the amount of the check.

The Federal Financial Institutions Examination Council has described the problems consumers may face when they use RDC.

> Faulty equipment, inadequate procedures, or inadequate training of customers … can lead to inappropriate document processing, poor image quality, and inaccurate electronic data. Ineffective controls at the customer location may lead to the intentional or unintentional alteration of deposit item information … or re-deposit of physical items. … There may also be risks related to Web application vulnerabilities, authentication of a customer to the RDC system, and encryption used at any point in the process.
>
> Risks associated with fraud are not unique to RDC; however, certain aspects of fraud risk are elevated in an RDC environment. Check alteration … may be more difficult to detect. … Similarly, forged or missing endorsements … may be less easily detected. … Certain check security features may be lost. … Counterfeit items may be … difficult to detect. Duplicate presentment of checks and images at the institution or at another depository institution represents both a business process and a fraud risk.[256]

The two parties in a deposit transaction are the "drawer" and the "depositor." In a consumer transaction, either one or both may be consumers. The following analysis assumes that both are consumers. Unless otherwise noted, the depositor is the payee, the person the drawer intends to pay. Both the drawer and the depositor may encounter problems when the depositor uses RDC.

A legal analysis of RDC is complicated by several factors. The transaction involves both a paper check and the electronic transfer of a digital image of the check. While the check is still in its paper form, the transaction is subject to the rules of the UCC. The UCC is not a consumer protection statute. It purposefully leaves consumer protection issues to other laws that the federal government or a state legislature may choose to enact.[257] In addition, its provisions are tailored to banking technology in use during the 1990s, when the current version of UCC Article 4 was drafted and RDC did not exist.[258]

Electronic transfer of the funds represented by the check is governed primarily by the EFTA and Reg. E.[259] Consumer protection is the explicit purpose of the EFTA.[260] However, how it applies to certain aspects of RDC is uncertain because the EFTA was enacted decades before RDC was invented. To the extent that no law applies to a problem the consumer encounters using RDC, the agreement between the consumer and the bank binds the consumer.[261]

For example, the amount credited in the depositor's bank account may not properly reflect the amount written on the check. As the FFIEC notes, the digital image may be of poor quality. Alternatively, faulty bank equipment may account for the problem. The credit to the depositor's account may be in an amount greater than that written on the check or may be less than that

amount. If it is less than that amount, the depositor will want to have the error corrected. But to do so, the depositor will have to try to identify how and at what stage of the transaction the error occurred, unless the depositor's bank is willing to correct the error without that information.

If the error resulted in a credit to the depositor's account that is greater than the amount written on the check, the drawer's account will be debited more than it should have been. In that case, it is the drawer who will seek to have the error corrected.

The EFTA and Reg. E include an error resolution procedure for consumers.[262] Consumer drawers and depositors can take advantage of those rules if they comply with Reg. E's requirements. Major limitations in those rules, however, may thwart the consumer's ability to have the problem corrected. For example, the definition of error does not include a dispute over the quality or nondelivery of goods or services the transfer is paying for. Furthermore, the consumer must notify the financial institution within a certain period of time. In addition, the institution can limit its investigation of the alleged error to its own records and need not contact other parties to the transaction as part of its investigation.[263] Moreover, if the drawer does not review the statement on which the error occurred, the drawer will not discover the error and will not be able to take advantage of the error resolution procedure. Even if the statement is reviewed, if the error is a small one, the consumer will not realize the mistake without carefully reviewing the exact amounts of the debits.

The drawer's account also can be debited more than the amount of the deposited check in a scenario known as the "double debit." This can occur in several ways. For example, a depositor may deposit the check using RDC. The depositor may forget having done so and take the paper check to the depositor's bank to deposit it or obtain cash for it. The depositor's bank forwards the check for collection, and it will be presented to the drawer's bank. If the drawer's bank does not realize the check has already been deposited via RDC, the drawer's account will be debited twice. In another scenario, the depositor may use RDC to deposit the check and leave the paper check at home. A spouse or other joint accountholder, trying to be helpful, may deposit the paper check.

These problems could be prevented if the depositor writes "void" on the check immediately after making the RDC deposit. Once the check includes the word "void," it cannot be deposited at a bank by anyone. Furthermore, no reasonable person, such as a check cashing store, should cash the check for the payee or any other holder. However, before voiding the check, depositors should verify that their bank has properly recorded the transaction. If the check was not properly recorded and has already been marked as void, the depositor will not be able to

deposit or cash it. Similarly, the consumer could prevent a double debit by destroying the check promptly after making the RDC deposit. However, that may also not be a good idea because the consumer may need the paper check if problems arise.[264]

Another safeguard the depositor could use would be to write a restrictive endorsement on the back of the check.[265] "For deposit only" is an example of a restrictive endorsement. Depositors should sign their name directly under the restrictive endorsement and not above the endorsement. Otherwise, another person who obtains the check could sign under the endorsement, claim to have written the endorsement, and try to deposit the check.[266]

Depositors also could write their account numbers along with the endorsement so even if the paper check is stolen, the thief who tries to deposit it cannot prevent the funds from being deposited into the depositor's account.

Adding a restrictive endorsement may be better than voiding the check. Since many consumers regularly sign their deposits in this manner already and writing "void" on a check is unusual, the depositor may forget to do it. In contrast, many depositors likely are accustomed to writing a restrictive endorsement as soon as they receive a check, and doing so in no way impedes their ability to use RDC.

However, clever wrongdoers can find ways to evade steps depositors take to protect themselves. For example, chemicals that are difficult to detect can erase restrictive endorsements and checks marked as void. When a person uses RDC to deposit a check by taking a picture of the front and back of the check, current technology cannot determine if the picture of the back of the check is actually what it purports to be.[267] As a result, a thief who steals the paper check containing a restrictive endorsement can take a picture of the back of a check that does not contain a restrictive endorsement and substitute that as the back of the stolen check the thief is depositing through RDC. Writing "deposit only" on the back of a check does not prevent a depositor from attempting to make multiple deposits via RDC by depositing the check at different banks.

Dishonest depositors have taken advantage of RDC to make double debits.[268] Even if the drawer correctly believes the person to whom the check is written is honest, a different person may be the one who deposits the check. A check is a negotiable instrument, meaning that simply by endorsing the check the original payee can transfer full right to payment to another person.[269] The drawer has no control over whom that subsequent holder of the check may be.

One scheme that dishonest depositors have engaged in is to deposit the check using RDC, then take the paper check to a check cashing store and cash it there. Unless that store takes the check in bad faith or has noticed that the drawer has a claim or defense, the store has the status under the UCC of a "holder in due course." If the drawer's bank refuses to pay the store because it has already honored the check when it was deposited via RDC, the store can go after the drawer for payment.[270]

A dishonest depositor also may alter the check by raising the amount for which the check is made payable. Chemicals are available to make such alterations difficult for banks to detect. If the check has been converted to a digital image and deposited via RDC, it may be impossible to detect.[271] As a result, the consumer's bank will honor the check and debit the consumer's account for the altered amount of the check.

The UCC includes provisions that allocate liability when problems such as alterations arise.[272] However, because the UCC was drafted long before RDC was developed, the law is ambiguous as to whether its provisions apply to RDC; if it does apply, it is unclear how. For example, the UCC includes a provision permitting the electronic presentment of checks.[273] Presentment occurs when a financial institution transfers a check to the drawer's bank for collection. If this provision applies to RDC, other provisions of the UCC may also apply. However, the language used in the presentment section seems to apply only to certain ways in which checks are presented to the drawer's bank.[274]

The Expedited Funds Availability Act and Reg. CC require the depositor's bank to make the funds from a deposited check available promptly.[275] However, since the statute and regulation were drafted prior to the development of RDC, there are gaps in the law.[276] If these laws do not apply to checks deposited via RDC, the contract between the consumer and the bank will be established when funds are made available.[277] As a result, a person who chooses to deposit the check using RDC may have to wait much longer until the funds from the check are available than if that person had deposited the check in person or through an ATM.[278] Consumers may wrongly assume that when checks are deposited through RDC the funds are available as quickly as deposits made in other ways. As a result, when consumers try to draw on deposited funds to make mobile payments, the funds may not be available and the consumers could overdraw their accounts.

Some banks that offer prepaid cards as well as nonbank prepaid card companies permit holders of the cards to use RDC to deposit checks in order to load money onto the cards.[279] For the most part, statutes and regulations covering RDC do not apply to prepaid cards.[280]

Consequently, consumers' rights are generally limited to those, if any, that are granted in the banks' agreement with consumers.

Even if the UCC and the EFTA apply to RDC, gaps remain. Neither law addresses issues that may arise. For example, who is liable if the consumer's camera takes a blurry image resulting in the wrong amount being deposited or the funds being deposited into the wrong account? Alternatively, who is liable if the camera takes a clear picture but because of a glitch in electronically transmitting the image, the wrong amount or account number is sent? Who is liable for a double debit in each of the several scenarios in which that may occur? Private agreements among the commercial parties that process the payments may answer some or all of those issues. But consumers are not parties to those agreements. Even if the agreements protect consumers against liability, most know nothing about them and have no recourse to take advantage of them.

To the extent that no law applies to RDC, consumers and their banks are bound by the terms of their deposit agreements. Those agreements are written by the banks, and many provisions may favor them, not consumers.[281] In addition to bank delays on the availability of funds, discussed above, many banks limit the amount that can be deposited through RDC each day or within 30 days.[282] Moreover, even if the UCC applies, for the most part its rules are default rules that can be superseded by deposit agreements.[283]

V. Security

There is a huge gap in the law related to data security. No comprehensive federal data security law establishing standards or substantive rights and responsibilities exists, nor are there statutes mandating any level of security when consumers make mobile payments. Instead, there are federal and state laws that provide partial coverage. The primary federal law is the Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (GLBA). It provides that "each financial institution has an affirmative and continuing obligation to respect the privacy of its customer and to protect the security and confidentiality of those customers' nonpublic personal information."[284] It defines "financial institution" very broadly to include any company that is significantly engaged in providing financial products or services.[285]

Pursuant to GLBA, federal agencies have required financial institutions to establish, monitor, and evaluate information security systems.[286] According to a guidance issued by the prudential regulators, an institution's review of its security system should include consideration of relevant changes in technology and the sensitivity of its customer information, as well as internal and

external threats to information. The FTC has issued a rule requiring financial institutions under its authority to establish measures to keep customer information secure.[287] Companies are required to evaluate and adjust their information security program in light of material changes to their operations and any other circumstances that they know or have reason to know may have a material impact on their information security program.[288]

GLBA requires companies to establish and monitor security programs, but its regulations impose only general standards of conduct. In light of the significant number of data security breaches affecting tens of millions of consumers, Congress has attempted to draft cybersecurity legislation that will be more effective. The approach taken in most bills has been to establish a structure in which government and private companies share information in order to prevent security breaches. But despite years of effort by both Congress and the Obama administration, disagreement over the details among the various parties involved—private and public, state government, and the federal government—has impeded final passage of any legislation.[289] Some states have enacted data security regulations, while many have not, creating a patchwork of legal rules.[290]

Federal and state agencies are authorized to enforce GLBA.[291] In addition, the FTC has sued companies for violating the FTC Act. The FTC has brought several cases against companies that it said engaged in deceptive representations regarding their security practices and unfair practices for failure to provide reasonable security.[292] Companies have challenged the FTC's authority to sue them for unfair practices in regard to data security.[293] In addition, they maintain that even if the FTC has the authority, it must first issue regulations subject to prior notice and hearing in order to give businesses fair notice of what constitutes an unfair practice in this context. As of this writing, the litigation is still pending.

Courts have created a serious gap in the law by holding that individuals have no private right of action under GLBA.[294] However, consumers may be able to use FTC lawsuits on data security to support using state UDAP laws when there is a data security breach. As noted, the FTC alleges that some companies' security measures violate the FTC Act because they constitute unfair or deceptive acts or practices. As explained in detail later in this report, state UDAP laws also prohibit unfair or deceptive acts or practices, and all states except Iowa permit a private right of action so consumers can sue companies that engage in prohibited conduct.[295] Consequently, consumers may be able to sue companies for practices related to security using their state's UDAP laws, even though they cannot sue them for violating GLBA's requirements for security programs.

The Communications Act of 1934 restricts a telecommunications carrier's use and disclosure of customary proprietary network information (CPNI) in order to protect the confidentiality of such personal call record information.[296] The Federal Communications Commission has issued rules to ensure that confidentiality by requiring carriers to "take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI."[297] In addition, the Communications Act provides that all practices must be "just and reasonable" and any practice that is "unjust or unreasonable is declared to be unlawful."[298] The FCC applied these laws in a case it brought against AT&T, the second-largest wireless carrier in the U.S.[299] The FCC alleged that an internal data breach occurred when some of the company's employees in call centers in Mexico, Colombia, and the Philippines sold information about customers to a third party. The FCC contended that the company violated its rules by failing to properly protect the confidentiality of sensitive personal information and account-related information. The matter was settled through a consent decree in 2015.[300]

The FCC also has adopted data breach notification rules. These may overlap with the state breach notification laws described below. The Communications Act of 1934 protects the privacy of consumer information by permitting wireless carriers to disclose or permit access to personal information about consumers only as "necessary."[301] To ensure that measures are taken when there has been unauthorized access, the FCC issued a rule requiring telecommunications carriers to notify the Secret Service and the FBI of any breach of its customers' CPNI as soon as practicable, but no later than seven business days after determining that a breach occurred.[302] After notifying law enforcement, the carrier must notify its customers of the breach or disclose it publicly.[303]

Since 2003, 47 states and the District of Columbia have enacted data breach notification laws.[304] These laws vary significantly from state to state in terms of what entities are required to provide notices to individuals and how "security breach" is defined, as well as how and when the entity must notify individuals.[305] An entity's duty to notify is triggered by a breach that may result or is likely to result in harm to the individuals whose personal information has been acquired. However, statutes have different definitions of what personal information is covered. North Carolina defines personal information to include information that mobile devices may use for authentication, such as digital signatures, biometric data, and fingerprints.[306] Finally, these statutes typically include a provision for substitute notice if an entity can show that it would cost more than $250,000 to provide notice in the way required by the statute, if the affected class of individuals exceeds 500,000 people, or if the entity can show it does not have sufficient information to contact those individuals. The substitute notice can be made using methods that could involve mobile devices, such as an email notice or posting a notice of the breach on the entity's website.[307]

These laws benefit consumers by alerting them to security breaches. With this information, consumers can take measures to try to protect themselves, such as carefully reviewing their billing statements and notifying card issuers of unauthorized transfers. In addition, they can obtain services that will monitor their accounts and alert them to possible unauthorized transactions. However, critics contend that some forms of identity theft may not be picked up by a credit monitoring service and that consumers may experience a delay in finding out about a problem because of the lag time in reporting. In addition, some companies have engaged in illegal practices when selling these products.[308]

Moreover, because of gaps, the statutes have several deficiencies from a consumer protection perspective. Some states have much weaker laws, so their residents risk the possibility of greater injury.[309] Although government databases are often targeted by wrongdoers, many states exempt government agencies.[310] Many states do not require notification if the breach involves encrypted data.[311] Many states do not require notification if an entity determines that the security breach has not resulted or is unlikely to result in harm to the individuals whose data has been breached.[312] Finally, some of the statutes do not provide individuals with a private right of action; only government agencies can enforce the laws in those states.[313] Even if the breach notification statute provides a private right of action, the individual may not be able to satisfy a court's requirement to show injury.[314]

When a company that holds consumers' funds discovers that a data breach occurred, it can protect consumers from unauthorized withdrawal of those funds by freezing consumers' accounts. But neither state nor federal laws require prompt notification to consumers that their accounts are frozen. Furthermore, no law requires the company to take steps to provide consumers access to their funds.[315]

Some states have enacted statutes intended to prevent breaches. They require companies to establish and maintain reasonable security measures to protect personal information from unauthorized access.[316]

Since federal and most state statutes do not expressly provide consumers a cause of action for security breaches, consumers have relied on various legal theories instead.[317] They have faced obstacles proving damages in the courts. Because companies usually have reimbursed consumers for their direct monetary losses when the companies' security is breached, in some cases consumers have been unable to satisfy federal courts that they have standing.[318] State courts, however, are not constrained by the U.S. Constitution's Article III requirements that dictate strict standing rules, and some have permitted lawsuits to go forward that the federal

courts would have dismissed.[319] These courts may be more amenable to consumer suits based on data breaches.

VI. Privacy

Privacy is closely related to security; to the extent a company's system lacks adequate security, consumer privacy is at risk. There is a major gap in American privacy law because no comprehensive federal law protecting consumer privacy exists, nor are there any statutes specifically protecting consumer privacy in the mobile payments environment. As discussed in the prior section on security, some states require companies to notify consumers when there is a data breach. In a sense, these laws are a bridge between security and privacy. Once a consumer has knowledge of a security breach, the consumer knows there is the risk that his or her privacy may be compromised. The consumer can then try to take measures to protect personal information.

The primary federal privacy statute is the Gramm-Leach-Bliley Act. Every institution subject to it is required to disclose its privacy policy to consumers with whom it has established a customer relationship.[320] Every year, an institution must disclose its practices for sharing nonpublic personal information about consumers to affiliates and nonaffiliated parties. In addition, it must disclose its policies and practices for protecting its consumers' nonpublic personal information. The consumer must be given the opportunity to opt out of the institution's disclosure of nonpublic personal information to third parties.[321] The FTC has issued regulations pursuant to GLBA.[322] Dodd-Frank transferred rule-making authority to the CFPB.[323]

In 2014, the CFPB issued an amendment to its GLBA regulations applicable to consumers using mobile devices. The amendment allows companies to provide the required annual notice by posting it on their websites under certain conditions.[324] In order for customers to know that its annual privacy notice is available on its website, the institution must insert a clear and conspicuous statement at least once a year on an account statement, a coupon book, or a notice or disclosure the institution issues under any provision of law. The statement must inform customers that the annual notice is available on its website and that the institution also will mail a notice to customers who request it by calling a specified telephone number. The institution must continuously post the annual privacy notice in a clear and conspicuous manner on a page of its website. It may not require a login or similar steps or an agreement to any conditions that consumers must meet in order to access the notice. Because some consumers have limited or no access to the Internet, the institution has to mail annual notices to customers who request them by telephone. They must be mailed within 10 days of the request.

In some instances, an institution must still use one of the delivery methods that were permitted prior to this amendment.[325]

GLBA requires the disclosure of important information to consumers about a company's privacy practices and policies. However, it does not establish any minimum requirements as to what those practices and policies must be. Enforcement is left exclusively to law enforcement agencies, which have limited resources and other priorities. Moreover, there is a significant gap in the rules regarding the sharing of information. A company can share information with affiliates, a significant exception for companies engaged in several lines of business. To prevent information sharing with third parties, the consumer must opt out. That is far more burdensome than opting in.[326] It relies on consumer understanding of the significance of information sharing and taking the time to follow the requirements each company has established for the consumer to opt out.

Using its authority under the FTC Act, the FTC has sued companies for unfair and deceptive practices regarding privacy. The FTC Act does not require companies to have a privacy policy; it does not include any privacy rules companies must follow, or even general standards. Rather, in effect, the FTC tells companies that if they have a privacy policy and privacy practices, they must follow those policies and practices, they must not be unfair, and the companies must not make misrepresentations about them.[327] The FTC case law has two limitations. One, it is fact-specific. Each case found an act or practice was unfair or deceptive under the specific circumstances of that individual case. Second, most of the cases have been settled, rather than fully litigated.[328] Consequently, it can be difficult to discern the development of a body of FTC Act law with which companies are required to comply.

Under those circumstances, a company may decide not to have a privacy policy unless it needs one to successfully compete with others. Alternatively, a company may have a privacy policy that is so general that the FTC is unlikely to bring an enforcement action. Put another way, if a company has a privacy policy, it is difficult for consumers, their lawyers, and government enforcement agencies to know when the company's policies and practices are unfair or deceptive.[329] That may make it challenging for state attorneys general and consumers to bring actions under their state UDAP laws.

As with actions involving data breaches, the difficulty that consumers have proving injury is another obstacle to bringing lawsuits for privacy violations. Federal courts are likely to find that the consumer has been unable to prove injury and therefore does not have standing.[330] However, a recent U.S. Supreme Court case may provide consumers with a way to avoid the federal courts' standing requirements in some instances. The justices held that the defendant in

a class action privacy suit brought by a state attorney general was not entitled to have the case moved to federal court.[331] Consequently, the case could remain in a state court. Many state courts have more liberal standing requirements.[332] In addition, many state constitutions include a right to privacy. In those states, a court is likely to take a more permissive approach to consumers trying to prove injury.

In a unanimous 2014 U.S. Supreme Court decision, the court showed it understood the privacy implications of the information routinely stored in mobile phones and in the cloud.[333] Because it was a criminal case involving constitutional search and seizure issues, it is not clear how the court or lower courts might apply that understanding to civil issues. Nevertheless, there is no doubt the court is knowledgeable about the information stored in mobile phones. Moreover, in rejecting the government's contention that a search of a mobile phone is subject to an exception to the rule requiring police to obtain a warrant, the court demonstrated it is sympathetic to privacy concerns and acknowledged the central role of mobile devices in the lives of most Americans.[334]

Consumers have sued Internet-related companies for privacy violations under a variety of statutes and state constitutional provisions. Although the cases have not specifically involved mobile payments, defendants have included companies such as Google and Apple that offer mobile payment services.[335] Consumers have lost many of these lawsuits.[336] In other cases, they have been successful in overcoming motions to dismiss and winning important procedural issues.[337] Winning on issues such as certification of a class often results in an eventual settlement.[338]

One of the greatest dangers of the consumer's privacy being invaded is the identity theft that can result. In these cases, the thief uses personal information, such as a Social Security number, date of birth, and address, to establish credit, obtain bank account information, make purchases, or withdraw money in the consumer's name. Identity theft can result in erroneous and damaging information in the consumer's files with consumer reporting agencies and can greatly lower the consumer's credit score.

In 2003, Congress responded by amending the Fair Credit Reporting Act to include provisions offering some protection when the consumer is subject to identity theft. (The amendment, the Fair and Accurate Credit Transactions Act, is known as FACTA.) Consumers can request that any disclosures to them of information in their file omit the first five digits of their Social Security number or similar consumer identification number.[339] If a consumer informs the consumer reporting agency that the consumer is a victim of identity theft, the agency must provide a summary of the consumer's rights as an identity theft victim.[340] Consumers who assert a

suspicion that they have become, or are about to become, a victim of fraud or related crime, including identity theft, can request that the agency include a fraud alert in their file.[341] A consumer reporting agency must block the reporting of any information in the consumer's file that the consumer identifies as information that resulted from an identity theft.[342] While FACTA provides greater identity theft protection to consumers in some states than they had under state law, in other states consumers have less protection from identity theft than before FACTA because that law pre-empted stronger state law.[343]

Other potential legal bases for consumers to use in the case of identity theft and other privacy invasions include common law and statutory tort causes of action and other state statutes.[344] But each of these presents substantial challenges for consumers, because of the gap in the law resulting from lack of a comprehensive, up-to-date federal privacy statute. For example, the tort of public disclosure of private facts applies when the disclosure would be highly offensive to a reasonable person.[345] One of the requirements is that plaintiffs must prove that their private information was disclosed to the public at large, not to just a few people or a small group. In most situations where consumers' privacy is invaded, consumers cannot meet that threshold.[346]

Another potential tort is the tort of intrusion. This occurs when there is an intentional intrusion into a person's private affairs.[347] However, consumers can use this tort only against the person who engaged in the intrusion, which in this case is an invasion of privacy, not against the person who disclosed information about the consumer. For example, in one case, the information about the consumer that the bank disclosed to others came from the bank's own records. The bank never intruded into the consumer's personal affairs because it didn't have to—it had ready access to the information. Consequently, the court held that the bank was not liable for the tort of intrusion.[348]

A major limitation for consumers suing on the basis of the disclosure of private personal information is that a great deal of personal information is no longer private. Instead, increasing types and amounts are stored in a variety of electronic databases and available to anyone with access to the Internet.

Some states have enacted privacy statutes that are especially pertinent to mobile payments. These laws prohibit the disclosure of consumers' financial information to nongovernmental third parties.[349] However, some of these states, including New York and California, do not grant consumers a private right of action, and that is a serious gap.[350] Other states include major exceptions to the prohibition.[351]

Another California statute, the Online Privacy Protection Act, does not prohibit collecting or sharing consumer information. Instead, it requires the operator of a commercial website or online service to "conspicuously" post its privacy policy if it collects "personally identifiable information" from California residents who use or even just visit the website or online service.[352] The statute contains detailed requirements for the contents of the disclosure.[353] However, an operator is not necessarily in violation of the law if it fails to post its privacy policy. Instead, it is in violation only if it fails to post its policy within 30 days of being notified it has not complied with the statute.[354] Moreover, an operator violates the law only if it fails to comply with the posting requirements or with the provisions of its privacy policy in one of two ways: that the noncompliance is done "knowingly and willfully" or "negligently and materially."[355]

In order to sue in federal court, plaintiffs must satisfy Article III of the U.S. Constitution, which requires plaintiffs to show they have "standing" to sue because they have suffered an "injury in fact." To do so, plaintiffs have to demonstrate, among other things, that their injury is actual or imminent and not hypothetical or conjectural.[356] Courts have strictly applied that standard in cases involving data privacy. As a result, it is a "significant barrier to entry" for plaintiffs.[357] One court explained that the plaintiff must allege and prove how the defendant's use of the plaintiff's information "deprived the plaintiff of the information's economic value … Plaintiff must sufficiently allege that in the process … [of the defendant using the information, the plaintiff] lost dollars of his own."[358] In one case, the court rejected the plaintiffs' information privacy claim. The plaintiffs alleged the defendant allowed others to obtain information about the plaintiffs' use of Apple apps. The court ruled there was no injury in fact because the plaintiffs did not allege that they attempted to profit from their own personal information but were prevented from doing so because of the defendant's conduct.[359] The plaintiffs did not allege they tried to sell their information or intended to do so in the future. Therefore, they did not suffer "injury in fact."

In another case, however, the court refused to dismiss a consumer's case based on Google's violation of its privacy policy when it disclosed user information to software developers.[360] The court held that the consumer had alleged facts sufficient to state a claim for breach of contract, breach of the covenant of good faith and fair dealing, and unfair competition. Consequently, she had "alleged that she suffered damages ('injury in fact') resulting from Google's" breaches and unfair competition.[361]

Some plaintiffs have tried to use California's Unfair Competition Law to demonstrate harm in privacy invasion cases. That statute requires plaintiffs to prove they "lost money or property." Consumers have argued that they have a property interest in their personal information. In the

absence of explicit statutory language granting consumers this property interest, courts have rejected that contention.[362]

VII. 'Kill switch' laws

The theft of mobile devices has become widespread.[363] "Kill switch" laws are designed to protect consumer privacy when there has been a security breach or the consumer's phone has been lost or stolen and privacy may be invaded. But there is a gap in the law of most states since these laws have been enacted only in California and Minnesota. The Minnesota statute simply provides: "Any new smartphone manufactured on or after July 1, 2015, sold or purchased in Minnesota must be equipped with preloaded antitheft functionality or be capable of downloading that functionality. The functionality must be available to purchasers at no cost."[364] The law's definition of a smartphone contains a gap because it "does not include a phone commonly referred to as a feature or messaging phone, a laptop computer, tablet device, or a device that has only electronic reading capability."[365]

The California statute is more detailed. It provides that any smartphone manufactured after July 1, 2015, and sold in California must "include a technological solution at the time of sale, to be provided by the manufacturer or operating system provider, that, once initiated and successfully communicated to the smartphone, can render the essential features of the smartphone inoperable to an unauthorized user when the smartphone is not in the possession of an authorized user."[366] The law provides that during the initial device setup process the smartphone must prompt an authorized user to enable this function. Moreover, the user must be able to reverse the process and restore the operation of the phone. The authorized user must be able to "affirmatively elect to disable or opt out of enabling" this feature at any time.[367] Like Minnesota's law, the statute excludes laptops, tablets, and devices that have only electronic reading capability.[368]

A person who engages in the knowing retail sale of a smartphone in violation of the California statute may be subject to a civil penalty of $500 to $2,500 for each smartphone it sells in California.[369] However, consumers cannot sue for violation of the law. Only the attorney general, a district attorney, or a city attorney can sue for a violation. Finally, there is no liability if the failure to comply with the law "results from or is caused by a failure of a technological solution required pursuant to this section, including any hacking or other third-party circumvention of technological solution, unless at the time of sale the seller had received notification from the manufacturer or operating system provider that the vulnerability cannot be remedied by a software patch or other solution."[370]

The U.S. Senate and House of Representatives have considered federal "kill switch" legislation. But neither has passed any of the bills.[371]

No laws prohibit companies from making mobile devices with disabling capabilities. Companies do not need legislation to permit them to voluntarily offer those features to consumers. Apple has included a "kill switch" in its iPhones. According to the New York attorney general, thefts of Apple phones in New York City, San Francisco, and London were significantly less frequent in the first five months of 2014, after Apple began selling phones that included the disabling feature.[372] During the same period, the theft of Samsung phones increased. This suggests that thieves are learning which types of phones are worth stealing because it is easier to access information from them.

VIII. Unauthorized payments charged to consumers' accounts with wireless carriers

The second stage of this report described the regulation of payments charged to accounts with wireless carriers. Many companies have engaged in cramming, the practice of causing unauthorized charges to be put on the consumer's bill.[373] This portion of the report discusses the FTC's lawsuits against these companies for violating the FTC Act. The FTC has found that some companies engaging in cramming have violated the FTC Act's prohibitions of unfair acts and practices as well as deceptive conduct.

For example, in one case, a company billed consumers for text message-based subscription services that consumers did not authorize.[374] The services included sending periodic text messages containing celebrity gossip alerts, horoscopes, and similar kinds of information. The charges placed on consumers' mobile phone bills often had abbreviated and uninformative descriptions. Many consumers unwittingly paid these charges on their mobile bills. Others disputed the charges but were unable to obtain refunds. The FTC contended that the text messaging company deceptively led consumers to believe they were obligated to pay for the messages. The FTC also contended that the company engaged in unfair practices by billing consumers for unauthorized services.

Another company offered "free" merchandise. The company failed to disclose that by sending the company their mobile phone number, consumers would be billed a monthly charge for services unrelated to the free merchandise. The FTC alleged that this amounted to a deceptive act or practice.[375]

One characteristic of these cases is their massive scale. In the first case, the company's scam resulted in millions of dollars in unauthorized charges.[376] In settling the case, the company surrendered more than $10 million in assets.[377] The second case involved an international network of scam artists that sent millions of unwanted text messages.[378]

In two other cases, the FTC sued the wireless carrier. In its suit against AT&T, the FTC alleged that the carrier had strong reason to suspect that charges for text messaging services on consumers' cellphone bills were unauthorized because many consumers complained and demanded refunds.[379] In some months, 40 percent of the third-party charges were disputed by consumers. AT&T profited by many millions of dollars since it took at least 35 percent of each charge. AT&T agreed to settle, paying $80 million to consumers and $25 million to the government. A similar case against T-Mobile resulted in $90 million in refunds. In addition, T-Mobile was ordered to pay $4.5 million to the FCC and $18 million to the attorneys general of all 50 states and the District of Columbia.[380]

A pending suit brought by the CFPB alleges that Sprint engaged in unfair acts and practices by illegally billing tens of millions of dollars of unauthorized third-party charges for messaging services, taking a 30 to 40 percent cut of each charge and ignoring consumer complaints.[381] In some instances, consumers were induced by website offers of "free" digital services; in other situations, the third parties had charges put on consumers' wireless bills without any communication with the consumers. The CFPB has filed a similar suit against Verizon.[382]

There is a significant gap in the law regulating cramming. If neither the FTC nor the CFPB takes action against a company, a consumer with a cramming complaint involving a mobile payment does not have the benefit of a statute or regulation explicitly providing a right of action. As explained in the Stage 2 portion of this paper, the FCC has regulated cramming only in connection with landlines.

In March 2015, Fair Isaac Corp., the marketer of the popular FICO credit score, announced that in the future it would make available a credit score based on a consumer's history of paying cellphone and cable bills as well as other factors.[383] The objective is to provide a new credit score for consumers who do not have good credit scores because of past problems such as bankruptcy, foreclosure, or debt collection. Consumers whose cellphone accounts are delinquent because they refused to pay charges due to cramming will not be able to take full advantage of this new type of credit score.

IX. Children making mobile payments without parental consent

The second stage of this report described the Children's Online Privacy Protection Act of 1998 (COPPA), the federal law imposing requirements on companies prior to collecting personal information from children under 13. In 2012, the FTC amended its COPPA regulations to take the mobile environment into account by including smartphones and tablets.

The FTC has brought cases where it alleged violations of COPPA claiming that the companies failed to provide notice to parents of its information practices and obtain parental consent prior to collecting, using, or disclosing information from children online.[384]

The FTC also has brought lawsuits alleging that companies violated the FTC Act prohibition on unfair practices by billing accountholders for "in-app" charges made by children without obtaining prior accountholder (usually parental) permission.[385] These are charges for items that cost money while the user is within the app. Often, these are charges for virtual items or currency used in playing a game.[386]

X. Insolvency and bankruptcy

If consumers charge their mobile payment to their debit card account, the funds will be withdrawn from the consumer's account with the financial institution that issued the debit card. Most consumer bank accounts are insured by the FDIC.[387] Therefore, consumers will not lose the money in their accounts if the bank fails.

However, if consumers use prepaid accounts when they make mobile payments, whether their funds are insured by FDIC deposit insurance depends on several factors due to gaps in the law governing deposit insurance.[388] The money consumers pay to fund prepaid card accounts are not held in a separate account for each consumer. They may still be insured, though, if the funds qualify for "pass-through" insurance. According to a 2008 FDIC general counsel's opinion, only funds deposited with an insured depository institution are eligible for pass-through insurance.[389] And if the bank fails, the consumer is entitled to be paid only under specified conditions.[390]

While under certain circumstances funds in prepaid cards may be insured, they very well may not be insured.[391]

> There are many ways in which the funds on a prepaid card could be uninsured. FDIC insurance is not required for these cards, so a program manager could choose not to provide it. In addition, prepaid cards must be registered with the program manager before FDIC pass-through insurance will apply. This means that "temporary cards," which are commonly distributed to consumers when they purchase a prepaid card at a retail store, are not FDIC-insured.[392]

Consumers use services such as Google Wallet, PayPal, and Apple Pay primarily as intermediaries to transfer money from their bank accounts to others. But many consumers also store some of their funds with Google Wallet and PayPal. While Apple Pay currently processes only person-to-business payments, the others also process person-to-person transfers. Because the companies are not chartered as depository banks, they cannot qualify for FDIC insurance to protect the consumers' funds if they go out of business. However, they can partner with banks and put consumers' funds in accounts in the company's name at these banks. Provided the company and the bank follow FDIC procedures, consumers' funds are protected by deposit insurance. In April 2015, Google announced that, going forward, funds stored in Google Wallet would be protected by FDIC insurance.[393]

At least three companies involved in prepaid card services have filed for bankruptcy or become insolvent. Only one was an FDIC-insured bank.[394]

As described above, FDIC insurance protects funds in prepaid accounts under some circumstances. However, due to gaps in the laws regulating deposit insurance, FDIC insurance applies only to funds held in an insured bank account. Under no circumstances does it cover funds consumers pay to merchants that issue prepaid cards; the insurance protects the funds only if and when it is subsequently deposited into an insured account.

> The loading process for prepaid cards creates situations in which funds are not under the control of a financial institution and are therefore uninsured. For example, when a customer uses a Green Dot MoneyPak to load funds, the funds are not insured [at first]. … Until the MoneyPak is used and Green Dot transfers the funds to the program manager, which then deposits the funds in an insured account, the money is not protected by the FDIC.[395]
>
> In addition, there are no supervisory safeguards to ensure that program managers that claim to hold customers' funds in an FDIC-insured account are in fact holding all of those funds in such an account. For example, a dishonest company might use customers'

funds for high-risk investments. If a program manager goes out of business, any funds that are not actually being held in an insured account could be lost.[396]

The consumer does not know and cannot assess the issuer's compliance with the FDIC's guidance.[397]

As discussed above in the Stage 2 portion of this paper, state money transmitter laws may apply, but they do not provide consumers with adequate protection if a company that is not a depository institution fails. [398]

If a bank that holds the funds consumers loaded on their prepaid cards fails, the FDIC takes control of the bank. Usually the FDIC transfers consumer accounts to another bank; if not, it pays consumers the amount of the money in their accounts up to the maximum insurance coverage.[399]

If a nonbank company that offers prepaid accounts goes out of business, consumers probably would not be able to recover their funds. Consumers have the status of unsecured creditors when they claim a right to the money they paid for prepaid cards. If the company simply closes down, state law will apply to the rights of the company's creditors.[400] Government authorities such as the IRS and secured creditors have priority over unsecured consumers to any money that can be obtained through the recovery of funds or proceeds from the sale of other assets.

If the nonbank company files a petition in bankruptcy or creditors force it into an involuntary bankruptcy, consumers' likelihood of being paid depends on whether the funds are held in a trust account.[401] Any funds in a trust account are not considered property of the bankruptcy "estate" and are not subject to claims by other creditors in the bankruptcy proceeding.[402]

If the funds are not in a trust account, the result will be far less favorable for consumers who placed funds on prepaid cards. The company may file a Chapter 7 petition under the U.S. Bankruptcy Code, in which case all property of the company will be liquidated and the resulting funds distributed. As unsecured consumer creditors who have deposited funds in connection with the purchase of services that were not provided, consumers are entitled to claim the seventh priority among other creditors.[403] While this is a superior status compared with general unsecured creditors, they are unlikely to be paid anything.[404]

Alternatively, the case may be filed as a Chapter 11 bankruptcy reorganization.[405] Consumers with claims as prepaid cardholders probably will receive little or nothing.[406] One commentator suggests that in a Chapter 11 reorganization, a company may honor gift cards "in order to

maintain goodwill."[407] If that is correct, companies may also honor general purpose prepaid cards used for mobile payments even though they are not required to do so. Unfortunately, however, many companies that file Chapter 11 petitions are unable to reorganize into successful firms.[408]

In addition to concerns about whether consumers will recover their funds when a nonbank goes out of business, consumers, state attorneys general, and the FTC have feared that consumers' privacy will be invaded if the nonbank sells the consumers' personal information to a third party in an effort to pay off creditors.[409] If a company liquidates its assets outside bankruptcy, state attorneys general and the FTC may oppose the sale of personal consumer information as an unfair act if they discover it may occur. But there is a gap in the law, as no law directly protects consumers' personal information under these circumstances.[410]

In 2005, Congress amended the Bankruptcy Code to include a provision to protect consumers' personal information when its sale is proposed during a bankruptcy proceeding. If a company disclosed to its customers that it had a policy "prohibiting the transfer of personally identifiable information" to people not affiliated with the company, and that policy was in effect on the day the bankruptcy case began, certain safeguards would come into play. The trustee may not sell or lease personally identifiable information unless the sale or lease is consistent with the company's privacy policy.[411]

Alternatively, under specified circumstances, the bankruptcy court can approve of the sale or lease of the information even though it is not consistent with the company's privacy policy. The court must first order the U.S. trustee to appoint a "consumer privacy ombudsman."[412] The ombudsman's task is to provide the court with information "to assist the court in its consideration of the facts, circumstances, and conditions" of the proposed sale or lease of the consumer information.[413] The court can approve the sale or lease after giving "due consideration" to the information the ombudsman has provided and a finding that the sale or lease would not violate applicable nonbankruptcy law.[414]

The privacy amendment provides consumers with some protection, but its vague and ambiguous language has been criticized as not providing "sufficient guidance" and failing to "state specific standards to assist a court in evaluating" the ombudsman's report.[415] In addition, the amendment does not apply if the company did not have a privacy policy prohibiting the transfer of personally identifiable information, or if it had the policy when the consumer purchased the company's goods or services but withdrew the policy before its bankruptcy case began. Finally, it does not apply if a company's bankruptcy proceeding is dismissed.[416]

XI. Remedies

A. Unauthorized use of credit and debit card accounts

In 2015, most credit cards with magnetic stripes are being replaced with more secure chip-and-PIN or chip-and-signature cards. It will likely be quite a while before the transition to the more secure type of card is fully implemented because of difficulties faced by merchants and small banks.[417] But eventually there should be less unauthorized use of credit cards when the cardholder uses the physical card to make a purchase.[418] However, Europe's experience demonstrates that fraudsters will instead target "card-not-present" transactions, such as mobile payments.[419] Consequently, the law protecting consumers from unauthorized credit card transactions will continue to be important, especially for those making mobile payments, since those are card-not-present transactions.

Under TILA and Reg. Z, the consumer's maximum liability for unauthorized charges is $50.[420] If the amount of charges before the consumer notifies the card issuer was less than $50, the consumer is liable for the lesser amount. Furthermore, the consumer has liability for unauthorized use only if the credit card is an "accepted credit card" and the card issuer gave adequate notice to the cardholder of the potential liability for unauthorized use.[421] If the card issuer fails to comply with these limits, the consumer can resort to the billing error and withholding procedures described below.

Under the EFTA and Reg. E, if an unauthorized purchase is charged to a debit card account and the consumer [actual holder of the card] notifies the financial institution within two business days after learning of the loss or theft of the consumer's "access device," the consumer's liability is limited to $50 or the amount of unauthorized transfers that occur before notice if that amount is less than $50.[422] The consumer's debit card is one type of "access device." Moreover, as discussed in the Stage 1 portion of this report, the mobile device itself may constitute an access device. If the consumer does not notify the financial institution within two business days, the consumer's liability is capped at the lesser of $500 or the $50 that occurred within two business days and the amount of unauthorized transfers after the two business days and before notice to the institution.[423] The consumer is liable for the amount in excess of $50 only if the institution establishes that these transfers would not have occurred if the consumer had notified the institution within the two-day period.

If an unauthorized electronic fund transfer appears on a periodic statement, the consumer must notify the institution that sent the statement within 60 days of the institution's

transmittal of the statement. This requirement applies whether or not a lost or stolen access device is involved in the unauthorized transfer. Therefore, it applies to card-not-present transactions such as mobile payments even if the consumer's mobile phone is not considered an access device.[424] If the consumer fails to notify the institution within 60 days, "the consumer's liability shall not exceed the amount of the unauthorized transfers that occur after the close of the 60 days and before notice to the institution, and that the institution establishes would not have occurred had the consumer notified the institution within the 60-day period."[425]

If the institution fails to comply with the limits on a consumer's liability, the consumer can use the law's error resolution procedure, described below, to attempt to persuade the institution to credit the account.

B. Other federal and state remedies

Various laws and rules cover payment mechanisms based on the type of payment method the consumer uses. For credit cards, TILA and Reg. Z provide consumers with the right to withhold payments and dispute errors they discover on their bills. Credit card issuers and others may be liable if they fail to comply with these laws. For debit cards, the EFTA and Reg. E also include a required error resolution procedure for consumers to use when they dispute charges on their statements as well as remedies against those who violate those laws. The NACHA rules also contain provisions that benefit consumers but that do not give them the right to sue for violation of the NACHA rules. Both the FTC Act and Dodd-Frank prohibit unfair and deceptive acts and practices, and Dodd-Frank also prohibits abusive acts and practices. However, these federal statutes fail to give consumers a private right of action. State laws prohibit unfair and deceptive acts and practices, and most give consumers the right to sue companies for violations of those laws. Appendix G contains a detailed discussion of these laws and rules.

C. Requiring arbitration and restricting class actions impede consumer remedies

As described above, consumers have many potential remedies in their arsenal if litigation is necessary to resolve a dispute involving mobile payments. However, there are two major impediments to consumers using them. One is the provision in many contracts that the consumer must resolve any disputes in an arbitration forum, not in court. While companies extoll arbitration's benefits for consumers, consumer advocates bemoan its many

disadvantages.[426] Courts also uphold arbitration clauses in which consumers waive their right to file class actions in court as well as class-wide arbitration.[427]

Pursuant to a mandate in Dodd-Frank, the CFPB has conducted studies of consumer arbitration clauses in financial services contracts to decide whether to fill the current gap in the law and regulate them.[428] The continuation of those aspects of arbitration that impede consumers' ability to take advantage of consumer protection laws may depend on whether the CFPB enacts regulations, and if it does, the substance of the rules.

The CFPB's future regulatory actions will have a direct bearing on mobile payments. Consumers typically use their credit, debit, and prepaid card accounts when making mobile payments. Many of these accounts are subject to agreements that contain arbitration clauses.[429] Any disputes regarding these mobile payments will be decided in arbitration, not in court. Furthermore, as discussed above, many consumers have discovered unauthorized charges claimed by third parties on their mobile wireless carrier's monthly bills, a practice known as cramming.[430] Consumers who refuse to pay the unauthorized charges may have their mobile service terminated by their wireless carrier, rendering it impossible for them to make mobile payments. Other than paying the unauthorized charges, the consumer's only recourse is to take the dispute to arbitration if the contract with the carrier requires arbitration.

The CFPB's 2015 study included the eight largest telecommunications companies that permit third parties to include charges on consumers' bills. Seven of the eight companies in the survey used contracts requiring arbitration.[431] The company not requiring arbitration was one with few subscribers. The seven mandating arbitration served 99.9 percent of all subscribers of the eight companies.

The CFPB study found that almost 86 percent of the wireless contracts reviewed contained arbitration clauses expressly stating that when the consumer's case was heard in an arbitration forum, it was not allowed to proceed as a class action.[432] The contracts of 63 percent of those consumers subject to arbitration provisions waived the consumer's right to participate in a class action filed in a court, including the consumer participating as a named plaintiff or a member of the class.[433] The contracts used by six of the seven companies requiring arbitration included a waiver of the consumer's right to recover consequential and punitive damages, meaning the most a consumer could receive would be actual, out-of-pocket monetary loss directly caused by the company's conduct.[434] None of the wireless contracts "provided that any arbitration hearing would be at a location 'reasonably convenient' for the consumer."[435] Only one company disclosed to consumers the differences between arbitration and litigation in court.[436] None of the customers would be entitled to a jury trial except those few who were customers

of the only company that did not require arbitration.[437] Five of the seven companies requiring arbitration permitted consumers to use only the American Arbitration Association to administer their arbitration proceedings.[438] Most permitted consumers to use small claims court instead of arbitration if they wished.[439] Most companies paid some or all of the initial fees required to arbitrate a case brought by a consumer.[440] Finally, most companies gave the arbitrator the authority to order the company to pay the consumer's attorney's fees if the consumer won the case.[441]

Some contracts do not include arbitration provisions, some arbitration provisions are unenforceable, and others may not contain a class action waiver. In those instances, theoretically consumers can take advantage of consumer protection law and sue companies in court. But because an individual consumer's monetary loss usually is relatively small, it is often financially infeasible for each consumer to hire a lawyer and bear the expense of a lawsuit.[442] Consumer class actions can be an effective and efficient means for large numbers of consumers to recover damages for their injuries in one action.[443] The Supreme Court, however, has decided several cases that greatly restrict a consumer's ability to obtain court certification of a class in the federal courts, and several state UDAP laws prohibit class actions. [444] As a result, without the ability to file a class action, many consumers are unable to pursue their grievances in court even if there is no arbitration provision to impede them.

XII. Conclusion

Stage 3 examines problems that may arise after the consumer makes a mobile payment. There are substantial gaps and much ambiguity in the laws applicable to these problems. As a result, the law is not as protective of consumers as it otherwise would be. Those gaps and ambiguities that may have the greatest impact on consumers making mobile payments are described briefly below.

Consumers' ability to stop and revoke authorization to make electronic transfers out of their accounts is a crucial self-help mechanism to protect against an unjustified and perhaps illegal action. But the law is ambiguous as to the effect on future transfers of a consumer's order to stop payment of a preauthorized transfer. In addition, the law is ambiguous about the effect of stop payment on payees. Lastly, there is a major gap in the law because it does not provide for the stop payment or revocation of transfers that are other than preauthorized.

Overdrafts result in consumers having to pay sizable fees. Because of substantial abuse by financial institutions, there is now a federal regulation prohibiting these fees unless the

consumer opts in. But there is a substantial gap in the rule's coverage: It applies only to one-time debit and ATM transactions.

Remote deposit capture is gaining in popularity. But because of gaps in the law, it is risky. For example, the law does not establish rules for who among the innocent parties suffers the loss when one party commits fraud and the loss cannot be recovered from the fraudulent party. In addition, the law requiring the depositor's bank to make funds available promptly is ambiguous as to whether it applies to remote deposit capture.

Security breaches occur frequently and put consumers' personal information at risk. The federal law does not provide comprehensive coverage, and consumers have no right to sue if a financial institution violates the law. State law varies greatly, has many gaps in who is covered, and merely provides for notification to consumers after a breach has occurred.

There is no comprehensive federal law providing relief to consumers when privacy invasions occur. A federal statute requires financial institutions to disclose only their privacy policies and practices. The FTC has brought enforcement cases alleging unfair and deceptive privacy conduct, but the law is ambiguous because there are few cases and each is grounded in the unique facts of that case. State law is not tailored to the electronic environment, and the courts have established rules that make it difficult for consumers to prove injury.

Because mobile devices are frequently stolen, laws requiring a "kill switch" allowing consumers to block the thief from accessing financial and other information in the device would help reduce loss to consumers. But there is no federal law requiring this safeguard, and only California and Minnesota have enacted such laws.

Consumers often have charges for their purchases put on their wireless carrier bills. Fraudsters have engaged in cramming, in which unauthorized charges are added to consumers' wireless bills. The FCC has failed to directly regulate this. Although the FTC has brought enforcement actions, its resources are limited and there is no explicit cause of action enabling consumers to sue for damages caused by this scam.

Finally, because of the lack of specific consumer protection law on the matter, companies providing mobile financial services are able to include provisions in their contracts requiring consumers to resolve their disputes through arbitration and prohibiting them from participating in class actions. This deprives consumers of the ability to choose between arbitration or suing in court. The limits set by private organizations' rules can result in consumers' inability to obtain

an adequate remedy when the law has been violated. It is uncertain whether forthcoming CFPB rules will ameliorate the problem by adequately filling this gap.

Options for lawmakers

This report describes and analyzes the large number and wide variety of laws applicable to mobile payments. It is evident from this study that the law has not kept pace with the rapid developments in technology that have enabled the industry to produce a steady stream of new products from which consumers can make mobile payments and innovative methods to process those payments. As a result, the law is replete with gaps, ambiguities, and overlap that undermine important consumer protections.

Making recommendations for what lawmakers should do about the inadequacies in the law is beyond the scope of this report. However, it may be helpful to suggest some choices policymakers might consider.

One option is to do nothing. Mobile payments occur in many different settings and involve many types of products that continually add new features. Enacting new laws may result in unneeded or unwise regulation that may stifle innovation that could benefit consumers. But doing nothing leaves consumers at risk of incurring substantial harm. In addition, a business case can be made for the government doing something to protect consumers. To the extent consumers understand they have meaningful legal protection, they will be more likely to use mobile payment services.

An alternative is to enact laws that require greater disclosure to consumers of the risks they take when they make mobile payments and the limits on their legal remedies if anything goes wrong. A better-educated consumer would have the information needed to make an informed decision about whether to make payments using mobile devices. However, consumers already encounter a huge number of disclosures—both legally required and voluntary, and often using confusing legal and technical jargon. Consequently, many consumers reach the point of "information overload" and decide not to pay attention to disclosures.

There are other alternatives to doing nothing besides disclosure. One example is for agencies to issue guidance. Guidance does not have the force of law, so the government cannot act against a company for its failure to comply. Nevertheless, since guidance is an explicit statement of

how an agency wants a company to conduct its business, firms often decide to follow it. An agency can easily update and revise guidance when needed.

Another course of action is for agencies to issue regulations. Regulations have the force of law and are issued only after a proposal is published and the public has ample opportunity to suggest changes or oppose the proposal altogether. Agencies often revise proposed regulations based on public comments. If an agency later discovers that a regulation is unneeded or requires revision, it can draft a proposed revision and invite public comment again. However, an agency can regulate only those matters dealt with in a statute. In addition, an agency can issue regulations on those matters only if the statute authorizes the agency to issue regulations. As this report documents, due to the many gaps, ambiguities, and overlap in many statutes, it is not clear that agencies have the authority to regulate many aspects of mobile payments.

Finally, Congress could pass legislation to remedy deficiencies in the law. However, because the mobile payments market is in great flux and consumer protection can be a controversial issue, it seems unlikely that new federal laws will be passed in the near future.

Even if policymakers decide to subject mobile payments to explicit statutes, regulations, or guidance, still another decision is the content of that law or guidance. Policymakers must choose which aspects of mobile payments are most in need of and amenable to regulation or guidance. Moreover, they must decide whether to draft specific substantive rules or general standards such as “reasonable,” “fair,” “in good faith,” “sufficient,” “adequate,” “effective,” and “state of the art.” Standards give businesses and regulators more flexibility, but they may encourage companies and consumers to file lawsuits to test the application of those standards to specific situations.

This report provides information on which policymakers can base these important decisions.

Appendix A. Credit cards: Withholding and billing error rights under TILA

If a cardholder has a dispute related to a purchase made with a credit card, TILA and Reg. Z contain two important rights: the right to withhold payment after asserting claims and defenses, and the right to assert a billing error. Consumers issued credit cards must be given a disclosure of billing error rights and the right to withhold payment.[445] The provisions of Reg. Z that provide these interrelated rights operate independently.[446] Moreover, there are important differences between the two rights.

These rights affect consumers making mobile payments in two respects. First, consumers purchasing goods and services can charge the sales to their credit card accounts, for example, by waving their phone in front of a card reader at the point of purchase. Second, consumers can pay their monthly credit card bill using their phone if they have registered for their bank's bill payment service.

Cardholders who have a dispute and want to withhold payment must first make a good-faith attempt to resolve the dispute with the person honoring the credit card, who is generally the seller.[447] If the cardholder is unable to resolve the dispute satisfactorily with that person, the cardholder can assert against the card issuer "all claims … and defenses arising out of the transaction and relating to the failure to resolve the dispute."[448] However, tort claims are excluded.[449] The cardholder may withhold payment of the amount of the outstanding credit for the property or services that gave rise to the dispute.[450] The cardholder may also withhold any finance or other charges imposed on that amount. If the cardholder withholds payment, the card issuer is prohibited from reporting that amount as delinquent to a credit reporting agency until the dispute is settled or a court renders a judgment in the matter.[451] If instead of withholding the disputed amount the cardholder pays it, the cardholder can still dispute the transaction through the billing error procedure.

For the cardholder to be entitled to withhold funds under this provision, the amount of the credit extended to purchase the property or services involved in the dispute must exceed $50.[452] In addition, the disputed transaction must have occurred in the same state as the cardholder's current designated address or, if the transaction was in another state, within 100 miles of that address.[453] However, these restrictions do not apply under certain circumstances. The most common one is when the person honoring the credit card is the same person as the card issuer.[454] For example, the restrictions do not apply if the cardholder uses a credit card issued by Sears to buy goods at a Sears store.

Cardholders can withhold payment even if they do not comply with the withholding rules in Reg. Z. The cardholder can instead withhold pursuant to the billing error procedures discussed below. Furthermore, cardholders can withhold the disputed amount even if they do not comply with either the withholding or the billing error procedures. However, if the rules are not followed, the card issuer can report the cardholder's delinquency to consumer reporting agencies. That may have an adverse effect on the cardholder's credit score and ability to obtain future credit on favorable terms.

In addition to withholding disputed charges, the cardholder can take advantage of the billing error procedures in Reg. Z. "Billing error" is defined to include unauthorized charges; a charge for property or services not accepted by the cardholder or not delivered to the cardholder; a charge that reflects the creditor's failure to properly credit a payment; a computational or similar error; a charge for which the cardholder requests clarification, including documentary evidence; and the creditor's failure to mail or deliver a periodic statement to the cardholder's last known address.[455] The definition of a billing error does not include a dispute over the quality of goods. In contrast, the "claims and defense" withholding rules do not preclude the quality of goods as a reason to withhold.

In its account agreement or account opening statement, as well as at least once a year, the creditor is required to inform consumers of the billing error procedure, including the creditor's name and the mailing address where consumers should send information about the error.[456]

In order to use the Reg. Z billing error procedure, the cardholder must send written notice to the creditor.[457] The notice must be received by the creditor no later than 60 days after the creditor sends the first periodic statement that reflects the alleged billing error; enable the creditor to identify the cardholder's name and account number; and, to the extent possible, indicate the cardholder's belief that a billing error exists and the reasons for that belief.[458] The notice also must include the type, date, and amount of the error. The cardholder is not required to resolve the dispute before providing the billing error notice to the creditor. The cardholder is not even required to first notify the seller or other payee of the dispute.[459]

The creditor is required to mail or deliver a written acknowledgment to the cardholder within 30 days of receiving a billing error notice from the consumer unless the creditor has already completed the required billing error procedures.[460] These procedures have to be completed within two complete billing cycles after receiving the billing error notice from the cardholder.

Until the billing error is resolved, the cardholder is not required to pay the portion that the cardholder believes is related to the disputed amount, including finance or other charges.[461] In addition, the creditor may not try to collect that portion. If the cardholder has enrolled in an automatic payment plan in which the cardholder agrees to pay the amount owed on the credit card by periodic deductions from the cardholder's deposit account, the card issuer cannot deduct any part of the disputed amount or related charges if the billing error notice is received up to three business days before the scheduled payment date. Importantly, during the billing error time period the creditor cannot make or threaten to make an adverse report about the cardholder's credit standing, or report that the disputed amount is delinquent. Finally, the creditor is not permitted to accelerate any part of the cardholder's indebtedness or restrict or close the cardholder's account solely because the consumer exercised these billing error rights in good faith.

If the creditor determines that a billing error has occurred as contended by the cardholder, it must correct the billing error and credit the cardholder's account with the disputed amount and related finance or other charges and mail or deliver a correction notice to the cardholder.[462] However, if the creditor determines after conducting a reasonable investigation that no billing error occurred or that the billing error that occurred is different from the one asserted by the cardholder, the creditor must mail or deliver to the cardholder an explanation of the reasons the creditor believes the billing error alleged by the cardholder is incorrect and furnish copies of documentary evidence of the consumer's indebtedness if the consumer requests it. If a different billing error occurred, the creditor must correct the billing error and credit the consumer's account with the disputed amount in related finance or other charges.[463] Finally, Reg. Z specifies the procedure the creditor must follow if it subsequently determines that the consumer owes all or part of the disputed amount.[464]

Appendix B. Liability for violations of TILA

All three parts of this report have described how the Truth in Lending Act applies to the various stages of transactions in which consumers make mobile payments using their credit card accounts. When a creditor violates TILA, the statute's liability provisions provide consumers with a remedy.

The general liability section in TILA provides that "any creditor who fails to comply with any requirement imposed under this part … with respect to any person is liable to such person in an amount equal to the sum of" any actual damage sustained by that person as a result of the

creditor's failure to comply.[465] In addition, a court may award statutory damages in which an individual brings an action related to open-end credit, which includes credit card accounts.[466] In that situation, the damages are twice the amount of any finance charge in connection with the transaction, but with a minimum of $500 and a maximum of $5,000. The court may award higher statutory damages if that is appropriate "in the case of an established pattern or practice" of failure to comply. If the court rules in favor of the consumer, it may award costs and a reasonable attorney's fee.[467] TILA includes a provision limiting the amount of recovery in class actions.[468]

A creditor or its assignee is not liable, however, if it can show "by a preponderance of evidence that the violation was not intentional and resulted from a bona fide error notwithstanding the maintenance of procedures reasonably adapted to avoid any such error. Examples of a bona fide error include, but are not limited to, clerical, calculation, computer malfunction and programming, and printing errors, except that an error of legal judgment with respect to a person's obligations under this subchapter is not a bona fide error."[469] In addition, there are other defenses to liability under TILA.[470]

Appendix C. Debit cards: Error resolution procedures under the EFTA

Reg. E contains a detailed procedure for consumers to use when they believe there has been an error in an electronic fund transfer. "Error" is defined as an unauthorized electronic fund transfer, an incorrect electronic transfer to or from the consumer's account, the omission of an electronic transfer from a periodic statement, a computational or bookkeeping mistake made by the financial institution that relates to an electronic transfer, the consumer's receipt of an incorrect amount of money from an electronic terminal, or an electronic transfer not identified as required by the regulation. The definition also includes the consumer's request for documentation or additional information or clarification, such as a request the consumer makes to determine whether there has been an error.[471] Unlike TILA, there is no provision permitting the consumer to assert claims and defenses such as the poor quality or nondelivery of goods and services the electronic transfer was paying for.[472]

The financial institution is required to inform its customers, in its initial disclosures and in either its annual disclosures or with each periodic statement, how to contact the institution to report errors.[473] The notice must include a telephone number, postal address, and email address.[474]

The consumer must provide an oral or written notice of the error no later than 60 days after the institution sends the periodic statement on which the alleged error is first reflected.[475] The notice must enable the institution to identify the consumer's name and account number and indicate why the consumer believes an error exists. To the extent possible, the consumer should include the type, date, and amount of the error. The financial institution can require the consumer to give written confirmation within 10 business days of the consumer's oral notice. The institution must inform the consumer of this requirement to provide written confirmation and provide the address where the written confirmation must be sent at the time the consumer gives oral notification. If the consumer has requested documentation or clarification, the consumer's notice of error must be received by the institution no later than 60 days after the institution sends the requested information.

The institution is required to investigate the alleged error "promptly."[476] Within 10 business days of receiving the consumer's notice of error, it must determine whether an error occurred. It then has to report the results to the consumer within three business days of completing its investigation. Furthermore, it must correct the error within one business day of determining that an error occurred.

However, if the institution is unable to complete an investigation within those 10 business days, the institution may take up to 45 days from receipt of the notice of error to investigate and determine whether an error occurred.[477] To take advantage of this extended period, the institution must provisionally credit the consumer's account in the amount of the alleged error within 10 business days of receiving the error notice. In addition, the institution must inform the consumer of the amount and date of the provisional credit and give the consumer full use of the funds during the investigation. If the institution determines that an error occurred, it must correct the error within one business day. Finally, the institution must report the results of its investigation within three business days of completing it.

Reg. E includes a major limitation on the scope of the institution's investigation. The financial institution's review can be limited to its own records regarding an alleged error.[478] Consequently, the institution's investigation need not include a consideration of whether other parties to the transfer may have caused the error. But this limitation applies only if the alleged error concerns a transfer to or from a third party and there is no agreement between the institution and the third party for the type of electronic fund transfer involved. This limitation could substantially curtail a consumer's ability to discover the source of an error, since several companies may be involved in processing and transferring a mobile payment.

Some companies have used fraudulent methods to thwart consumers' attempts to use the EFTA's error resolution procedure. In one case, consumers disputed electronic withdrawals made by a payday lender, alleging they never authorized the withdrawals or even agreed to take out loans. As part of their investigation of the consumers' claims, the banks contacted the lender to determine if the withdrawals were unauthorized. According to the CFPB, the consumers did not agree to take out the loans but the lender had sent the banks fraudulent documents purporting to show the consumers had agreed to the loans and authorized the withdrawals. As a result, in some instances the bank rejected the consumers' claims and refused to recredit their accounts in the amounts of the unauthorized withdrawals.[479]

If the institution determines that no error occurred or there was an error but it was different from that alleged by the consumer, the institution must report the results of its investigation to the consumer.[480] This must include a written explanation of the institution's findings and inform the consumer of the right to request the documents on which the institution relied. If the institution has determined that no error occurred, the institution can debit the provisional credit. It must notify the consumer of the date and amount of the debit. In addition, it is required to notify the consumer that the institution will honor checks and similar instruments payable to third parties as well as preauthorized transfers from the consumer's account for five business days after this notification of the debit.

Appendix D. Liability for violations of EFTA

The EFTA contains two provisions that impose liability on entities that fail to comply with the requirements of the statute. One provision applies only to financial institutions. Under that section, the financial institution is liable to a consumer for all damages proximately caused in three situations listed in the EFTA.[481] These are: (1) the financial institution's failure to make a transfer in the correct amount or in a timely manner according to the terms and conditions of the account where the consumer properly instructs the institution to make the transfer; (2) the institution's failure to make a transfer due to insufficient funds when there would have been sufficient funds had the institution properly made a credit or a deposit of funds to the consumer's account; or (3) the institution's failure to stop payment of a preauthorized transfer from the consumer's account when instructed to do so in accordance with the terms and conditions of the account. [482]

The institution is not liable where it shows by a preponderance of evidence that its action or failure resulted from an act of God or other circumstances beyond its control.[483] This exception

applies as long as the institution exercised reasonable care to prevent the occurrence and it exercised such diligence as the circumstances required. Alternatively, the exception applies in a technical malfunction that the consumer knew about when the consumer attempted to initiate the transfer. Another section limits the damages that a court can award to a consumer. Where the failure was not intentional and resulted from a bona fide error, notwithstanding the institution's maintenance of procedures reasonably adapted to avoid the error, damages are limited to actual damages the consumer can prove.[484]

The second section that imposes liability on entities that fail to comply with the statute is broader than the first one in two respects. First, it imposes liability on parties in addition to the financial institution. Second, it has a more extensive damages provision. "Any person who fails to comply with any provision of [the EFTA] … is liable to such consumer in an amount equal to the sum of … any actual damage sustained by such consumer as a result of such failure."[485] A court also may award statutory damages of $100 to $1,000. There are limits on the amount of the award that can be made in class actions. If the consumer is successful, the court may award costs and a reasonable attorney's fee.

However, a person is not liable if that person "shows by a preponderance of evidence that the violation was not intentional and resulted from a bona fide error notwithstanding the maintenance of procedures reasonably adapted to avoid any such error."[486] In addition, a person is not liable if, before the consumer sues, the person notifies the consumer of the failure to comply with the statute, complies with its requirements, and makes an appropriate adjustment to the consumer's account as well as paying actual damages.[487] Finally, the EFTA includes a provision to deter certain consumer lawsuits. If the consumer is unsuccessful and the court finds the action was brought in bad faith or for purposes of harassment, the court can award attorney's fees to the defendant.[488]

Appendix E. Liability for violations of the NACHA rules

The NACHA Operating Rules include several provisions that benefit consumers beyond what is required in the EFTA or other statutes and regulations. For example, if a consumer believes that a transfer was unauthorized and complies with the rules' notification requirements, the institution must "promptly" credit the amount of the debit entry. Reg. E allows the institution to investigate for 10 business days before crediting the consumer's account. But under the NACHA rules, the consumer must notify the institution much sooner than Reg. E requires, 15 days rather than 60.[489]

However, the NACHA rules include a major limitation for consumers. The rules provide that "nothing in these Rules is intended to, and nothing in these Rules is implied to, give any legal or equitable right, remedy, or claim to … any Originator, Receiver …."[490] The intention of this provision, apparently, is to preclude consumers from bringing lawsuits based on a violation of the rules or to raise a violation of the rules as a defense when they are sued. Nevertheless, consumers may be able to raise a violation of the rules in litigation. For example, some bank agreements with consumers incorporate the NACHA rules.[491] If a financial institution violates the rules, the consumer may be able to successfully argue that the violation is a breach of the contract between the consumer and the institution.[492] Consumers may be able to successfully sue companies that violate the NACHA rules by alleging that the violation constitutes an unfair practice under the state's UDAP statute. The FTC and state attorneys general have brought suits claiming the violation of NACHA rules was an unfair practice.[493]

Appendix F: Federal laws prohibiting unfair, deceptive, and abusive acts or practices

The Federal Trade Commission Act prohibits unfair and deceptive acts or practices.[494] In a 1983 policy statement and its case law, the FTC has described the three elements of a deceptive act or practice: "(1) there must be a representation, practice, or omission likely to mislead consumers; (2) the consumers must be interpreting the message reasonably under the circumstances; and (3) the misleading effects must be 'material,' that is, likely to affect consumers' conduct or decision with regard to a product."[495]

An amendment to the FTC Act defines unfair acts or practices: the act or practice must cause or is likely to cause substantial injury; the injury is not reasonably avoidable; and declaring an act

or practice unfair is not outweighed by countervailing benefits to consumers or to competition.[496]

Whether other agencies besides the FTC can enforce the FTC Act's prohibition of unfair and deceptive acts and practices has become unclear since the adoption of the Dodd-Frank Act.[497]

Consumers have no private right of action under the FTC Act. However, they may be able to successfully use case law under the FTC Act when bringing lawsuits under their state UDAP statutes.

The CFPB has the authority to enforce the Dodd-Frank Act; consumers have no authority to do so. Dodd-Frank includes the prohibition of deceptive and unfair acts or practices. It does not define deceptive acts or practices, but the CFPB has applied the same definition as that used by the FTC.[498] Unfair acts or practices are defined the same way as under the FTC Act.[499] In addition, Dodd-Frank adds a new category: abusive acts or practices.[500] "Abusive" is defined as an act or practice that:

> (1) materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service; or (2) takes unreasonable advantage of:
>
> (A) a lack of understanding on the part of the consumer of the material risks, costs, or conditions of the product or service;
>
> (B) the inability of the consumer to protect the interests of the consumer in selecting or using a consumer financial product or service; or
>
> (C) the reasonable reliance by the consumer on a … person [subject to Dodd-Frank] to act in the interests of the consumer.

Although consumers have no private right of action under Dodd-Frank, they may be able to successfully use case law under the FTC Act when bringing cases for unfair and deceptive acts and practices under their state UDAP statutes. And perhaps courts also will consider CFPB enforcement actions since Dodd-Frank adopted the FTC's definition of deceptive acts and practices and Dodd-Frank includes the FTC Act's definition of unfair practices.[501] However, UDAP statutes, unlike Dodd-Frank, do not prohibit abusive acts and practices. Therefore, consumers and state attorneys general cannot use their UDAP laws to sue for abusive acts or practices.

Appendix G. State unfair and deceptive acts or practices statutes

States have enacted consumer protection laws prohibiting unfair and deceptive acts and practices (UDAP statutes). State attorneys general and other state government agencies can bring enforcement actions to stop this conduct. In every state except Iowa, consumers have a private right of action, so they also can seek to enforce UDAP laws.[502]

However, the UDAP statutes and court decisions in many states significantly restrict a consumer's ability to successfully enforce these laws. For example, under the UDAP laws of five states, consumers cannot recover their attorney's fees.[503] This is a significant barrier for consumers because, in most cases, each consumer suffers a relatively small monetary amount of damages. Consequently, they usually cannot afford to bring a lawsuit if they have to pay the attorney out of their own pockets even if they win. States that prohibit class actions also make most consumer lawsuits infeasible.[504] In two states, consumers who do not win their UDAP lawsuit must pay thousands of dollars to the business they sued even when they filed their suit in good faith.[505] States have made it difficult for consumers to successfully pursue UDAP lawsuits by requiring them to prove their lawsuits are in the "public interest" and by incorporating the common law requirement that the consumer prove reliance on the seller's representations.[506] States carve out entire industries by exempting banks and most creditors.[507] Some states exempt all regulated industries.[508] Colorado, Indiana, Nevada, North Dakota, and Wyoming make it difficult even for the state attorney general to use the state's UDAP statute by providing that the attorney general can obtain an injunction and any other relief only by proving that the company engaged in unfair or deceptive practices knowingly or intentionally.[509]

Endnotes

[1] As used in this report, references to breaches of data security have the same meaning as when used in the state data breach notification laws that are analyzed in this report. Most of these laws are modeled after California's. That law that defines a breach as the "unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information." Cal. Civ. Code 1798(g). New York added a definition of "acquisition: The downloading, copying, or unauthorized using of information, including opening fraudulent accounts and identity theft." N.Y. Gen. Bus. Law 899-aa(1)(c). These laws are "sectoral," meaning they apply to specific types of companies. Mark Burdon, "Contextualizing the Tensions and Weaknesses of Information Privacy and Data Breach Notification Laws," 27 Santa Clara Computer & High Tech. L. J. 63, 83 (2010-2011). These laws are designed to "provide a particular remedy to a specific problem," Ibid, 86, adopting "market-based remedies that are conscious of the compliance requirements of data collecting organizations." Ibid, 88. In contrast, the law applicable to privacy invasions derives from the common law of torts. Ibid, 84. It grants "broad rights to individuals regarding the personal information exchange process," Ibid, 86, and focuses more on individual protections. Ibid, 88. It is not limited to specific types of firms and not restricted to a company's computerized data.

[2] Firms against which the Securities and Exchange Commission has brought administrative proceedings are filing constitutional challenges to the SEC's right to bring such proceedings. A federal District Court judge ordered a temporary halt to a pending SEC administrative proceeding in which the plaintiff contends administrative law judges must be appointed by the five commissioners, not by a unit within the SEC. The judge held the plaintiff had a "'substantial likelihood of success'" on his constitutional claim. Jean Eaglesham, "SEC Faces Block on In-House Judge," Wall St. J., June 9, 2015, at C1. Bebo v. Securities and Exchange Comm., 2015 WL 905349 (ED Wis. 2015) (case dismissed for lack of subject matter jurisdiction; plaintiff must bring challenge before administrative law judge; if unsuccessful, before the commission; if still unsuccessful, in the U.S. Court of Appeals). Mary P. Hansen, "SEC Faces New Constitutional Challenge to Administrative Proceedings Based on Tenure Protection of Administrative Law Judges," 2014 WLNR 29030538, National L. Rev., Oct. 17, 2014 (reporting on pending legal challenge in Securities and Exchange Comm. v. Stillwell). See Jean Eaglesham, "Overhaul of SEC Judge System Urged," Wall St. J., May 13, 2015, at C3 (reporting that the former SEC enforcement chief has called for changing the agency's current structure in which the commissioners decide which cases will be assigned to administrative law judges for trial and then decide whether to uphold the judge's decision when it is appealed to the commission). The SEC does not enforce the laws that regulate mobile payments. But if these challenges are ultimately successful, administrative proceedings brought by the agencies that do regulate mobile payments may be struck down as well.

[3] The prudential regulators and the financial institutions they regulate are as follows: Office of Comptroller of the Currency (OCC) – national banks; Federal Reserve Board (FRB) – state chartered banks that are members of the Federal Reserve system; Federal Deposit Insurance Corp. – state chartered banks that are not members of the Federal Reserve system; National Credit Union Administration – credit unions.

[4] "Financial product or service" is defined, inter alia, as "(i) extending credit and servicing loans … (iv) engaging in deposit-taking activities, transmitting or exchanging funds, or otherwise acting as a custodian of funds or any financial instrument for use by or on behalf of a consumer; (v) selling, providing, or issuing stored value instruments, except that, in the case of a sale of, or transaction to reload, stored value, only if the seller exercises substantial control over the terms or conditions of the stored value provided to the consumer … (vii) providing payments or other financial data processing products or services to a consumer by any technological means, including processing or storing financial or banking data for any payment instrument, or through any payments systems or network used for processing payments data, including payments made through an online banking system or mobile telecommunications network, except that a person shall not be deemed to be a covered person with respect to financial data processing solely because the person - (I) is a merchant, retailer, or seller of any nonfinancial good or service who engages in financial data processing by transmitting or storing payments data about a consumer exclusively for purpose of initiating payments instructions by the consumer to pay such person

for the purchase of, or to complete a commercial transaction for, such nonfinancial good or service sold directly by such person to the consumer." 12 USC 5481(15).

[5] 12 USC 5516(d). "The prudential regulator is authorized to enforce the requirements of Federal consumer financial laws and, with respect to a covered person … shall have exclusive authority (relative to the Bureau) to enforce such laws." 5516(d)(1). "When the Bureau has reason to believe that a person has engaged in a material violation … the Bureau shall notify the prudential regulator … and recommend appropriate action to respond." 5516(d)(2)(A). "The prudential regulator shall provide a written response to the Bureau not later than 60 days thereafter." 5515(d)(2)(B).

[6] In a case against a credit card company service provider, the CFPB subjected the company to its supervision for the first time as part of its enforcement action. In the Matter of Continental Finance Co., No. 2015-CFPB-0003 (Consent Order, Feb. 4, 2015). The prudential regulators also have enforcement authority over the third-party service providers used by banks under their authority.

[7] "Memorandum of Understanding between the Consumer Financial Protection Bureau and the Federal Trade Commission," March 6, 2015. Available at www.ftc.gov. "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." Catherine M. Sharkey, "Agency Coordination in Consumer Protection," 2013 U. Chi. Legal F. 329, 337 (2013). "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." Ibid, 337 n. 36.

[8] 12 CFR 1026.2(a)(15)(i).

[9] Interpretation 12 CFR 1026.2(a)(15) -2(ii)(C). Underlining added.

[10] Munoz v. Seventh Ave., 2004 WL 1593906, *4 (ND Ill. 2004), noted in Diane E. Thompson & Elizabeth Renuart, *Truth in Lending* 344 (9th ed., 2015).

[11] Thompson and Renuart, Ibid.

[12] Ibid.

[13] 12 CFR 1026.12.

[14] 12 CFR 1005.2(a)(1). "Electronic fund transfer" is defined as "any transfer of funds that is initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer's account. The term includes, but is not limited to – (i) Point-of-sale transfers; (ii) Automated teller machine transfers; (iii) Direct deposits or withdrawals of funds; (iv) Transfers initiated by telephone; and (v) Transfers resulting from debit card transactions, whether or not initiated through an electronic terminal." 1005.3(b).

[15] 12 CFR 1005.2(a)-1 Official staff interpretations. Italics in original. Underlining added.

[16] Lauren K. Saunders et al., *Consumer Banking and Payments Law* 144 (5th ed. 2013) (hereafter "Saunders"). See Benjamin Geva, *The Law of Electronic Funds Transfers*, 6-80 (2014) ("Central to EFTA and Regulation E are the definitions of 'access device' and 'electronic fund transfer.' Both definitions contemplate the use of computers and telephones to access funds in a consumer's access account to make payments.").

[17] 12 CFR 1005.5. Categorizing mobile phones as access devices may also pose difficulties for consumers. Reg. E provides that in order to limit their liability for unauthorized transfers, consumers must report, within specified periods of time, the loss or theft of an access device to the financial institution with which they have their debit card account. 12 CFR 1005.6(b). Consumers are unlikely to realize this reporting requirement applies to loss or theft of a mobile phone as well as to a lost or stolen debit card. Comments of National Consumer Law Center,

California Asset Building Coalition, California Reinvestment Coalition, Consumer Action, Consumer Federation of America, National Association of Consumer Advocates to the Consumer Financial Protection Bureau on Request for Information Regarding Mobile Financial Services, Docket No. CFPB-2014-0012, Sept. 10, 2014, at 8 (hereafter cited as NCLC et al. Comments to CFPB). This report sometimes uses the term "bank" in regard to the EFTA and Reg. E and sometimes uses the term "financial institution." When this report uses the term "bank" in connection with the EFTA and Reg. E, it refers to those entities that the laws call "financial institutions" and that are defined as "a bank, savings association, credit union, or any other person that directly or indirectly holds an account belonging to a consumer, or that issues an access device and agrees with a consumer to provide electronic fund transfer services." 12 CFR 1005.2(i).

[18] The FTC has studied the disclosures made in mobile shopping apps. "What's the Deal? An FTC Study on Mobile Shopping Apps" (Aug. 1, 2014) (hereafter "FTC Study"). The FTC found the mobile apps did not clearly inform consumers of their rights and liability limits for unauthorized, fraudulent, or erroneous transactions and how the apps collect, use, and share information about customers. The FTC urged companies to take advantage of technological advances built into many smartphones that provide the potential for strong data security.

[19] Companies can be liable for actual and statutory damages for violating the disclosure laws regulating credit cards, 15 USC 1640, and debit cards, 15 USC 1693m. In light of the disclosure inadequacies the FTC discovered, there may be violations of the FTC Act and state laws prohibiting unfair and deceptive practices. See FTC Study, supra note 10.

[20] "Solicitation" is defined as "an offer by the card issuer to open a credit or charge card account that does not require the consumer to complete an application." 12 CFR 1026.60(a)(1). Issuance of unsolicited credit cards is prohibited. The credit card may not be issued except "in response to an oral or written request or application for the card" or as a renewal of, or substitute for, a card that the consumer has already accepted. 12 CFR 1026.12(a).

[21] 15 USC 1632(a). For credit cards, TILA generally permits the consumer to collect both actual and statutory damages. However, some courts have held that consumers cannot collect statutory damages for violation of the section requiring disclosures to be clear and conspicuous. But see Barrer v. Chase Bank, 2011 WL 11421 (D. Or. 2011); Thompson & Renuart, supra at 836.

[22] 15 USC 1632(a); e.g., "finance charge" and "annual percentage rate."

[23] 12 CFR 1026.60(b).

[24] E.g., 12 CFR 1026.5(a)(3) & 1026.60(a)(2).

[25] E.g., Barrer v. Chase Bank, 2011 WL 11421 (D. Or. 2011).

[26] UCC 1-201(10).

[27] 15 USC 1665e, 12 CFR 1026.51(a)(1)(i).

[28] 15 USC 1665e, 12 CFR 1026.51(a)(1)(ii).

[29] 15 USC 1637(c)(8)(A), 12 CFR 1026.51(b)(1).

[30] 12 CFR 1026.51(b)(1)(ii).

[31] 12 CFR 1026.51(b)(1)(i).

[32] 15 USC 1681b(c)(1)(B)(iv).

[33] 15 USC 1650(f)(2). Some card issuers are able to get around this provision by contacting students via email and the Internet. Eboni Nelson, "The CARD Act and Young Consumer Protection: Two Years Later," 31 Banking & Fin. Services Pol'y Rep. 12, 15 (2012).

[34] 15 USC 1650(f)(1).

[35] 12 CFR 1026.5(a)(1)(iii).

[36] 12 CFR 1026.60(c)(2).

[37] Official interpretation 12 CFR 1026.60(a)(2)-6.i.

[38] If the consumer accesses an application or solicitation from a terminal or kiosk at the card issuer's office, the issuer has the option of providing the disclosures in either paper or electronic form. Ibid, 1026.60(a)(2)-6.ii.

[39] 12 CFR 1026.5(a)(1)(iii). E-Sign is at 15 USC 7001 et seq. Reg. Z provides that generally the manner in which a company makes TILA disclosures electronically must comply with E-Sign. However, Reg. Z makes an exception in regard to disclosures required with a solicitation or application to open a credit card account. In those situations, the issuer is not required to comply with E-Sign. 12 CFR 1026.5(a)(1)(iii).

[40] 12 CFR 1005.4(a). The official staff interpretation provides: "Although no particular rules govern type size, number of pages, or the relative conspicuousness of various terms, the disclosures must be in a clear and readily understandable written form that the consumer may retain." 12 CFR 1005.4-4(a).

[41] 12 CFR 1005.7(a).

[42] 12 CFR 1005.7(b).

[43] 205 Ill. Comp. Stat. 616/10 & 616/46. The following must be disclosed before the card is purchased: the card purchase fee, monthly maintenance fee, cash withdrawal fee at an ATM and cash advance fee at retail locations, reload fee, and balance inquiry fee. Ibid, 616/46(b)(1).The latter fee need not be disclosed if the balance is available without cost from a telephone or Internet access. In addition, the following disclosures that the consumer can use to obtain information about fees must be made on the card: the expiration date, if any, and a toll-free number and the Internet website, if the issuer has one. A toll-free number and Internet website address also must be disclosed in order for the consumer to obtain a replacement card after the card expires if the underlying funds may be available after expiration. Ibid, 616/46(b)(2).

[44] 205 Ill. Comp. Stat. 616/46.

[45] Ibid.

[46] Montana, New Mexico, and South Carolina do not regulate money transmitters. "Imperfect Protection: Using Money Transmitter Law to Insure Prepaid Cards" The Pew Charitable Trusts (March 5, 2013) at 2 (hereafter referred to as "Imperfect Protection").

[47] 79 Fed. Reg. 77102, 77116 (Dec. 23, 2014). A study by The Pew Charitable Trusts found that "only 11 of the 45 states that had money transmitter laws included provisions covering stored-value products such as prepaid cards." Imperfect Protection, supra at 2.

[48] See infra text accompanying notes 174-78.

[49] 79 Fed. Reg. 77102, 77127. The FTC staff has expressed concern that at present no law protects consumers from liability for unauthorized charges when a consumer uses "a prepaid or gift card, or moves money into a stored value account within the app, to make a mobile payment transaction." Comments of FTC Staff before the Consumer Financial Protection Bureau, In the Matter of Request for Information Regarding the Use of Mobile Financial Services by Consumers and Its Potential for Improving the Financial Lives of Economically Vulnerable Consumers, Docket No. CFPB-2014-0012, Sept. 10, 2014, at 3.

[50] "The Bureau understands that the use of GPR prepaid products … to store and transfer funds via the internet, text, or mobile phone is growing." Ibid, 77104.

[51] The card issuer has the option of either following the regular periodic statement requirements of Reg. E or providing the information included in periodic statements by other means including an electronic history of account transactions that covers at least 18 months. Ibid, 77103.

[52] 79 Fed. Reg. 77102, 77110 (2014).

[53] Ibid, 77129. The CFPB calls a prepaid account feature on a mobile phone a "mobile wallet," which is a type of "digital wallet." Ibid, 77110. A prepaid account is defined as an account subject to Reg. E that is "a card, code, or other device … established primarily for personal, family, or household purposes, and which" (A) is either issued on a prepaid basis in a specific amount or not issued on a prepaid basis but capable of being loaded with funds thereafter; (B) is redeemable at multiple, unaffiliated merchants for goods or services, usable at ATMs, or for person-to-person transfers; and (C) is not a gift certificate or card, a loyalty, award, or promotional gift card or general-use prepaid card marketed that is both marketed and labeled as a gift certificate or card. Proposed Reg. Z, 1005.2(3).

[54] Proposed 12 CFR 1026.2(15). See generally, "Overdraft Frequency and Payday Borrowing," The Pew Charitable Trusts (Feb. 2015).

[55] The electronic disclosure must be provided "in a manner which is reasonably expected to be accessible in light of how a consumer is acquiring a prepaid account." 79 Fed. Reg. at 77170. The institution can provide both the short and long-form disclosures on the same or two different Web pages as long as the disclosures are "easy to locate." Ibid. The electronic disclosures must be made "using machine-readable text that is accessible via both Web browsers and screen readers." Ibid.

[56] Proposed 12 CFR 1005.19 (e).

[57] "If a financial institution principally uses a foreign language on prepaid account packaging material, by telephone, in person or on the Web site a consumer utilizes to acquire a prepaid account, the short-form and long-form disclosures … would have to be provided in that same foreign language. A financial institution would also have to provide the long form … in English upon a consumer's request and on any part of the Web site where it provides the long-form disclosure in a foreign language." 79 Fed. Reg. at 77175.

[58] Norman I. Silber, "Reasonable Behavior at the CFPB," 7 Brook. J. Corp. Fin. & Com. L. 87, 101 (2012).

[59] 15 USC 5481(14); 15 USC 5531.

[60] "The FDIC has affirmed its authority to prevent unfair and deceptive acts and practices generally under §8 of the FDI Act." Sharkey, supra at 337. In August 2014, the FDIC, FRB, CFPB, and National Credit Union Administration issued guidance in regard to one specific FTC rule. The Credit Practices Rule prohibited the use of certain provisions in consumer credit contracts, misrepresentation of the nature or extent of co-signer liability and the pyramiding of late fees. According to the guidance, "The authority to issue credit practices rules for banks, savings associations, and federal credit unions was repealed as a consequence of [Dodd-Frank]; however, institutions should not construe the repeal to indicate that the unfair or deceptive practices described in these former regulations are permissible. These practices remain subject to Section 5 of the [FTC] Act." "Unfair or Deceptive Acts or Practices (Regulation AA)," Board of Governors of the Federal Reserve System, 79 Fed. Reg. 51115 (Aug. 27, 2014); "Interagency Guidance Regarding Unfair or Deceptive Credit Practices," FDIC Financial Institution Letter, FIL-44-2014 (Aug. 22, 2014); and OCC Bulletin 2014-42 (Aug. 22, 2014). The CFPB's notice is available at www.consumerfinance.govhttp://www.consumerfinance.gov. The FRB went further in its guidance in a statement of its authority that appears to go beyond the Credit Practices Rule: "[T]he Board continues to have supervisory and enforcement authority regarding unfair or deceptive acts or practices under section 5 of the FTC Act and sections 1031 and 1036 of the Dodd-Frank Act." Ibid, 51116.

[61] .com Disclosures, FTC (March 2013).

[62] 75 Fed. Reg. 31665 (June 4, 2010). The statement is in connection with an amendment to Reg. E that applies to overdraft fees imposed on debit cards and ATM transactions.

[63] Restatement of the Law, Consumer Contracts, Preliminary Draft No. 1, Am. Law Institute 14 (Oct. 28, 2014) (hereafter cited as Consumer Contract Restatement). See Nancy S. Kim, *Wrap Contracts: Foundations and Ramifications* (2013) (analyzing clickwrap, browsewrap, and shrinkwrap contracts).

[64] For example, in West Virginia ex rel. U-Haul Co. v. Zakaib, 232 W. Va. 432, 752 SE2d 586 (Sup. Ct. App. 2013), the court held the lessor's wording of an online incorporation by reference clause was insufficient under state law.

In Comb v. PayPal, 218 F. Supp 2d 1165 (ND Cal. 2002), the court assumed the consumers assented to the clickwrap contract, but found the arbitration clause unconscionable. In regard to the sale of goods, the Uniform Commercial Code does not define "unconscionability," but the official comment states: "The principle is one of prevention of oppression and unfair surprise and not of disturbance of allocation of risks because of superior bargaining power. The basic test is whether, in light of the general commercial background and commercial needs of the particular trade or case, the term or contract involved is so one-sided as to be unconscionable." UCC, Official Comment to 2-302. The Restatement (Second) of Contracts states that the determination of unconscionability "is made in the light of its setting, purpose and effect." Sec. 208. The Texas Supreme Court recently repeated language found in numerous cases when it said "Unconscionability … is not easily defined. The term defies a precise legal definition because 'it is not a concept, but a determination to be made in light of a variety of factors not unifiable into a formula.'" Venture Cotton Cooperative v. Freeman, 435 SW2d 222, 228 (Tex. Sup. Ct. 2014). Hundreds of American cases quote a description of an unconscionable contract from a 1750 English case: a contract "such as no man in his senses and not under delusion would make on the one hand, and as no honest and fair man would accept on the other." AMS Staff Leasing v. Taylor, 2015 WL 71705, *4 (D. Ct. App. Fla 2015).

[65] FTC v. Direct Benefits Group, 2013 WL 3771322 (MD Fla. 2013).

[66] For example, in Caspi v. The Microsoft Network, 323 NJ Super 118, 732 A2d 528 (Super Ct. NJ 1999), the court examined the size and placement of the challenged forum selection clause and the style and mode of presentation. The court satisfied itself that there was no basis for concluding that the clause was presented in such a way as to conceal or de-emphasize it. Even if consumers clearly assent to be bound to contract terms and those terms are easily accessible, few consumers may actually read the contracts. One study found that only one or two of every 1,000 persons purchasing retail software online accessed the license agreement, and those who did access it read only a small portion. The researchers attributed the low numbers to the cost of comprehending the terms. Yannis Bakos, Florencia Marotta-Wurgler, & David Trossen, "Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts," 43 J. Legal Studies 1 (2014).

[67] U-Haul v. Zakaib, at 232 W. Va. 440, 752 SE2d 594.

[68] Be In, Inc., v. Google, Inc., 2013 WL 5568706 (ND Cal. 2013).

[69] Nguyen v. Barnes & Noble, 763 F.3d 1171, 1175 (9th Cir. 2014), quoting Specht v. Netscape, 306 F.3d 17, 29 (2d Cir. 2002).

[70] Van Tassell v. United Mktg Group, 795 F. Supp 2d 770, 790 (ND Ill. 2011). "Constructive knowledge is defined as '[k]nowledge that one using reasonable care or diligence should have, and that is attributed by law to a given person.'" (citing Black's Law Dictionary) Morris-Schindler, LLC v. City and County of Denver, 251 P2d 1076, 1083 (Colo. Ct. App. 2010).

[71] Fteja v. Facebook, 841 F. Supp 2d 829 (SD NY 2012); Zaltz v. JDATE, 952 F. Supp 2d 439, 451-52 (EDNY 2013).

[72] Nguyen v. Barnes & Noble, 763 F.3d at 1175, 1177.

[73] Hines v. Overstock.com, 668 F. Supp 2d 362, 367 (ED NY 2009) (user could not see the link without scrolling to the bottom of the screen). Pollstar v. Gigmania Ltd., 170 F. Supp 2d 974, 981 (ED Cal. 2000) (textual notice was in small gray print against a gray background); Van Tassell, 795 F. Supp 2d at 792.

[74] Nguyen v. Barnes & Noble, 763 F.3d at 1177.

[75] Specht v. Netscape, 306 F.3d 17, 23 (2d Cir. 2002) (terms visible only by scrolling down to next screen).

[76] The 2d Circuit noted "the breadth of the range of technological savvy of online purchasers." Nguyen v. Barnes, 763 F.3d at 1179.

[77] Ibid, 1177; Be In, Inc., v. Google, Inc., at *7. "Negligence is defined as the doing of some act that a reasonably prudent person would not do or the failure to do some act that a reasonably prudent person would do under the same or similar circumstances." Benton v. Diamond Services, 16 F.3d 1215, *2 (5th Cir. 1994).

[78] Nguyen v. Barnes & Noble, 763 F.3d at 1177.

[79] Margaret Jane Radin, "Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law 11" (2013). See generally, Florencia Marotta-Wurgler, "Are 'Pay Now, Terms Later' Contracts Worse for Buyers? Evidence from Software License Agreements," 38 J. Legal Studies 309 (2009) (comparing the terms of online rolling license agreements with those whose terms are disclosed prior to purchase).

[80] Hill v. Gateway 2000, 105 F.3d 1147 (7th Cir. 1997); ProCD v. Zeidenberg, 86 F.3d 1447 (7th Cir. 1996). Both decisions were decided by the same judge. ProCD was a commercial transaction; it did not involve any consumers.

[81] Klocek v. Gateway, 104 F. Supp 2d 1332 (D. Kan. 2000). Other cases following the reasoning of the Klocek case include Bowdoin v. Showell Growers, 817 F.2d 1543 (11th Cir. 1987); Sanco v. Ford Motor Co., 771 F.2d 1081 (7th Cir. 1985). "An empirical study of all published and unpublished [rolling contract] cases involving consumer contracts in federal and state courts contracts" found that "[a]bsent intervening factors such as fraud or unconscionability, courts have enforced [rolling contracts] in 76 percent of the cases … as long as the requirements of notice and opportunity to review and to reject, were met. … Restricting analysis to the state supreme and appellate-court cases ... [rolling contracts] have been enforced in a slight majority, 56 percent." Restatement of the Law Consumer Contracts, Preliminary Draft No. 2, 26—28 (Oct. 20, 2015).

[82] ProCD, 86 F.3d at 1453.

[83] Ibid, 1452. (Italics in original.)

[84] See generally, James J. White, "Warranties in the Box," 46 San Diego L. Rev. 733, 740-41 (2009) (Buyers who paid for and received goods reasonably believe they own the goods. To hold that legally the buyer accepts subsequent terms contradicts reasonable expectations); Roger C. Bern, "'Terms Later' Contracting: Bad Economics, Bad Morals, and a Bad Idea for a Uniform Law, Judge Easterbrook Notwithstanding," 12 J.L. & Pol'y 641, 744-45 (2004) (sellers can have no reasonable expectation that use of the goods signals buyer's agreement with adverse terms). In ProCD, the license terms appeared on the screen every time the buyer ran the software program. ProCD, 86 F.3d at 1450.

[85] Brower v. Gateway 2000, 246 AD2d 246, 251, 676 NYS2d 569, 572 (NY Sup. Ct. 1998).

[86] Hill, 105 F.3d at 1150. A Comment in the American Law Institute's Preliminary Draft No. 1 of its restatement of the law of consumer contracts states that a restocking fee of 15 percent would not be part of the contract because it "unreasonably encumbers the right to terminate." Consumer Contract Restatement, supra at 12. The Reporter's Notes state that the cost of exercising the right to reject "must not be too large." Ibid, 14.

[87] See e.g., Bischoff v. DirectTV, Inc., 180 F. Supp 2d 1097, 1101-02 (CD Cal. 2002) (contract for satellite TV service, opportunity to cancel service after review of terms). Noted in Clayton P. Gillette, "Rolling Contracts as an Agency Problem," 2004 Wis. L. Rev. 679, 681 n. 12 (2004). American Law Institute "Reporters," in drafting a Restatement of the Law of Consumer Contracts, conducted a study of "shrinkwrap" cases decided after ProCD and Hill. It is not clear whether the study includes the type of rolling contract involved in mobile payments in which software is loaded onto the mobile device and terms supplied later are disclosed in an electronic medium. According to the study, before ProCD was decided, almost half of the 11 cases enforced shrinkwrap agreements. After ProCD, 50 out of 61 (82 percent) of the courts enforced them. Clearly, most courts enforce that type of rolling contract. However, there was no breakdown identifying which courts were included in the study. Consequently, we do not

know, for example, which cases were decided by the highest appellate court in the state, a decision having state-wide application, and which by a single trial-level judge, a decision with limited application within a state. In addition, we do not know which cases were decided by federal courts that were guessing how the state's highest court would decide based on that state's law. The federal courts' decisions are guesses because it would be highly unusual for a state court to have decided a rolling contract case involving the same facts as the case before the federal court. Consequently, the federal courts try to predict how the court in that state would apply that state's common law to the unique circumstances in the cases before them.

[88] Alan S. Kaplinsky & Mark J. Levin, "Consumer Arbitration: If the FAA 'Ain't Broke,' Don't Fix It," 63 Bus. Law. 907 (2008).

[89] See "Banking on Arbitration: Big Banks, Consumers, and Checking Account Dispute Resolution," The Pew Charitable Trusts (Nov. 27, 2012) at 7.

[90] Judith Resnick, "Diffusing Disputes: The Public in the Private of Arbitration, the Private in Courts, and the Erasure of Rights," 124 Yale L. J. (2015 (forthcoming) available at www.SSSRN.com/abstract=2601132 (posted May 2015); Richard M. Alderman, "What's Really Wrong with Forced Consumer Arbitration?" Bus. Law Today 1 (Nov. 2010); Richard M. Alderman, "Pre-Dispute Mandatory Arbitration in Consumer Contracts: A Call for Reform," 38 Hous. L. Rev. 1237 (2002). See F. Paul Bland, Jr., et al., *Consumer Arbitration Agreements* 3-4 (7th ed. 2015); Jean R. Sternlight, "The Rise and Spread of Mandatory Arbitration as a Substitute for the Jury Trial," 38 U.S.F.L. Rev. 17 (2003). One disadvantage of mandatory consumer arbitration is that many lawyers refuse to represent consumers whose contracts contain arbitration clauses. Arbitration Study, supra at Section 6, at 4-5.

[91] Bland, supra at 4-5, 85-86, 178-180, 304-05. Alan S. Kaplinsky, Mark J. Levin, & Martin C. Bryce, Jr., "2014 Arbitration Developments: Courts Continue to Apply *Concepcion* and *Italian Colors*," 70 Bus. Law. 649, 650-56 (2015).

[92] Nguyen v. Barnes & Noble, 763 F.3d 1171 (2d Cir. 2014); Schnable v. Trilegiant Corp., 697 F.3d 110 (2d Cir. 2012).

[93] 12 USC 1028(a); Arbitration Study, Report to Congress, Pursuant to Dodd-Frank Wall Street Reform and Consumer Protection Act, CFPB (March 2015) (hereafter cited as Arbitration Study); Arbitration Study Preliminary Results, CFPB (Dec. 12, 2013).

[94] Rottner v. AVG Tech, USA, 943 F. Supp 2d 222, 230 (D. Mass. 2013). UCC Art. 2 "applies to transactions in goods." 2-102. "Goods" are defined as "all things … which are movable at the time of identification to the contract." 2-105. But see Holly K. Towle, "Enough Already: It Is Time to Acknowledge that UCC Article 2 Does Not Apply to Software and Other Information," 52 S. Tex. L. Rev. 531 (2011). Three states have enacted laws providing that UCC Article 2 does not apply to software. Ibid, 568-69.

[95] Simulados Software Ltd. v. Photon Infotech Private, Ltd., 40 F. Supp 3d 1191, 1199 (ND Cal. 2014). Most courts have decided that the UCC applies to mass-produced standardized software and software that is generally available. Ibid.

[96] E.g., express warranties, UCC 2-313; implied warranties of merchantability and usage of trade, UCC 2-314. These sections refer to sellers, not licensors or licensees. The statute of frauds provision, UCC 2-201, applies to a contract for the sale of goods, not to licenses.

[97] E.g., FTC v. Direct Benefits Group, 2013 WL 3771322 (MD Fla. 2013).

[98] E.g., FTC v. Direct Benefits Group, 2013 WL 3771322 (MD Fla. 2013); Press Release, U.S. Consumer Fin. Prot. Bureau, "Federal Deposit Insurance Corporation and Consumer Financial Protection Bureau Order Discover to Pay $200 Million Consumer Refund for Deceptive Marketing" (Sept. 24, 2012); Press Release, U.S. Consumer Fin. Prot. Bureau, "CFPB Probe into Capital One Credit Card Marketing Results in $140 Million Consumer Refund" (July 18, 2012); Press Release, "U.S. Consumer Fin. Prot. Bureau, CFPB Orders Chase and JPMorgan Chase to Pay $309 Million Refund for Illegal Credit Card Practices" (Sept. 19, 2013).

[99] "Marketing of Credit Card Add-on Products," CFPB Bulletin 2012-06 (July 18, 2012).

[100] CARD Act Report, CFPB (Oct. 1, 2013) at 76.

[101] Carolyn L. Carter & Jonathan A. Sheldon, *Unfair and Deceptive Acts and Practices* (8th ed. 2012). Examples include exempting regulated industries, Ibid, 81-102, prohibiting class actions, Ibid, 770, imposing a "public interest" test, Ibid, 651-66, and requiring the consumer to prove reliance, Ibid, 225-27.

[102] Ackerberg v. Citicorp USA, 898 F. Supp 2d 1172 (ND Cal. 2012).

[103] E.g., Martin v. Wells Fargo Bank, 2013 WL 6236762 (ND Cal. 2013) (bank did not meet its burden to prove that it mailed notice of modification or that consumer saw the modification on its website); in re Zappos.com, 893 F. Supp 2d 1058 (D. Nev. 2012) (modification not enforceable where hyperlink to modification was inconspicuous). See also Van Tassell v. United Mktg. Grp., 795 F. Supp 2d 770 (ND Ill. 2011); Koch Indus. v. Does, 2011 WL 1775765 (D. Utah 2011); Hines v. Overstock.com, 668 F. Supp 2d 362 (ED NY 2009) aff'd 380 Fed. Appx. 22 (2d Cir. 2010).

[104] .com Disclosures, "How to Make Effective Disclosures in Digital Advertising," FTC (March 2013).

[105] Mobile phones now come in a variety of shapes as well as sizes. "Making an app display well on a plethora of screen shapes and sizes is not easy. … A button may not show up, or appear only partially on the screen." Penny Crosman, "3 Mobile App Problems and How to Fix Them," Am. Banker, Aug. 6, 2013, at 7.

[106] "FTC Permanently Shuts Down Notorious Rogue Internet Service Provider," Press Release, May 19, 2010, available at www.ftc.gov.

[107] For more information about NACHA, see: https://www.nacha.org/about

[108] 12 CFR 1026.6.

[109] 15 USC 1637(a).

[110] 15 USC 7001(c)(1). See 72 Fed. Reg. 63,462, 63,468 (Nov. 9, 2007). See Margot Saunders, "A Case Study of the Challenge of Designing Effective Electronic Consumer Credit Disclosures: The Interim Rule for the Truth In Lending Act," 7 N.C. Banking Inst. 39 (2003) (describing problems consumers may encounter when disclosures are delivered electronically). See generally, Saunders, supra at ch. 11.

[111] Official interpretation 12 CFR 1026.5(a)(1)-3;12 CFR 1026.5(a)(3)(iv); 12 CFR 1026.5(a)(3)(vii) & 12 CFR 1026.5(a)(3)(viii).

[112] See generally, Martin v. Wells Fargo Bank, 2013 WL 6236762 (ND Cal. 2013) (bank did not meet its burden to prove that it mailed notice of modification or that consumer saw the modification on its website).

[113] 12 CFR 1026.12(b)(2)(iii). In Crestar Bank v. Cheevers, 744 A2d 1043 (DC 2000), the court held this requirement was not satisfied where the machines consumers used to buy Amtrak tickets with credit cards provided no means to identify the cardholder, such as a signature or photograph. Although TILA provides the consumer is not liable for unauthorized use unless this condition is satisfied, the courts are not in agreement as to whether the statute provides consumers with the right to sue the creditor for damages. Thompson & Renuart, supra at 490.

[114] Official staff interpretation, 12 CFR 1026.12 (b)(1)(iii)-1 (italics supplied).

[115] Ibid. 1026.12 (b)(2)(iii)-2.

[116] Ibid. 1026.12 (b)(2)(iii)-3.

[117] These procedures are described in the Stage 3 portion of this report, text accompanying notes 447-64.

[118] Daisuke Wakabayashi & Robin Sidel, "Fraud Takes Bite Out of Apple Pay," Wall St. J, B4 (March 4, 2015). The information includes "the type of phone, the last four digits of the user's phone number and the user's general location to the bank that issued the card." Ibid.

[119] Ibid.

[120] 15 USC 1681c(g).

[121] Shlahtichman v. 1-800 Contacts, 615 F.3d 794 (7th Cir. 2010) cert. denied, 131 S. Ct. 1007 (2011). See Simonoff v. Kaplan, 2010 WL 4823597 (SD NY 2010) (discussing legislative history).

[122] Grabein v. 1-800-Flowers, 2008 WL 343179 (SD Fla. 2008); Vasquez-Torres v. Stubhub, 2007 U.S. Dist. LEXIS 63719 (CD Cal 2007).

[123] 12 CFR 1026.41(c); official interpretation, 12 CFR 1026.41(c)-3; 12 CFR 1026.8. The disclosures include the beginning balance, amount and date of each credit extension, the periodic rate expressed as an annual percentage rate, the finance charge, the total of other charges, when the payment is due, minimum payment requirements, late payment fees, and the creditor's address for registering a dispute.

[124] 15 USC 7001(c)(1)(B) & 7001(c)(1)(C).

[125] Pub. L. No. 111-24, 123 Stat. 1734 (May 22, 2009).

[126] CARD Act Report, CFPB (Oct. 1, 2013) at 8.

[127] 15 USC 1666b(a). 12 CFR 1026.5(2)(ii)(A)(1).

[128] 15 USC 1666c(a); 12 CFR 1026.10(b)(1); 15 USC 1666c(a).

[129] 12 CFR 1026.10(e); 12 CFR 1026.53(a).

[130] 12 CFR 1026.52(a) (total fees during first year may not exceed 25 percent of account's credit limit).

[131] 15 USC 1637(a)(7), 12 CFR 1026.9(a).

[132] 12 CFR 1026.9(b).

[133] 15 USC 1637(i)(1); 15 USC 1637(i)(2).

[134] 12 CFR 1026.7(b)(7).

[135] Carolyn L. Carter, Andrew G. Pizor, & Jonathan Sheldon, *Consumer Credit Regulation* 8 (1st ed. 2012).

[136] Marquette Nat'l Bank v. First of Omaha Service Corp., 439 US 299 (1978). See Smiley v. Citibank, 517 US 735 (1996) (extending Marquette to late fees allowed by issuer's home state).

[137] Penny Crosman, "Banks Experiment with Apps for the Underbanked," 2014 WL 26359015 (Sept. 23, 2014).

[138] 12 CFR 1005.3(b)(1).

[139] 12 CFR 1005.3(c)(6).

[140] Saunders, supra at 150, interprets the provision to refer to "a telephone call."

[141] Ibid.

[142] 12 CFR 1005.4(a)(1).

[143] Official interpretation 12 CFR 1005.4(a)-1.

[144] 12 CFR 1005.7(a).

[145] 12 CFR 1005.7(b).

[146] 12 CFR 1005.8(a)(1).

[147] 15 USC 1693(a)(7).

[148] 15 USC 1639d(c); 12 CFR 1005.9(b).

[149] 12 CFR 1005.9(b).

[150] 12 CFR 1005.4(a)(1). See 72 Fed. Reg. 63,452, 63,456 (Nov. 9, 2007). See generally, Saunders, ch. 11.

[151] See generally, Martin v. Wells Fargo Bank, 2013 WL 6236762 (ND Cal. 2013) (bank did not meet its burden to prove that it mailed notice of modification or that consumer saw the modification on its website).

[152] 2015 NACHA Operating Rules & Guidelines, Rule 1.4.4. Rule 1.4.4 states: "A record that is required by these Rules to be signed or similarly authenticated may be signed with an Electronic Signature in conformity with the terms of [E-Sign] including the provisions that reference state versions of [UETA]" (hereafter NACHA Rules). E-Sign section 7002 references UETA. That section provides an "exemption to pre-emption" for UETA, but does so in language that commentators have found extremely confusing. "Looked at as a whole, Section 7002 is a shockingly bad piece of work. Indeed, the more one ponders this section, the more it seems to be gibberish and nonsense." Jean Braucher, "Rent-Seeking and Risk Fixing in the New Statutory Law of Electronic Commerce: Difficulties in Moving Consumer Protection Online," 2001 Wis. L. Rev. 397, 557 (2001). Most important is whether the consumer consent requirements of section 7001(c) of E-Sign apply in states that have enacted E-Sign. While Braucher believes E-Sign's consumer consent requirements definitely still apply, Ibid, 560, Meehan and Beard think it is uncertain if they apply. Shea C. Meehan & D. Benjamin Beard, "What Hath Congress Wrought: E-Sign, the UETA, and the Question of Preemption," 37 Idaho L. Rev. 389, 406 (2002). Unlike the EFTA, which is a consumer protection law, and E-Sign, whose consumer consent requirements are intended to benefit consumers, UETA "has no specific consumer protections." Ibid. Sommer contends provisions on parties agreeing to conduct transactions by electronic means, variation by agreement and attribution disadvantage consumers. Jared Sommer, "Electronic Signatures and the UETA: E-Commerce in an Insecure E-World," 37 Idaho L. Rev. 507, 512, 514-15, 524 (2001).

[153] "Record" is defined as "information that is inscribed on a tangible medium or that is stored in an Electronic or other medium and is retrievable in perceivable form." NACHA Rule 8.85.

[154] NACHA Rule 1.4.2.

[155] NACHA Rule 1.4.3.

[156] NACHA Rules 2.5.17.1, 2.5.17.2.

[157] Ibid., NACHA Rule 2.5.17.4; Saunders, supra at 153.

[158] NACHA Rule 1.9.

[159] 12 CFR 1005.9(a). The receipt requirement does not apply if the amount of the transfer is $15 or less. 1005.9(e).

[160] 15 USC 1693a(8); 12 CFR 1005.2(h).

[161] 12 CFR 1005.2(h)-1)(ii).

[162] Susan Pandy, "Update on the U.S. Regulatory Landscape for Mobile Payments, Summary of Meeting Between Mobile Payments Industry Workgroup (MPIW) and Federal and State Regulators," at 13 (Fed'l Reserve Bank of Boston, Aug. 18, 2014).

[163] 15 USC 1681c(g).

[164] Shlahtichman v. 1-800 Contacts, 615 F.3d 794 (7th Cir. 2010) cert. denied, 131 S. Ct. 1007 (2011); Simonoff v. Kaplan, 2010 WL 4823597 (SD NY 2010).

[165] See generally, "Loaded with Uncertainty: Are Prepaid Cards a Smart Alternative to Checking Accounts?" The Pew Charitable Trusts (Sept. 6, 2012) (hereafter referred to as "Loaded with Uncertainty").

[166] See Saunders, supra at 193 & 263.

[167] 79 Fed. Reg., 77102, 77103.

[168] "The [Consumer Financial Protection] Bureau understands that the only credit features being offered on prepaid cards currently are structured as overdraft services." "Prepaid Accounts Under the Electronic Fund Transfer Act (Regulation E) and the Truth in Lending Act (Regulation Z)," Proposed Rule; request for public comment, 79 Fed. Reg. 77102, 77111 (Dec. 23, 2014).

[169] The CFPB defines a nonbank as "a company that offers consumer financial products or services, but does not have a bank, thrift, or credit union charter and does not take deposits." www.consumerfinance.gov/blog/category/explainer.

[170] "Entities like Square, Intuit, Google, and PayPal process debit, credit, and prepaid card payments to payees." Saunders, supra at 194. "Users who sign up for PayPal accounts can fund them from any bank account they choose —or … use a store-bought MoneyPak from Green Dot Corp." Sean Sposito, "PayPal Partnering with Banks to Attract New Customers," 2012 WLNR 3310941, Am. Banker, Feb. 16, 2013.

[171] Saunders, supra at 193.

[172] Ibid.

[173] E.g., "Consumer Financial Protection Bureau Takes Action against PayPal for Illegally Signing Up Consumers for Unwanted Online Credit," CFPB Press Release, May 19, 2015, available at www.consumerfinance.gov.

[174] See generally, Imperfect Protection, supra.

[175] Cal. A.B. 2789 (2010).

[176] Saunders, supra at 227.

[177] Ibid, 229.

[178] The states are Montana, New Mexico, and South Carolina. Imperfect Protection, supra at 3.

[179] Truth in Billing Policy, www.fcc.gov/encyclopedia/truth-billing. Section 64.2401 provides that "a telephone company's bill must: (1) provide a brief, clear, non-misleading, plain language description of the service or services rendered to accompany each charge; (2) identify the service provider associated with each charge; (3) clearly and conspicuously identify any change in service provider; (4) contain full and non-misleading descriptions of charges; (5) identify those charges for which failure to pay will not result in disconnection of the customer's basic local service; (6) provide a toll-free number for customers to call in order to lodge a complaint or obtain information; (7) place charges from third parties that are not telephone companies in a distinct section of the bill, separate from telephone company charges; and (8) provide a separate subtotal for third-party charges in the separate bill section and on the payment page. Telephone companies also must notify consumers, on their websites and at the point of sale, of any options they offer to block charges from third parties that are not telephone companies." Ibid.

[180] See Committee on Commerce, Science, and Transportation, U.S. Senate, Office of Oversight and Investigations, Majority Staff Report, "Unauthorized Charges on Telephone Bills," July 12, 2011 (reporting that thousands of consumers have complained about cramming to the FTC and the FCC).

[181] In the Matter of Empowering Consumers to Prevent and Detect Billing for Unauthorized Charges ("Cramming"), CG Docket No. 11-116, Reply Comment of the Federal Trade Commission, July 20, 2012, available at www.ftc.gov. "The FTC recommends that wireless providers be required to offer consumers the ability to block third-party charges and to make this option clear to consumers so that consumers are empowered to avoid any possibility of unauthorized third party charges." Ibid, 7. This should be done "by law or regulation to ensure that consumers have baseline protection." Ibid, 12. The FTC recommended a ban on or default blocking of third-party charges on landline bills because they are usually fraudulent. But the FTC did not recommend such strong measures for wireless bills because, in addition to cramming, they are used for legitimate purposes such as mobile payments. Ibid, 11-12. See also the statement to the CFPB by consumer advocates pointing out that FCC law sets no limits on

consumer liability for unauthorized charges and contains no "strong dispute rights." NCLC et al. Comments to CFPB, supra at 7.

[182] Press Release, "T-Mobile Pays $90 Million to Settle Investigation into Mobile Cramming and Truth-in-Billing Practices," Dec. 19, 2014, available at www.fcc.gov.

[183] Press Release, "CFPB Takes Action to Obtain $120 Million in Redress from Sprint and Verizon for Illegal Mobile Cramming," May 12, 2015, available at www.consumerfinance.gov.

[184] The appendix to this report discusses the FTC's enforcement authority as well as remedies under TILA and the EFTA. The FCC's jurisdiction is limited to enforcing the Telephone Consumer Protection Act. That law prohibits automatically dialed phone calls (robocalls) and live telemarketing calls to numbers on the national Do-Not-Call list. It shares enforcement of this law with the FTC. The FCC also has jurisdiction over cramming and "slamming." The latter refers to the practice of switching a consumer phone carrier or service provider without the consumer's permission. This information is available at www.fcc.gov/opa/2013/03/mobilepymts.shtm.

[185] "Paper, Plastic … or Mobile?" At 12, FTC Workshop, March 2013. Staff report available at www.ftc.gov

[186] Brianna L. Reed, "Mobilizing Payments: Behind the Screen of the Latest Payment Trend," 14 J. High Tech. L. 451, 464 (2014).

[187] FFIEC Guidance, Authentication in an Internet Banking Environment, FFIEC-103-2005 (Oct. 12, 2005) (effective Dec. 31, 2006). The FFIEC is an interagency group consisting of the CFPB, FRB, FDIC, OCC, NCUA, and the State Liaison Committee. [TP: The FFIEC is an interagency body that provides uniform standards for the federal examination of financial institutions by the FRB, FDIC, NCUA, OCC, and CFPB. www.ffiec.gov.]

[188] Ibid, 2.

[189] FFIEC Supplement to Authentication in an Internet Banking Environment, FIL-50-2011 (June 29, 2011) (effective Jan. 1, 2012). In June 2015, the FFIEC issued a Cybersecurity Assessment Tool to assist financial institutions evaluate their cybersecurity systems. Available at www.ffiec.gov/cybersecurityassessmenttool.htm.

[190] The guidance describes various techniques that should be considered in a layered security program. Ibid.

[191] For device identification the guidance recommends using "one-time" cookies, the customer's computer configuration, its Internet protocol address and geolocation. It suggests using challenge questions whose answers do not rely on information publicly available, such as information on social networking sites. Ibid.

[192] Avivah Litan, "FFIEC Finally Releases New Guidance on Internet Banking Authentication; Better Late than Never," June 28, 2011, available at www.blogs.gartner.com

[193] Uniform Electronic Transactions Act § 10. The Uniform Law Commission is the sponsor of this law. The commission provides states with proposed legislation "that brings clarity and stability to critical areas of state statutory law." www.uniformlaws.org. Its members are lawyers appointed by state governments. The act has been adopted in the District of Columbia and every state except Illinois, New York, and Washington state. www.uniformlaws.org.

[194] Instead of including a provision authorizing persons to sue, Section 3(d) states that "a transaction subject to this [Act] is also subject to other applicable substantive law." This has been taken to mean "traditional contract law remedies, like fraud and mistake, are available." Stephanie Lillie, "Will ESIGN Force States to Adopt UETA?" 42 Jurimetrics J. 21, 26, n. 43 (2001).

[195] Bailey Reutzel, "Apple's Mobile Buzz Impacts Bitcoin but Regs Still Unclear," 2014 WL 29502957, PaymentsSource (Oct. 22, 2014). "Bitcoin transactions at brick and mortar retailers are usually facilitated through mobile payments, with the consumer either scanning a QR code associated with the merchant's Bitcoin account or typing in the alpha-numeric merchant Bitcoin address." Ibid. Venture capital firms are investing in bitcoin companies because they believe the underlying technology has widespread applications unrelated to payment

transactions. Michael J. Casey, "Noted Names Put Cash in Bitcoin Startup 21 Inc." Wall St. J., March 11, 2015, at C1, C2. That underlying technology is unregulated.

[196] Testimony of Jerry Brito, U.S. House of Representatives, House Small Business Committee Hearing, "Bitcoin: Examining the Benefits and Risks for Small Business," 2014 WLNR 1309468 (April 2, 2014).

[197] According to the IRS, virtual currency is not legal tender; it is treated by the IRS as property, not currency. IRS Guidance, 2014-21 (March 2014).

[198] See Task Force on Stored-Value Cards, "A Commercial Lawyer's Take on the Electronic Purse: An Analysis of Commercial Law Issues Associated with Stored-Value Cards and Electronic Money," 52 Bus. Lawyer 653, 669-70 (1997).

[199] IRS Guidance, 2014-21 (March 2014).

[200] At least one exchange, Mt. Gox, has filed for bankruptcy in Japan. The company claimed that 850,000 bitcoins were unaccounted for. In 2015, an involuntary bankruptcy was filed against its parent. The company's bankruptcy trustee announced the company has few assets and not enough money to fight lawsuits filed against it. Bill Rochelle & Sherri Toub, "Bitcoin Company Mt. Gox Parent Tibanne Seeks Chapter 15 Protection in New York," Bloomberg BNA Electronic Commerce & Law Report, Feb. 10, 2015" BNA Banking Rep. (Feb. 10, 2015).

[201] Consumer Advisory Warning, "CFPB Warns Consumers about Bitcoin (Aug. 11, 2014). See Kristen Cohen, "Before paying with bitcoins …" FTC Office of Technology Research and Investigation, June 22, 2015; Gov't Accountability Office, "Virtual Currencies: Emerging Regulatory Law, Law Enforcement, and Consumer Protection Challenges," GAO 14-496 (May 2014).

[202] "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," Financial Crimes Enforcement Network, FIN-2013-G001, March 18, 2013.

[203] Ryan Tracy, "U.S. Fines Virtual-Currency Business," Wall St. J., May 6, 2015, at C2 (reporting that Ripple, the second-most-popular virtual currency, reached a settlement in a case brought by the federal government).

[204] N.Y. Codes, Rules and Regulations, Title 23, Chapter I. Regulations of the Superintendent of Financial Services, Part 200. Virtual Currencies, available at http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf.

[205] Sarah Jane Hughes & Stephen T. Middlebrook, "Are These Game Changers? Developments in the Law Affecting Virtual Currencies, Prepaid Payroll Cards, Online Tribal Lending, and Payday Lenders," 70 Bus. Lawyer 261, 263 (2014-2015).

[206] As of May 2015, only Delaware had enacted the law. It was rejected by the legislatures in Kentucky, Mississippi, and Virginia. It was being considered in 26 other state legislatures. www.uniformlaws.org. Opponents claim it violates the privacy of the decedent and others and conflicts with federal and state law. Supporters counter that the law merely applies well-established fiduciary law and is carefully tailored to avoid the problems claimed by its critics. Alexis Kramer, "Uniform Law on Decedent's Digital Assets Rejected in 3 States, Still Alive in 23 others," Bloomberg BNA Electronic Commerce & Law Rep., March 17, 2015.

[207] 15 USC 6501-6506; 16 CFR Pt. 312.

[208] "Information Security: Distributed Denial of Service Attacks and Customer Account Fraud," OCC Alert 2012-16, Dec. 21, 2012. Sean Michael Kerner, "High-Bandwidth DDOS Attacks Becoming More Commonplace, Verisign Finds," Dec. 5, 2014, www.eweek.com.

[209] Ibid..

[210] 15 USC 1693j.

[211] Reg. E does not require disclosure of this right. See 12 CFR 1005.7 (initial disclosures); 12 CFR 1005.9 (periodic statements).

[212] Julia S. Cheney & Sherrie L.W. Rhine, "How Effective Were the Financial Safety Nets in the Aftermath of Katrina?" Federal Reserve Bank of N.Y., Jan. 2006 (finding that use of card payment applications such as credit, debit and prepaid cards that require electronic connections to the payment system were impaired).

[213] Payment Processor Relationships, FDIC Guidance (2012).

[214] "Risk Management Guidance," OCC Bulletin 2008-12, April 24, 2008. Press Release, "CFPB Takes Action against Global Client Solutions for Processing Illegal Debt-Settlement Fees," Aug. 25, 2014; Press Release, "CFPB Takes Action against Meracord for Processing Illegal Debt-Settlement Fees," Oct. 3, 2013.

[215] The previous section discussed third-party payment processors. They work for merchants from whom consumers have purchased goods and services. Often these merchants have no contractual relationship with a bank, so they need to use a third-party payment processor in order to arrange electronic transfers from consumer bank accounts. This section discusses third-party service providers. They work for the financial institutions in which consumers have their accounts, engaging in tasks the institution contracts out for others to do on their behalf.

[216] CFPB Bulletin 2012-03 (April 13, 2012).

[217] "Third-Party Relationships, Risk Management Guidance," OCC Bulletin 2013-29; "Supervision of Technology Service Providers," FFIEC booklet (FFIEC Oct. 31, 2012). The FFIEC booklet is part of the "FFIEC Information Technology Handbook." Concurrently, the FRB, FDIC, and OCC issued "Federal Agencies' Administrative Guidelines, Implementation of the Interagency Program for the Supervision of Technology Service Providers" (Oct 2012). The FRB issued "Guidance on Managing Outsourcing Risks" (FRB, Dec. 5, 2013).

[218] 12 CFR 1005.2(m).

[219] Unauthorized use includes a transfer made by a person who obtains an access device through "fraud or robbery." Official interpretation 12 CFR 1005.2(m)-3. However, unauthorized use is a much broader category that encompasses conduct by persons who do not engage in criminal conduct. For example, if a consumer gives a family member or a co-worker authority to use a debit card for 30 days, transfers by that person during the 30 days are treated as authorized use. But if the person exceeds that authority, any further transfers are unauthorized as long as the consumer has notified the institution that issued the card that transfers by the person are no longer authorized. Official interpretation 12 CFR 1005.2(m)-2. Examples of exceeding authority include making charges in amounts greater than permitted or for a longer period of time. TILA and Reg. Z use somewhat similar language for unauthorized use: a person who does not have actual, implied or apparent authority. 12 CFR 1026.12(b). Courts apply state law on agency to determine a person's authority. E.g,. Asher v. Chase Bank, 310 Fed. Appx. 912 (7th Cir. 2009) (TILA case). See official interpretation 12 CFR 1026.12(b)(1)(ii)-1 ("Whether such authority [actual, implied or apparent] exists must be determined under state agency or other applicable law.").

[220] In order to clarify its definition of unauthorized transfers, Reg. E identifies a narrow set of circumstances that are not considered unauthorized transfers such as a transfer made by a consumer with fraudulent intent or where the consumer gave authorization to another person, then withdrew that authorization without notifying the bank that the person was no longer authorized. 12 CFR 1005.2(m).

[221] 12 CFR 1005.2(k).

[222] 12 CFR 1005.10(c).

[223] See text accompanying note 233.

[224] Letter dated Sept. 29, 2014, from 30 national, state, and local consumer protection and civil rights organizations to the heads of all the prudential regulators, the CFPB, and the Electronic Payments Association (hereafter cited as "Consumer Org. Letter"). Organizations include the Center for Responsible Lending, Consumer Action, Consumer Federation of America, Consumers Union, NAACP, National Consumer Law Center, and US PIRG. The letter states it is based on the organizations' experience with consumers. Although the focus of the letter is on preauthorized payments to payday lenders, the letter states consumers' difficulties persuading banks to stop payment is

"systematic" and occurs with other payments in addition to those that are preauthorized. Consumer Org. Letter at 1. In addition, the other problems described were not confined to predatory lending, but "also harmed people in many other situations." Ibid, 2. Furthermore, even if the practices were confined to payday lenders or preauthorized payments generally, those practices have a significant impact on one-time mobile payments. A bank's failure to comply with the consumer's stop-payment instruction or honor the consumer's revocation of authorization unjustifiably drains funds from the consumer's bank account. As a result, when the consumer tries to make a mobile payment, there may not be sufficient funds in the account and the payment may be refused. Alternatively, the payment may be permitted, but an overdraft fee will typically be imposed.

[225] Ibid, 1 & 4.

[226] Ibid. 4.

[227] Nancy Vendrely, "Keeping a Good Name: Identity Theft Becoming More Common," Fort Wayne J. Gazette, 2002 WLNR 11634694, June 24, 2002 ("Obtain a copy of the police report; you may need it to verify the crime for your credit card company, bank and others.");Bill Lubinger, "If Someone Steals Your Wallet, Get Busy on the Phone," 1999 WLNR 7395972 ("File a police report, which banks, credit card issuers and insurers may require as proof before processing a claim."); Ann Landers, "Rude Comments of Strangers Distress Families of Multiples," 1996 WLNR 5823391, June 29, 1996 ("File a police report. Banks, credit-card and insurance companies may require such a report to verify the crime.").

[228] 12 CFR 1005.10(c).

[229] 12 CFR 1005.2(k).

[230] Reg. E, official interpretations 12 CFR § 1005.10(b)-5.

[231] 12 CFR 1005.10

[232] 12 CFR 1005.10(c).

[233] Reg. E, official interpretations 12 CFR 1005.10(c)-1. (Italics added.)

[234] The "payee" is the person the consumer intends to receive funds from the consumer's account. For example, when a consumer makes a mobile payment to a merchant to pay for a purchase, the consumer is the payor and the merchant is the payee.

[235] Compare Murphy v. Law Offices of Howard Lee Schiff, PC, 2014 WL 710959, at *3 (D. Mass. 2014) (applies only to financial institutions) with Johnson v. Tele-Cash, 82 F. Supp 2d 264 (D. Del. 1999) (court denied payee's motion to dismiss); rev'd in part on other grounds, 225 F.3d 366 (3d Cir. 2000). Saunders et al., Consumer Banking and Payments Law (2014 Supp) (hereafter Saunders Supp.) at 51.

[236] Murphy v. Law Offices of Howard Lee Schiff, PC, 2014 WL 710959, at *3 (D. Mass. 2014).

[237] Johnson v. Tele-Cash, 82 F. Supp 2d 264 (D. Del. 1999) rev'd in part on other grounds, 225 F.3d 366 (3d Cir. 2000).

[238] See Saunders, supra at 156.

[239] Reg. E, official interpretations 12 CFR 1005.10(c)-2. (Italics added.)

[240] Community Org. Letter, supra at 7. Some banks refuse to close the account because transactions are pending or the account is overdrawn and the consumer must first pay overdraft fees. Some banks engage in a practice called a "soft close" in which the account is reopened if needed to process an incoming debit. Ibid. "Trapped at the Bank: Removing Obstacles to Consumer Choice in Banking," Consumers Union, May 30, 2012 (study found that closing an account at one bank and establishing an account at a new bank can be complicated and confusing and can take months). Available at www.consumersunion.org. In 2013 members of the U.S. House filed a bill to protect the rights of consumers who wanted to close their accounts. H.R. 3137, 113th Congress, available at

www.govtrack.us/congress/bills/113/hr3137. See generally, Liran Haim, "Rethinking Consumer Protection Policy in Financial Markets," 32 J. L. & Commerce 23, 42 (2013) (Survey that found many consumers are dissatisfied with their bank's financial services but do not switch to another bank because it is too much trouble. Author attributes the reluctance to change banks to the high search costs and "incomprehensibility of alternative financial products."). Ibid. Consumers' problems may not end when they close their accounts. This is illustrated by a CFPB enforcement action against an online payday lender. According to the complaint, when consumers closed their accounts to stop unauthorized withdrawals, debt collectors demanded they pay for loans the consumers had never agreed to. "CFPB Sues Online Payday Lender for Cash-Grab Scam," CFPB Press Release, Sept. 17, 2014, available at www.consumerfinance.gov.

[241] Financial institutions process electronic payments through the automated clearinghouse (ACH) system. Two institutions operate the system, and all banks that want to use it are required to comply with the NACHA Rules. See www.nacha.org/about; Saunders, supra at 138-41. Section 1.2 provides that a financial institution participating in the ACH system "must comply with these Rules and warrants that it is legally able to comply with all applicable requirements of these Rules." NACHA Rules, Section 1.2.

[242] NACHA Rules, Section 3.7.1.2.

[243] Ibid, Section 2.3.2.3(c). The consumer, called a "receiver" in the Rules, "may revoke the authorization only by notifying the Originator [the business] in the time and manner stated in the authorization. For a Single Entry [one-time transfer] scheduled in advance, any such revocation right shall afford the Originator a reasonable opportunity to act on such revocation prior to the initiation of the Entry [the transfer]." Ibid. A "wireless network" is defined as "an Unsecured Electronic Network for the communication of data using wireless technology." Section 8.114.

[244] Ibid, Section 3.7.1.2.

[245] 12 CFR 1005.17(b). See AnnaMaria Andriotis & Peter Rudegeair, "Declining Overdraft Fees Gnaw at Banks," Wall St. J., June 17, 2015, at C1, C2 (reporting that bank revenue from overdraft fees has been falling since the Reg. E restrictions went into effect).

[246] 12 CFR 1005.17(b)(1)(iv).

[247] 12 CFR 1005.17(b)(2).

[248] 12 CFR Part 1030.

[249] In 2005, the OCC, FRB, FDIC, and NCUA issued "Joint Guidance on Overdraft Protection Programs," 70 Fed. Reg. 9127 (Feb. 24. 2005). In 2010, the FDIC issued "Overdraft Payment Programs and Consumer Protection, Final Overdraft Payment Supervisory Guidance," FIL-81-2010 (Nov. 24, 2010), available at www.fdic.gov. On Feb. 11, 2015, the OCC issued a booklet titled "Deposit-Related Consumer Credit." That booklet included a section on overdraft programs that required banks to perform an assessment of the consumer's ability to pay and imposed limits on fees. On Feb. 20, 2015, OCC removed the booklet from its website. It reissued the booklet on March 6, 2015. In the reissued version, the OCC deleted the overdraft section from the previous version and replaced it with what the OCC characterized as merely a summary of existing laws and policies that did not reflect any change in OCC policy. Jeffrey Werthan, "OCC Issues New Handbook on Deposit-Related Consumer Credit," Nat'l L. Rev., April 17, 2015, available at www.natlawreview.com; Rachel Witkowski, "OCC Mistake Sparks Three-Week Panic on Overdraft Rules," 2015 WLNR 7567355, Am. Banker, March 13, 2015.

[250] Joint Guidance on Overdraft Protection Programs, OCC, FRB, FDIC, & NCUA, 70 Fed. Reg. 9127 (2005). See Carter Dougherty, "Banks' Billions in Overdraft Fees Seen Dodging Tough U.S. Rules," 104 BloombergBNA's Banking Report 1083, June 5, 2015 (predicting that the CFPB will propose overdraft rules in late 2015 or early 2016. The CFPB likely will require improved disclosures and prohibit reordering transactions to increase fees, but probably will not place a limit on how frequently fees may be imposed or the amount of the charges).

[251] FDIC Supervisory Guidance for Overdraft Protection Programs and Consumer Protection, FIL-81-2010 (2010). As described supra in note 249, in 2015 the OCC issued a booklet with language limiting fees, but subsequently withdrew it and issued a revised version that omitted that protection.

[252] In re RBS Citizens, AA-EC-10-93 (2013) (OCC action in conjunction with FDIC); in re Woodforest Nat'l Bank, AA-EC-10-93 (2010) (OCC action).

[253] Jonathan Stempel, "PNC Settles Overdraft Fee Case for $90 Million," Reuters News, June 26, 2012, available on WestLaw; "JP Morgan settles overdraft fee case for $110mln," Reuters News, Feb. 6, 2012, available on WestLaw; Phil Villarreal, "Judge Approves B of A's $410M Overdraft Settlement," Consumerist, 2011 WLNR 23070127, Nov. 8, 2011. The case law is summarized in Saunders, supra at 24-28. In one case that has been ongoing for many years, class actions have been certified against Wells Fargo. In re Checking Account Overdraft Litigation, 2015 WL 3551527 (SD Fla. 2015); in re Checking Account Overdraft Litigation, 2015 WL 3551555 (SD Fla. 2015). Another strategy is to contend that under certain circumstances overdraft charges constitute illegal usurious interest. In a class action lawsuit filed in March 2015, the consumers challenged an overdraft program on that basis. In addition to the usual $35 overdraft fee, if that fee was not paid in five days, another $35 fee was imposed. McGee v. Bank of America, No. 15-cv-60480 (SD Fla.), reported in Aubin, "BofA fights proposed class action over extended overdraft fees," Reuters Legal, April 22, 2015, available on WestLaw (reporting that the bank has filed a motion to dismiss).

[254] UCC 1-201(b)(21).(Citations to Article 1 of the UCC are to Revised Version 2001).

[255] UCC 3-103(a)(5).

[256] Risk Management of Remote Deposit Capture, Federal Financial Institutions Examination Council (undated) at 4-5, available at www.ffiec.gov.

[257] See Comment 3, 4-401, Comment 3, 4-406. Gail K. Hillebrand, "Revised Articles 3 and 4 of the Uniform Commercial Code: A Consumer Perspective," 42 Ala. L. Rev. 679 (1991); Edwin Rubin, "Efficiency, Equity and the Proposed Revision of Articles 3 and 4," 42 Ala. L. Rev. 551 (1991).

[258] See Comment 1, 4-406: "The provision … is based upon the existing state of technology. … It is expected that technological advances such as imaging processing may make it possible for banks to give customers more information in the future in a manner that is fully compatible with automation or truncation systems. At that time the Permanent Editorial Board may wish to make recommendations for an amendment revising the safe harbor requirements in light of those advances." The official version of the UCC has never been amended to reflect technological advances that have occurred since the 1990s. The official version is the version that is approved by the sponsoring organizations, the American Law Institute, and the Uniform Law Commission.

[259] The UCC also plays a role to the extent the electronic check presentment rules apply, see infra text accompanying notes 273-74.

[260] 15 USC 1693(b): "The primary objective of this subchapter [the EFTA] … is the provision of individual consumer rights."

[261] See "Terms and Conditions of Mobile Remote Deposit Capture," The Pew Charitable Trusts (Nov. 14, 2014).

[262] See description of the EFTA's error resolution procedure, text accompanying notes 471-80. infra. Although the EFTA and Reg. E do not explicitly mention RDC, it appears to come within the definition of an electronic fund transfer. "The term electronic fund transfer means any transfer of funds that is initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer's account." 12 CFR 1005.3(b)(1).

[263] See infra text accompanying note 478.

[264] "Mobile Check Deposit: Pros and Cons," Record-Journal, 2014 WLRN 2774139 (Oct. 6, 2014) (reporting that Consumer Reports recommends delaying destruction of the check for two weeks). Susan Tompor, "Know When the Check Clears with Smartphone Deposits," Detroit Free Press, Jan. 8, 2015 (reporting that some banks advise their customers to retain paper checks for two weeks).

[265] UCC 3-206(c).

[266] See UCC 3-206, Comment 3.

[267] Mary Wisniewski, "Fighting Mobile Deposit Fraud without Inconveniencing Customers," 2014 WLNR 30894088, Am. Banker, Nov. 14, 2014.

[268] Mary Wisniewski, "The Lesser-Known Risks of Mobile Check Deposit," 2013 WLNR 16866220, Am. Banker, July 12, 2013 (quoting the CEO of remotedepositcapture.com saying that there is evidence of "double depositing"). See Frank Stokes, "Don't Be Duped: Remote Checks Risky," 2010 WLNR 10774008, Am. Banker, May 26, 2010 ("The possibility of duplicate payments being made from a single check is more than conceivable—it's inevitable. … A customer with multiple banking relationships could easily deposit the same check to separate institutions—once via RDC and again in person.").

[269] UCC 3-204, 3-205. A subsequent holder has the right to payment of the check unless it contains a restrictive endorsement or the holder has engaged in illegal conduct. Unfortunately, the honest parties to the transaction may not discover the depositor is a thief until the thief has taken the drawer's funds and is "of parts unknown."

[270] See Saunders, supra at 48-49.

[271] Under the UCC, the drawer is not liable for the alteration unless the drawer was negligent. UCC 3-406, 3-407. As between the drawer's bank and the depositor's bank, courts disagree on who has the burden of proof on the issue of whether there was an alteration of a digitized check. Compare Chevy Chase Bank v. Wachovia Bank, 208 Fed. Appx. 232 (4th Cir. 2006) (burden on drawer's bank) with Wachovia Bank v. Foster Bancshares, 457 F.3d 619 (7th Cir 2006) (depositary bank has burden). If the drawer's bank has the burden, it may be less willing to credit the drawer's account the amount claimed by the drawer because it will either have to bear the loss or try to recover its loss from the depository bank. Adam J. Levitin, "Remote Deposit Capture: A Legal and Transactional Overview," 126 Banking L. J. 115, 119 (2009). The FRB favors putting the burden on the depositor's bank but has requested the views of others before it makes a final decision. "Availability of Funds and Collection of Checks," Proposed rule, request for comment, 79 Fed. Reg. 6674, 6703 (Feb. 4, 2014).

[272] UCC 3-407.

[273] UCC 4-110.

[274] Mark Budnitz, "Mobile Banking: Gaps in the Law Impede Risk Assessment," 32 Banking & Financial Services Policy Rep. 11, 14-15 (2013); Stephanie Heller, "An Endangered Species: The Increasing Irrelevance of Article 4 of the UCC in an Electronic-Based Payments System," 40 Loyola L. Rev. 513, 526-37 (2006).

[275] The funds from cash, electronic payments, U.S. Treasury checks, U.S. Postal Service money orders, state and local government checks, as well as cashier's, certified, and teller's checks must be made available to the depositor according to what Reg. CC terms "next-day availability." Next-day availability is the first business day following the banking day of deposit. The funds from checks not subject to next-day availability, such as regular personal checks, must be made available by the second business day following the day of deposit. But the first $200 from any such check must be available on the business day after the banking day of deposit. 12 CFR 229.10 & 229.12. There are special rules permitting banks to delay availability for checks deposited at ATMs, deposits greater than $5,000 unless they are made in cash or electronic payments, deposits to accounts repeatedly overdrawn, accounts where the bank has reasonable cause to doubt collectability, accounts of new customers, and emergency conditions such as natural disasters and communications failures. 12 CFR 229.13. Funds from the accounts subject to the exceptions must be made available "by a reasonable period of time." 12 CFR 229.13(h). "Banking day" is "that part

of any business day on which an office of a bank is open to the public for carrying on substantially all of its banking functions." 12 CFR 229.2(f). "Business day" is defined as any day except Saturday or Sunday and specified federal holidays. 12 CFR 229.2(g).

[276] Budnitz, supra at 15. Levitin, supra at 120. NCLC et al. Comments to CFPB, supra at 19, See Saunders, supra at 113 (suggesting that Reg. CC may apply because a mobile device may come within Reg. CC's definition of "ATM."). The list of statutes within the CFPB's jurisdiction does not include Reg. CC. 12 USC 5481(12). See generally, "Hidden Risks: The Case for Safe and Transparent Checking Accounts," The Pew Charitable Trusts (April 2011).

[277] See "Terms and Conditions of Mobile Remote Deposit Capture," supra; Meg Sczyrba & Thomas Healy, "Mobile Banking and Payments: What Are the Rules?" ABA Bank Compliance 8 (Sept.-Oct. 2012) at 12.

[278] Walmart's GoBank account permits RDC, but does not make funds available for 10 business days. "Snapping a Pic Doesn't Make Funds Available," Augusta (GA) Chronicle, 2015 WLNR 1448763 (Jan. 14, 2015). See "Mobile Check Deposit: Pros and Cons," Record-Journal, 2014 WLRN 2774139 (Oct. 6, 2014).

[279] The Pew Charitable Trusts study included 21 nonbank prepaid companies that offered RDC. "Terms and Conditions of Mobile Remote Deposit Capture," supra. "American Express buys into the notion that mobile and prepaid are perfect bedfellows. The card brand transformed its Serve digital wallet into a prepaid product. 'Mobile impacts every way we think about prepaid.'" David Heun, "How Prepaid Can Light the Way to Success for Mobile," 2015 WLNR 10760947, Am. Banker, April 13, 2015 (quoting the vice president of business development & strategy for Amex's enterprise growth unit). When it issued its proposed rule on prepaid cards, the CFPB noted: "GPR [general purpose reloadable] cards can generally be reloaded through … deposit of a check … via remote deposit capture." 79 Fed. Reg. 77102, 77105.

[280] Saunders, supra at 241. The CFPB's proposed prepaid card rule does not specifically address whether or how the rule would apply to RDC. However, apparently the rule would apply to cards loaded by means of RDC since in its commentary on the proposed rule the CFPB acknowledged that the cards could be reloaded via RDC, 79 Fed. Reg. 77102, 77105, and never explicitly excludes or restricts that method of reloading cards from the rule's application. See the Stage 1 portion of this report for a description of the proposed rule.

[281] See "Terms and Conditions of Mobile Remote Deposit Capture," supra; see e.g., Costoso v. Bank of America, 2015 WL 774478, *10 (ED NY 2015) (bank agreement did not obligate bank to comply with NACHA Rules).

[282] Susan Tompor, "Know When the Check Clears with Smartphone Deposits," Detroit Free Press, Jan. 8, 2015.

[283] UCC 1-302(a).

[284] 15 USC 6801(a).

[285] According to the FTC the following companies are subject to the rule if they are "significantly engaged": check cashing businesses, payday lenders, mortgage brokers, nonbank lenders, personal property or real estate appraisers, professional tax preparers, and courier services. The FTC rule "also applies to credit reporting agencies and ATM operators that receive information about the customers of other institutions" "Companies covered by the Rule are responsible for taking steps to ensure that their affiliates and service providers safeguard customer information in their care." https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/standards-safeguarding-customer.

[286] Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 12 CFR pt, 225, App F, sup. A.

[287] Standards for Safeguarding Customer Information, 16 CFR pt 314.

[288] 16 CFR 314.4(e).

[289] Companies worry about sharing information with competitors and the government. "Industry praises move on antitrust issue; impact on info-sharing legislation unclear," Inside CyberSecurity, 2014 WLNR 10237388 (April 14,

2014) (reporting on joint FTC and Dept. of Justice statement permitting "legitimate sharing of cyber threat information"). States object to federal legislation that will pre-empt their authority. Ian McKendry & Rachel Witkowski, "State, Federal Officials Clash over Data Security," Am. Banker, March 19, 2015, at 1.

[290] Massachusetts' regulation applies to anyone who owns or licenses personal information about a state resident, a broad category that includes many types of firms in addition to financial institutions. Standards for the Protection of Personal Information of Residents of the Commonwealth, 201 CMR 17.03(1):M.G.L. c. 93H. Mass. has aggressively enforced this regulation. Elizabeth McGinn, Thomas Sporkin, Alexander D. Lutch, & James T. Shreve, "The Board of Directors and Cybersecurity: Setting Up the Right Structure," BNA U.S. L. Week, 744, 747 (Nov. 18, 2014). The N.Y. Department of Financial Services is considering requiring state chartered banks to appoint chief information security officers. In addition, they would be subject to tests of their security systems' vulnerabilities. Chris Cumming & Marc Hochstein, "N.Y.'s Lawsky Considering Strict Cybersecurity Regime for Banks," 2014 WLRN 29012222, Am. Banker, Oct. 20, 2014.

[291] The CFPB, FTC, "functional regulators" and state insurance authorities have the power to enforce GLBA. 15 USC 6805(a). See e.g., FTC v. Ameridebt, 343 F. Supp 2d 451 (D Md. 2004).

[292] In the Matter of HTC, Docket No. C-4406, Decision & Order (June 25, 2013). In two cases, companies misrepresented the level of security and privacy they provided. In the Matter of Credit Karma, Docket No. C-4480, Decision & Order (Aug. 13, 2014); In the Matter of Fandango, Docket No. C-4481, Decision & Order (Aug. 13, 2014). In the Matter of Trendnet, Docket No. C-4426, Decision & Order (Jan. 16, 2013).

[293] Wyndham Worldwide Corp., 10 F. Supp 3d 602 (D NJ 2014), motion to certify appeal granted, June 23, 2014; FTC v. LabMD, 2014 WL 253518 (pending FTC Admin. Proceeding 2014), LabMD v. FTC, 776 F.3d 1275 (11th Cir. 2015) (court lacked subject matter jurisdiction because there has been no final agency action).

[294] E.g., C.S. v. United Bank, 2009 WL 777643, at *5 (SD W.Va. 2009).

[295] Infra text accompanying note 502.

[296] 47 USC 222(c). "CPNI includes information such as the phone numbers called by a consumer, the frequency, duration, and timing of any such calls; and any services purchased by the consumer, such as call waiting." Implementation of the Telecommunications Act of 1996, 21 FCCR 1782, 1884 (2006)(notice of proposed rulemaking).

[297] 47 CFR 64.2010(a).

[298] USC 201(b). In addition to requiring that all practices be just and reasonable, all charges, classifications and regulations for and in connection with wireless services must be just and reasonable. Ibid.

[299] In the Matter of AT&T Services, Inc., File No. EB-TCD-14-00016243 Order and Consent Decree, April 8, 2015. According to the FCC, AT&T failed to properly protect the confidentiality of its information about almost 280,000 customers. The consent order requires the company to pay a civil penalty of $25 million, develop and implement a compliance program, regularly train employees on the company's privacy policies and applicable law, and appoint a senior compliance manager.

[300] In the Matter of AT&T Services, Inc., File No. EB-TCD-14-00016243 Order and Consent Decree, April 8, 2015.

[301] 47 USC 222(c).

[302] 47 CFR 64.2011(b). A "breach" occurs when a person who does not have authorization, or who exceeds authorization, intentionally gains access to, uses, or discloses CPNI. 47 CFR 64.2011(e).

[303] 47 CFR 64.2011(a).

[304] The following states have not passed data breach notification laws: Alabama, Kentucky, New Mexico, and South Dakota. Jill Joerling, "Data Breach Notification Laws: An Argument for a Comprehensive Federal Law to Protect Consumer Data," 32 Wash. U. J.L. & Pol'y 467, 473 n. 33.

[305] Some statutes include government units, others do not. Ibid, 476; Burdon, supra at 77.

[306] N. Caro. Gen. Stat. Ann. 75-65(a).

[307] Joerling, supra at 473.

[308] Consumer Reports Money Adviser, "Debunking the Hype over ID Theft: You Don't Need a Costly Service to Protect Your Good Name," Feb. 2012, accessed June 3, 2015, http://www.consumerreports.org/cro/2012/02/debunking-the-hype-over-id-theft/index.htm. In 2014, the CFPB ordered U.S. Bank to pay $48 million in refunds to consumers who were unfairly charged for identity theft protection and credit monitoring services they never received. "CFPB Orders U.S. Bank to Pay $48 Million Refund to Consumers Illegally Billed for Services Not Received," CFPB Press Release, Sept. 25, 2014, available at www.consumerfinance.gov. In 2012, the CFPB brought a case against Capital One Bank for deceptive practices in pressuring or misleading consumers into paying for "add-on" products, including credit monitoring. "CFPB Probe into Capital One Card Marketing Results in $140 Million Consumer Refund," CFPB Press Release, July 18, 2012, available at www.consumerfinance.gov.

[309] Bills to require notice nationally in a uniform manner have been introduced, but none has passed. Burdon, supra at 77-78.

[310] Joerling, supra at 476.

[311] Ibid. 475.

[312] Ibid.

[313] Ibid. 479.

[314] Peter J. Arant, "Understanding Data Breach Liability: The Basics Every Attorney Should Know," 40 Mont. L 8, *10 (Feb. 2015).

[315] NCLC et al. Comments to CFPB, supra at 18.

[316] E.g., 201 Mass. Code Regs. § 17.03. Peter Sloan, "The Reasonable Information Security Program," 21 Rich. J.L. & Tech. 2, 3-15 (2014); Joerling, supra at 479-80.

[317] E.g., P.F. Chiang's China Bistro, 2014 WL 7005097 (ND Ill. 2014) (breach of implied contract and violation of Illinois' UDAP statute).

[318] Rachael Peters, "So You've Been Notified, Now What? The Problem with Current Data-Breach Notification Laws," 56 Ariz. L. Rev. 1171, 1187-95 (2014). But see in re Target Corp. Data Sec. Breach Litigation, 2014 WL 7192478, *2 (D Minn. 2014) (plaintiffs alleged injury sufficient for court to reject motion to dismiss where they alleged unlawful charges, restricted and blocked access to bank accounts, inability to pay other bills, late payment charges, and new card fees); Robins v. Spokeo, 742 F.3d 409 (9th Cir. 2014), petition for cert. granted, April 27, 2015, 2015, WL 1879778 (court held that consumer established injury sufficient to satisfy Article III standing where Fair Credit Reporting Act's statutory cause of action did not require consumer to show actual harm when suing for a willful violation); in Mabary v. Home Town Bank, 771 F.3d 820 (5th Cir. 2014) the court found that although the consumer did not receive the ATM notice required by the EFTA, she did receive actual notice. Therefore, she suffered no concrete injury. Nevertheless, the court found the consumer had standing. "Congress' determination that consumers were entitled to the fee information … before investing the time needed to initiate [an ATM transaction] protects a substantive, small right, and its deprivation is an injury-in-fact that allows [the consumer] to pursue her claim here." Ibid, 823-24.

[319] Eliseuson, "Supreme Court's CAFA Ruling Might Open the Floodgates to State Attorney General Data Breach and Privacy Suits," U.S. Law Week 358, 361 (Sept. 9, 2014). But see P.F Chang's China Bistro, 2014 WL 7005097 (ND Ill. 2014) (consumer's claim for breach of implied contract and violation of Illinois' UDAP law dismissed for lack of standing); in re Michaels Stores Pin Pad Litig., 830 F. Supp 2d 518 (ND Ill. 2011) (consumers suffered no actual injury; were reimbursed for unauthorized withdrawals and bank fees).

[320] 15 USC 6803. GLBA has rules for "customers," such as persons who apply for credit, regardless of whether credit is extended, and "consumers," who are persons in a continuing relationship with the institution.

[321] 15 USC 6802(b).

[322] 16 CFR pt. 313.

[323] 15 USC 6804. The FTC still has rule-making authority for auto dealers as provided in 15 USC 6804(a)(1)(C).

[324] Amendment to the Annual Privacy Notice Requirement under the Gramm-Leach-Bliley Act (Regulation P), 79 Fed. Reg. 64057 (Oct. 28, 2014). To be codified at 12 CFR 1016.9.

[325] The older permissible delivery methods are required if the institution has changed its privacy practices or engages in information sharing activities for which customers have a right to opt out.

[326] Eric Poggemiller, "The Consumer Response to Provisions in Gramm-Leach-Bliley: Much Ado about Nothing," 6 N.C. Banking Inst. 617, 619 (2002).

[327] E.g., In the Matter of Nomi Technologies, Statement of Chairwoman Ramirez & Commissioners Brill & McSweeney, April 23, 2015 (company that provided retailers with technology that allowed them to track the location of shoppers via a WiFi interface with shoppers' mobile devices misrepresented that "privacy is our first priority" and shoppers could opt out of retailers' location tracking) (two commissioners dissented); In the Matter of Goldenshores Technologies, Decision & Order, C-4446 (March 31, 2014) (privacy policy was deceptive because it did not reflect app's use of personal data); In the matter of Snapchat, Decision & Order, C-4501 (Dec. 23, 2014) (deceived consumers over amount of personal data collected and security measures taken to protect that data from misuse and unauthorized disclosure); FTC v. Acquinity Interactive, 14-60166-CIV-SCOLA/OTAZO-REYES (SD Fla. Oct. 16, 2014) (FTC alleged that an international network of scammers promised free gifts, sent text messages to consumers, and deceived them into providing sensitive personal information that was sold to third parties; final judgment, permanent injunction, and other equitable relief stipulated and agreed to by the parties). The alleged facts are in FTC v. Acquinity Interactive, 2014 WL 37808 (ND Ill. 2014). An FTC staff report recommends providing consumers with timely, easy-to-understand disclosures informing them what data the company collects and how the data are used. "Mobile Privacy Disclosures, Building Trust through Transparency," FTC Staff Rep. (Feb. 2013).

[328] Daniel J. Solove & Woodrow Hartzog, "The FTC and the New Common Law of Privacy," 114 Colum. L. Rev. 583, 585 (2014).

[329] Solove & Hartzog, nevertheless, believe the FTC has developed a common law of privacy. Ibid, 648-67. Although consumers have no private right of action under the FTC Act, they can use FTC case law when bringing state UDAP cases. See text in paragraph that accompanies note 501; see generally, Section G, supra.

[330] But see Google Android Consumer Privacy Litigation, 2014 WL 988889 (ND Cal. 2014) (court finds standing based on reduced functionality of phones due to depleted battery power).

[331] Miss. ex rel. Hood v. AU Optronics Corp., 134 S. Ct. 736 (2014). The court held the defendant could not remove the case to federal court pursuant to the "mass action" provision of the federal Class Action Fairness Act.

[332] Eliseuson, supra at 361.

[333] Riley v. California, 134 S. Ct. 2473 (2014). In describing the information accessible from mobile phones, the court referred to items related to mobile payments. For example, the court included bank statements in its list of the various types of information stored in mobile phones. Ibid, 2489. The court mentioned electronic commerce.

"There are popular apps for buying or selling just about anything, and the records of such transactions may be accessible on the phone indefinitely." Ibid, 2490. The court pointed out that private information may not be stored in the phone at all, but rather in the cloud. Ibid, 2491.

[334] The Supreme Court held that a person who does not carry "a cache of sensitive personal information with them as they went about their day" is the exception. Ibid, 2490.

[335] The email addresses of beta testers and others expressing an interest in the mobile payment company Merchant Customer Exchange, a future competitor of Apple Pay, were accessed by an unauthorized third party. Owens, "Apple Pay rival exposed users' email addresses,"

[336] In re Google, 2014 WL 1102660 (ND Cal. 2014) (alleged violation of state and federal wiretap laws; class certification denied); in re Yahoo Mail Litigation, 2014 WL 3962824 (ND Cal. 2014) (alleged violation of California Constitution; motion to dismiss granted); Apple v. Superior Ct., 292 P3d 883 (Cal. Sup. Ct. 2013) (alleged violation of Beverly-Song Credit Card Act restricting use of "personal identification information"; court held that law does not apply to online purchases of downloadable music because its safeguards against fraud do not apply to such purchases).

[337] In re Yahoo Mail Litigation, 2014 WL 3962824 (ND Cal. 2014) (alleged violation of federal Stored Communications Act; motion to dismiss denied); Google Android Consumer Privacy Litigation, 2014 WL 988889 (ND Cal. 2014) (alleged violation of California Unfair Competition Law; motion to dismiss denied regarding unfair practices); Pirozzi v. Apple, 966 F Supp 2d 909 (ND Cal. 2013) (alleged violation of California's Uniform Competition Law, False and Misleading Advertising Law & Consumer Legal Remedies Act; motion to dismiss denied); Capp v. Nordstrom. 2013 WL 5739102 (ED Cal. 2013) (alleged violation of Beverly-Song Credit Card Act restricting use of "personal identification information"; court held email address constituted such information); Pineda v. Williams-Sonoma Stores, 246 P3d 612 (Cal. Sup. Ct. 2011) (court held zip code is "personal identification information"); Tyler v. Michaels Stores, 984 NE2d 737 (Mass. Sup. Ct. 2013) (court held that including zip code on credit card transaction forms constitutes "personal identification information" violating Mass. law prohibiting such information on credit card transaction forms).

[338] See Scott S. Partridge & Perry J. Miller, "Some Practical Considerations for Defending and Settling Products Liability and Consumer Class Actions," 74 Tul. L. Rev. 2125 (2000); Conor Dougherty, "Jay Edelson, the Class-Action Lawyer Who May Be Tech's Least Friendly Man," N.Y. Times, Sunday Business, April 5, 2015, 1, 4 ("If the judge lets the case go forward as a class action, companies usually start thinking about settlements.").

[339] 15 USC 1681g(a)(1)(A).

[340] 15 USC 1681g(d).

[341] 15 USC 1681c-1.

[342] 15 USC 1681c-2.

[343] 15 USC 1681t(b). Chi Chi Wu, Elizabeth De Armond, Carolyn Carter, Richard Rubin, Arielle Cohen, Charles Delbaum, Persis S. Yu & Lauren K. Saunders, 1 *Fair Credit Reporting* 707 (8th ed. 2013) (hereafter "Wu et al.").

[344] Wu et al., supra at 685-90. In some states the tort actions are based on the common law; in others they are established by statute. Ibid, 685, 705-07. See e.g., California's Invasion of Privacy Act § 631. The provision is discussed in Campbell v. Facebook, 2014 WL 7336475 (ND Cal. 2014). A tort is a civil (not criminal) wrong, other than a breach of contract, for which the law provides a remedy, such as damages, for the person wronged. There are several varieties of torts including: 1) intentional torts, such as battery where a person makes physical contact with another person without the other person's consent; 2) unintentional torts, such as negligence where a person fails to exercise the standard of care that a reasonably prudent person would exercise; and 3) strict liability torts, that impose liability even where the person causing the injury had no intention to injure another and was not

negligent. For example, strict liability applies to persons dealing in abnormally dangerous products. Black's Law Dictionary (10th ed. 2014), available on WestLaw.

[345] Restatement (Second) of Torts § 625D.

[346] Wu et al., supra at 686.

[347] Restatement (Second) of Torts § 625B.

[348] Blanche v. First Nationwide Mortgage Corp., 2002 Tex. Ct. App. LEXIS 1892, *19 (Tex. Ct. App. 2002), cited in Wu et al., supra at 689, n. 68.

[349] Wu et al., supra at 703, n. 268. Under the California statute, a financial institution cannot disclose consumer information to others unless the consumer opts in. Cal. Fin. Code 4053(a). The city of Los Angeles has sued Wells Fargo, claiming it violated California's Unfair Competition Law by pressuring its employees to use customers' confidential information in order to charge the customers for services they did not authorize. E. Scott Reckard, "L.A. Sues Big Bank over Sales Quotas," 2015 WLNR 13044608, LA Times, May 5, 2015 (reporting that the bank misused customers' confidential information"); Peter Rudegeair, "Los Angeles Sues Wells over Pressuring Workers," Wall St. J., May 6, 2015, at C2 (reporting that LA claimed the bank violated California's unfair competition law).

[350] Wu et al., supra at 703-04.

[351] For example, Massachusetts law generally prohibits providers of electronic fund transfers from disclosing information without the consumer's permission. But there are major exceptions: they can supply information to debt collectors, consumer reporting agencies and others. Mass. Gen. Laws, ch. 167B, § 16, noted in Wu et al., supra at 705, n. 280.

[352] Cal. Bus. & Prof. Code 22575. "'Any [privacy] policy will do. The bill simply requires that an operator have a policy and then follow it.'" Apple v. Superior Ct., 292 P.3d 883, 895 (Cal. Sup. Ct. 2013) (quoting from Cal. Assembly Committee on Judiciary, Analysis of Assembly Bill No. 68).

[353] Ibid. For example, the privacy policy must identify the categories of personally identified information the operator collects through the website or online service and the categories of third parties it may share the information with. If the operator has a process for a consumer to review and request a change in collected personally identified information, that process must be described. The policy must describe the process used by the operator to notify consumers of material changes to its privacy policy.

[354] Cal. Bus. & Prof. Code 22575(a).

[355] Ibid, 22576.

[356] Friends of the Earth v. Laidlaw Envt'l Sys., 528 US 167, 180-81 (2000).

[357] In re Google, Inc., Privacy Policy Litigation, 2013 WL 6248499, at *4 (ND Cal. 2013) (hereafter Google Privacy Litigation).

[358] Ibid, *5.

[359] Opperman v. Path, 2014 WL 1973378, at *23 (ND Cal. 2014).

[360] Svenson v. Google, 2015 WL 1503429, *2 (ND Cal. 2015). Even if a plaintiff does not suffer injury that confers standing, a statute itself may confer standing if the plaintiff was deprived of a right granted by the statute. Golan v. Veritas Entertainment, 2015 WL 3540573, *3 (8th Cir. 2015) (holding the Telephone Consumer Protection Act conferred standing where plaintiffs were subjected to unsolicited prerecorded phone calls).

[361] Ibid.

[362] In Campbell v. Facebook, supra at *12 the court simply rejected the plaintiff's property interest contention, citing previous cases that involved different types of information and different defendants. In Claridge v. Rockyou, 785 F. Supp 2d 855, 863 (ND Cal. 2011), the plaintiff claimed a property interest in his login and password, both of which had been subject to being discovered and used by a hacker due to the defendant's alleged failure to act reasonably upon learning of the hack. The court pointed out the plaintiff had not lost his property. His login and password still belonged to him. In the case of in re Facebook Privacy Litigation, 791 F. Supp 2d 705, 715 (ND Cal. 2011), the court held the plaintiff had not lost property or money due to disclosure of information about him to advertisers because he had obtained services from the defendant free of charge.

[363] "How the Kill Switch Law Affects Businesses," Bus. Rev. USA, 2015 WLNR 5956778 (Feb. 25, 2015) ("Approximately 40% of robberies in major cities involve stealing of mobile communication devices.").

[364] 1024 Minnesota Session Laws, ch. 241-S.F. No. 1740, Smartphone Antitheft Protection, Section 1 [325F.698], subdivision 2. The Minnesota statute spells the mobile device as two words, "smart phone"; the California statute spells it as one word.

[365] Ibid, subdivision 1(b).

[366] West's Ann. Cal. Bus. & Prof. Code § 22761(b)(1).

[367] Ibid, (b)(2).

[368] Ibid, (a)(1)(B).

[369] Ibid, (c).

[370] Ibid, (d).

[371] "Congress Should Enact Kill Switch Legislation," Wash. Internet Daily, 2015 WLNR 5275087 (Feb. 18, 2015) (reporting that Rep. Serrano announced he will reintroduce the Smartphone Theft Prevention Act in 2015. The act was introduced in 2014 in both the House and Senate, but it was never approved.).

[372] Rolfe Winkler, "IPhone 'Kill Switch' Appears to Reduce Thefts," Wall St. J., June 20, 2014, at B3.

[373] E.g., "Consumer Financial Protection Bureau Takes Action to Obtain $120 Million In Redress from Sprint and Verizon for Illegal Mobile Cramming," Press Release, May 12, 2015, available at www.consumerfinance.gov. (hereafter "Sprint & Verizon Proposed Order").

[374] FTC v. Tatto, 2013 WL 6979682 (CD Cal. 2013) (complaint). The court issued a temporary restraining order and an asset freeze.

[375] Acquinity Interactive, 2014 WL 37808 (ND Ill. 2014) (complaint) (final judgment, permanent injunction and other equitable relief stipulated and agreed to by the parties Oct. 22, 2014). The FTC also charged the company with violating the Telemarketing Sales Rule, 15 USC 6101-08.

[376] FTC Press Release, Dec. 16, 2013. Available at ftc.gov.

[377] FTC Press Release, June 13, 2014. Available at ftc.gov.

[378] FTC Press Release, July 29, 2013. Available at ftc.gov.

[379] Opening remarks of Chairwoman Edith Ramirez, AT&T Cramming Settlement Conference, Oct. 8, 2014, available at ftc.gov.

[380] FTC Press Release, Dec. 19, 2014.

[381] CFPB v. Sprint Corp., 14 CV 9931 (SD NY) (complaint filed Dec. 17, 2014), Press Release, Dec. 17, 2014. Available at www.consumerfinance.gov. In 2015 the CFPB filed a proposed consent order that would require Sprint to pay $50 million in redress to consumers, millions of dollars in federal and state fines, clearly and conspicuously disclose

third-party charges on wireless bills, obtain informed consent from consumers prior to third-party billing, improve dispute resolution procedures, and enhance customer-service training programs. Sprint & Verizon Proposed Order, supra.

[382] Sprint & Verizon Proposed Order, supra.

[383] Penny Crosman & Andy Peters, "New Underbanked FICO Score Faces Old Banker Skepticism," 2015 WLNR 9748784 (April 6, 2015); AnnaMaria Andriotis, "New Metric Aids Weak Credit Risks," Wall St. J., April 1, 2015, at C1. Consumers have many FICO credit scores, and consumers don't know which one a creditor may use. "The exact score a lender pulls up depends in part on the credit-reporting firm that supplies it and the type of FICO score the lender chooses to use." AnnaMaria Andriotis, "Which FICO Score Counts?" Wall St. J., June 27-28, 2015, at B8.

[384] United States of America v. Path, 3:13cv-00448-RS (ND Cal. Feb. 8, 2013) (Consent Decree and Order for Civil Penalties, Permanent Injunction and Other Relief), FTC Press Release, Feb. 1, 2013 (information obtained from about 3,000 children under 13); United States of America v. Artist Arena, 1:12cv-07386-JGK (SD NY Oct. 3, 2012) (Consent Decree and Order for Civil Penalties), FTC Press Release, Oct. 4, 2012 (information obtained from about 100,000 children under 13); United States of America v. W3 Innovations, CV11-0 3958 (ND Cal. Aug. 12, 2011), FTC Press Release, Aug. 15, 2011 (collected and disclosed personal information on tens of thousands of children under 13).

[385] FTC v. Amazon, 2:14-cv-01038 (WD Washington) (alleging Amazon billed parents for in-app charges without parental consent; pending) (complaint filed July, 10, 2014), Press Release, July 10, 2014; In the Matter of Apple, Before the FTC, FTC Press Release, April 23, 2014 (alleging Apple failed to inform accountholders that entering a password would open a 15-minute window in which children could incur unlimited in-app charges with no further action by accountholder; Apple agreed to refund $32 million to parents); In the Matter of Google, Before the FTC, Docket No. C-4499, Decision and Order (Dec. 2, 2014), FTC Press Release, Dec. 5, 2014 (alleging Google failed to inform accountholders that entering a password to incur in-app charges would open a 30-minute window in which children could make unlimited charges with no further action by accountholder).

[386] In the Matter of Apple, Before the FTC, FTC Press Release, April 23, 2014.

[387] "Every national member bank that receives or will receive non-trust funds is required to obtain FDIC deposit insurance. As a matter of fact, however, federal deposit insurance is virtually a necessity for all depository institutions." Michael Malloy, *Principles of Bank Regulation* 57 (3d ed. 2011) (citations omitted). Accounts at credit unions are insured through the NCUA. 12 USC 1781-89. "The standard insurance amount is $250,000 per depositor, per insured bank, for each account." Fdic.gov. Both principal and interest are insured. Massachusetts chartered savings banks have established a private industry-sponsored insurance company, the Depositors Insurance Fund, that insures deposits above the FDIC insurance amount. www.difxs.com A few banks, however, do not have FDIC insurance. "Suspected Scam Shut Down," 2002 WLNR 14892194, Ariz. Republic, April 5, 2002 (court halted operations of bank chartered by Indian tribe; not subject to FDIC rules); Dan Rutherford, "Tribal Bank Bypasses FDIC Rules on Deposit," 1997 WLNR 6701303, Tulsa World (March 22, 1997); "Dept. of Labor Issues Warning about SD Bank," AP Alert, March 8, 2013 (reporting that bank operating on Indian reservation had no FDIC insurance and was not connected to the tribe), available on WestLaw.

[388] Marc Lane Roark, "Payment Systems, Consumer Tragedy, and Ineffective Remedies," 88 St. Johns L. Rev. 39, 43 n. 11, 44 n. 12 (2014); Sarah Jane Hughes, "Federal Payroll, Gift, and Prepaid Card Developments: FDIC Deposit Insurance Eligibility and the Credit Card Act of 2009," 65 Bus. Law. 261, 263-66 (2009); Loaded with Uncertainty, supra at 9-10.

[389] Insurability of Funds Underlying Stored Value Cards and Other Nontraditional Access Mechanisms, 3 Fed. Reg. 67155 (Nov. 13, 2008).

[390] Those conditions are included in 12 CFR 330.7.

[391] A 2013 survey by The Pew Charitable Trusts found that while most nonbank prepaid card issuers disclosed that they held the funds in FDIC-insured accounts, at least one major issuer, American Express, did not make that disclosure. Imperfect Protection. Professor Wilson later wrote that American Express had subsequently added deposit insurance to its prepaid cards. Catherine Lee Wilson, "Making Prepaid Safe for Consumers: A Framework for Providing Deposit Insurance and Regulation E Protections," at 24, n. 64, available at www.SSRN.org, forthcoming in U. Penn. J. of Business Law. However, as she points out, providing deposit insurance is voluntary and new nonbanks may enter the market and not provide insurance. Ibid, 24. In the absence of deposit insurance, state money transmitter laws provide the only relief consumers might be able to obtain if the company fails. As discussed supra at text accompanying notes 47 & 177 these laws do not adequately protect consumers. Roark suggests requiring non-depository firms to purchase third-party insurance, but also notes the costs of doing so. Roark, supra at 98-99.

[392] Loaded with Uncertainty, supra at 9.

[393] Joe Adler & Rob Blackwell, "Cheat Sheet: Why Google Wallet's FDIC Insurance Matters to Banks," 2015 WLNR 11512721, Am. Banker, April 20, 2015; Woodruff, "Google Wallet funds are now FDIC-insured," Yahoo Finance, April 20, 2015, available at www.finance.yahoo.com. Previously, PayPal funds were protected by FDIC insurance, but PayPal no longer provides this benefit. Ibid.

[394] Wilson, supra at 44-45. One non-FDIC company was a program manager for a prepaid card program. The other was a seller of prepaid cards. See Philip Keitel, "Insolvency Risk in the Network-Branded Prepaid-Card Value Chain," Payment Cards Center, Federal Reserve Bank of Philadelphia, Sept. 2011.

[395] Loaded with Uncertainty, supra at 9-10. "A MoneyPak is a credit that can be purchased at a retailer with cash that then can be used to load or reload funds onto any participating prepaid card." Ibid, 9.

[396] Ibid, 10.

[397] Wilson, supra at 38.

[398] See supra, text accompanying notes 47 and 177; Imperfect Protection, supra at 2-4.

[399] Malloy, supra at 362.

[400] See Jeffrey T. Ferriell & Edward J. Janger, *Understanding Bankruptcy* 92-93 (2d ed. 2007).

[401] Christopher B. Woods, "Stored Value Cards," 59 Consumer Fin. L.Q. Rep. 211, 221 (2005). "Most open prepaid card systems are structured so that the funds underlying the cards are maintained in some form of a trust account, and that is certainly suggested." Ibid.

[402] 11 USC 541 lists the property that is "property of the estate." In A.E.F.S. v. Wiese & Cox, LTD, 51 BR 340 (Bankr. D. Minn. 1985) the consumer division of the Minnesota Attorney General's Office accused a company of engaging in deceptive practices. The company agreed to permit customers to rescind their contracts and receive refunds. The company's law firm established a trust account at a bank. The trustee in bankruptcy demanded that the funds be turned over to the bankrupt's estate. The bankruptcy judge refused to grant the trustee's request, finding that the trust account was not property of the estate. "The entire equitable interest remained in defrauded parties." Ibid, 344.

[403] 11 USC 507(a)(7) & 726(b). The amount of the claim is limited to money on deposit before commencement of the bankruptcy case. In addition, it is currently limited to $2,775. The amount is subject to periodic inflation adjustments and will be readjusted on April 1, 2016.

[404] Roark, supra at 49. See Ferriell & Janger, supra at 376. In June 2015, a petition was filed in the Supreme Court seeking to recover the millions of dollars stored in millions of unredeemed gift cards when Borders filed for bankruptcy. Sara Randazzo, "Unused Borders Gift Cards Spur Fight," Wall St. J., June 29, 2015, at B5. The Texas attorney general has sued RadioShack in its bankruptcy proceeding, alleging that the firm did not inform its

customers they had to file a claim with the court in order to share in any possible recovery for holders of unredeemed gift cards. Ibid.

[405] 11 USC 707. The case also could be dismissed. Ibid.

[406] Roark, supra at 49. See Ferriell & Janger, supra at 376.

[407] Woods, supra at 221. Sharper Image filed for bankruptcy under Chapter 11. The court approved its request to be permitted to honor its gift cards while the bankruptcy was proceeding in order to retain consumer business. The court allowed the company to offer consumers a modified program under which the cards would be honored only if the consumer purchased an item costing twice as much as the value of the gift card. Consumers who chose not to take advantage of this offer would have to take their chances of recovering their money under whatever plan the court ultimately approved. Roark, supra at 49; Sarah Jane Hughes, Stephen T. Middlebrook, & Patricia J. Allouise, "Developments in the Laws Affecting Electronic Payments and Stored-Value Products: A Year of Stored-Value Bankruptcies, Significant Legislative Proposals, and Federal Enforcement Actions," 64 Bus. Law. 219, 221-22 (2008).

[408] Edward I. Altman, "Revisiting the Recidivism-Chapter 22 Phenomenon In the U.S. Bankruptcy System," 8 Brook. J. Corp. Fin. & Com. L. 253, 257 (2014) (empirical study found that 18.25 percent of publicly held companies filed Chapter 11 petitions a second time); Edward I. Altman, "Evaluating the Chapter 11 Bankruptcy Reorganization Process," 1993 Col. Bus. L. Rev. 1, 6 (1993) (empirical study found many publicly held companies do not emerge as continuing entities).

[409] Kenneth M. Misken & Camisha L. Simmons, "Government Addresses Privacy Concerns in Bankruptcy Sales," 31 Am. Bankr. Inst. J 28 (Nov. 2012) available on WestLaw (describing the opposition of state attorneys general to the FTC's settlement with toysmart.com over proposed sale of personal consumer information. Ultimately, one of the company's equity owners purchased the information and destroyed it). Edward J. Janger, "Muddy Property: Generating and Protecting Information Privacy Norms in Bankruptcy," 44 Wm. & Mary L. Rev. 1801, 1805 (2003) (stating that there was public opposition to toysmart.com's proposed sale of personal consumer information). The attorneys general of almost 40 states sought to protect the information on shoppers that RadioShack wanted to sell to hedge fund Standard General. The bankruptcy judge approved an agreement whereby General Wireless, an affiliate of Standard General, could purchase the data subject to substantial limitations. General Wireless was allowed to purchase only about half of RadioShack's 117 million files, and it may not sell the information to or share it with others. RadioShack is required to destroy the remaining files. Furthermore, no credit and debit card numbers may be transferred. Alexei Alexis and Dawn McCarty, "RadioShack Customer Data Sale Accord with States Seen by FTC as Privacy Win," 20 BloombergBNA Electronic Commerce & Law Rep. 799, May 22, 2015.

[410] There appears to be no law outside bankruptcy that specifically addresses consumers' privacy rights to information when a company goes out of business and sells that information. Given the interest of state attorneys general and the FTC in this issue when companies are in bankruptcy, it is reasonable to assume they might act to protect consumers' information when a company liquidates outside bankruptcy. However, it is doubtful that government agencies would learn of a company's intention to sell the information in time to prevent it. The failure of state law to require notice of a proposed sale would make timely intervention unlikely. In addition, even if government agencies could intervene at a meaningful time, lack of resources and higher priority matters likely would preclude them from doing so unless a company had personal information about a great many consumers.

[411] "Personally identifiable information" is defined in 11 USC 101(41A); 11 USC 363(b)(1)(A).

[412] 11 USC 363(b)(1)(B).

[413] 11 USC 332(b).

[414] 11 USC 363(b)(1)(B).

[415] Warren E. Agin, "Reconciling the FTC Act with the Consumer Privacy Ombudsman's Role," 29 Am. Bankr. Inst. J 38 (Oct. 2010), available in WestLaw.

[416] 11 USC 707, 1112.

[417] Merchants must purchase expensive new equipment such as card readers. Makers of the equipment cannot promptly meet the demand. Visa, MasterCard, American Express, and Discover have set an October 2015 deadline for implementation. After that date, liability for fraudulent transactions shifts from the card-issuing banks to the merchants who fail to use terminals that can accommodate chip cards. A trade group representing grocers and pharmacies wants a delay until October 2016. Small banks are finding the transition expensive and complex. Those banks predict they will not issue chip cards to consumers until 2016 or later. Robin Sidel, "Chip-Card Plant Rocks Around Clock," Wall St. J. April 21, 2015, at 1, 2. Some merchants, however, are upgrading their terminals before the October 2015 deadline. These terminals have the technology to accept mobile payments such as Apple Pay and Google Wallet. Jackie Stewart, "EMV Push Spurring Smaller Banks' Interest in Apple Pay," 2015 WLNR 10045508, Am. Banker, April 7, 2015.

[418] Penny Crosman, "Banks Are EMV-Ready but So Are Hackers," Am. Banker, March 19, 2015, at 1. Many merchants probably will not have terminals equipped to take the new cards until at least 2016. Consumers nevertheless will be able to use their new cards because many of the new cards will still have magnetic stripes as well as the chips. Cards with magnetic stripes are more vulnerable to hackers than cards containing only a chip. Ibid, 2.

[419] Ibid, 2. Card-not-present transactions are those where the physical debit or credit card is not swiped through a card reading device. In addition to mobile payments, an example is where a consumer shops from a computer and types the credit or debit card account number and other information onto the online order form. Another example is where the consumer talks to the seller using a traditional landline, providing the information on the card orally. The remote seller relies on that information rather than on the card itself. See generally, www.cardnotpresent.com/news. Even before the widespread migration to EMV cards begins, card-not-present fraud is already a significant problem in the U.S. David Lott, "Is the Conventional Wisdom about EMV Migration Right?" Take On Payments, Federal Reserve Bank of Atlanta, June 8, 2015 (referring to an FRB study that CNP fraud by volume is three times that of card-present fraud).

[420] 12 CFR 1026.12(b).

[421] 15 USC 1643(a). An "accepted credit card" is a "credit card which the cardholder has requested and received or has signed or has used, or authorized another to use, for the purpose of obtaining money, property, labor, or services on credit." 15 USC 1602(m).

[422] 12 CFR 1005.6(b)(1). The consumer gives notice when the consumer "takes steps reasonably necessary to provide the institution with pertinent information." 1005.6(b)(5)(i). "The consumer may notify the institution in person, by telephone, or in writing." 1005.6(b)(5)(ii).

[423] 12 CFR 1005.6(b)(2).

[424] As discussed in the Stage 1 part of this report, see text accompanying note 14-17, an argument can be made that a cellphone capable of initiating debit card transactions is itself an "access device" as defined in the EFTA and Reg. E. If the phone is an access device, consumers have the same protection if their phone is lost or stolen as they do if their cards are lost or stolen. If the courts, Congress, or the CFPB ultimately determine that a cellphone is not an access device, consumers would not have that protection if their cellphone is lost or stolen. Nevertheless, if their phone is lost or stolen and an unauthorized transfer appears on their periodic statement, they would have the same protection as those using debit cards, as long as they notify their financial institution within 60 days.

[425] 12 CFR 1005.6(b)(3).

[426] See supra endnotes 88-90. See infra endnotes 431-41.

[427] Bland, supra at 4-5, 85-86, 178-180, 304-05. Kaplinsky, Levin, & Bryce, supra at 649, 650-56.

[428] 12 USC 5518. Arbitration Study, supra.; Arbitration Study Preliminary Results, supra.

[429] Arbitration Study, supra at Section 1, 9-10.

[430] See supra text accompanying note 180.

[431] Arbitration Study, supra, Section 2, at 26.

[432] Ibid, 44.

[433] Ibid, 45.

[434] Ibid, 48.

[435] Ibid, 53.

[436] Ibid, 74.

[437] Ibid.

[438] Ibid, 35.

[439] Ibid, 33.

[440] Ibid, 59.

[441] Ibid, 68.

[442] Amchem Prod. v. Windsor, 521 US 591, 617 (1997); Stuart T. Rossman, Charles Delbaum, & Arielle Cohen, *Consumer Class Actions* 3-4 (8th ed. 2013).

[443] Rossman et al., supra at 3-4. Another advantages of class actions is their deterrent effect on illegal behavior by others. Ibid.

[444] Rossman et al., supra at 162-64; Jeffrey D. Pilgrim, Katrina S. Christakis, & Candice Voticky, "Class Action Developments," 70 Bus. Law. 669 (2015). See generally, Jean R. Sternlight & Elizabeth J. Jensen, "Using Arbitration to Eliminate Consumer Class Actions: Efficient Business Practice or Unconscionable Abuse?" 67-SPG Law & Contemp. Probs. 75 (2004); Carter, supra at 22.

[445] 12 CFR 1026.6(2)(b)(xv); 1026.7(a)(9).

[446] Official interpretation 12 CFR 1026.12(c)-1.

[447] 12 CFR 1026.12(c)(3)(i)(A). The withholding provision includes Internet orders. Official interpretation 12 CFR 1026.12(c)(1).

[448] 12 CFR 1026.12(c)(1).

[449] Ibid. "The tort limitation was designed to screen out personal injury claims, which might be very large in amount." Michael M. Greenfield, Consumer Law: A Guide for Those Who Represent Sellers, Lenders, and Consumers (1995), at 254. Product liability is another type of tort claim excluded from the withholding provision. Statement of Edward M. Gramlich, member, Board of Governors, Federal Reserve System, before the Senate Banking, Housing and Urban Affairs Committee, May 7, 2005, 2005 WL 1156845.

[450] 12 CFR 1026.12(c)(1). Because of this limitation on the amount the consumer can withhold, there was no need to exclude tort claims to prevent consumers from withholding large amounts. Greenfield, supra at 254.

[451] 12 CFR 1026.12(c)(2).

[452] 12 CFR 1026.12(c)(3)(i)(B).

[453] Ibid.

[454] 12 CFR 1026.12(c)(3)(iii)(A).

[455] 12 CFR 1026.13(a).

[456] 12 CFR 1026.6(b)(2)(xv), 1026.9(a); Appendix G, Model Forms G-3, G-3A & G-4A.

[457] 12 CFR 1026.13(b).

[458] 12 CFR 1026.13(b).

[459] Official interpretation 12 CR 1026.13(a)(1)-3.

[460] 12 CFR 1026.13(c).

[461] 12 CFR 1026.13(d)(1).

[462] 12 CFR 1026.13(e).

[463] 12 CFR 1026.13(f).

[464] 12 CFR 1026.13(g).

[465] 15 USC 1640(a)(1). In several federal circuits cardholders will have a difficult time proving actual damages. The 3d, 5th, 6th, 8th, 9th and 11th Circuits require consumers to prove detrimental reliance. Thompson & Renuart, supra at 811-21.

[466] 15 USC 1640(a)(2). "To obtain statutory damages the consumer need not show that the creditor intended or knew about the violation or that the consumer was deceived. ... Nor need the consumer show any actual damages. Statutory damages may be awarded even after the loan in question has been paid off." Thompson & Renuart, supra at 825-26.

[467] 15 USC 1640(a)(3).

[468] 15 USC 1640(a)(2)(B).

[469] 15 USC 1640(c).

[470] 15 USC 1640(b) and (f).

[471] 12 CR 1005.11(a)(1).

[472] Saunders et al., supra at 167.

[473] 12 CFR 1005.8(b).

[474] 12 CFR 1005.8, Appendix A, Model Form A-3(a).

[475] 12 CR 1005.11(b)(3).

[476] 12 CR 1005.11(c)(1).

[477] 12 CR 1005.11(c)(2).

[478] 12 CR 1005.11(c)(4).

[479] "CFPB Sues Online Payday Lender for Cash-Grab Scam," CFPB Press Release, Sept. 17, 2014, available at www.consumerfinance.gov.

[480] 12 CR 1005.11(d).

[481] 15 USC 1693h(a).

[482] The institution is not liable for its failure to make a transfer where the consumer's account has insufficient funds, the funds are subject to legal process or other encumbrance, the transfer would exceed an established credit limit, an electronic terminal has insufficient cash, or as otherwise provided in Reg. E. 15 USC 1693h(a).

[483] 15 USC 1693h(b).

[484] 15 USC 1693h(c).

[485] 15 USC 1693m(a).

[486] 15 USC 1693m(c).

[487] 15 USC 1693(e).

[488] 15 USC 1693(f).

[489] The institution must receive the consumer's notification within 15 days from the day the institution sends the consumer information related to the debit entry. NACHA Rules, supra, Section 3.11.1.

[490] NACHA Rules, supra, Section 1.9. The originator is the party that authorizes its financial institution to transmit a debit entry to the receiver's account at the Receiver's financial institution. Ibid, Section 8.67. The receiver is the party that authorized the originator to initiate the debit entry. Ibid, Section 8.80.

[491] Saunders et al., supra at 206.

[492] See Security First Network Bank v. C.A.P.S., 2002 WL 485352 (ND Ill. 2002) (case was decided prior to NACHA adopting Section 1.9 in 2008). For other possible arguments that may prove successful, see Saunders Supp., supra at 57-59.

[493] FTC v. Electronic Fin. Group, No. W-03-CA-211 (WD Tex. March 26, 2004) (Stipulated Order for Permanent Injunction & Monetary Judgment) available at www.ftc.gov; State ex rel. McGraw v. Telecheck Serv., 582 SE2d 885 (W.Va. 2003) (action brought by state attorney general).

[494] 15 USC 45(a)(1).

[495] In the Matter of International Harvester Co., 104 FTC 949, 1984 WL 565290, *85 (1984).

[496] 15 USC 45(n).

[497] "Before Dodd-Frank, the FDIC had explicit authority to enforce the FTC Act over its regulated banks. 15 USC §57(f). Curiously, Dodd-Frank repealed this explicit enforcement authority but preserved the exemption for banks from FTC enforcement authority. 15 USC §45(a)(1). Although one could read this legislative action as contemplating a complete removal of UDAP enforcement authority from the FDIC, the FDIC has affirmed its authority to prevent unfair or deceptive acts and practices generally under §8 of the FDI Act." Catherine M. Sharkey, "Agency Coordination in Consumer Protection," 2013 U. Chi. Legal F. 329, 339 n. 38 (2013). See endnote 60, supra, describing an interagency guidance regarding the continuing authority of an FTC Rule and the FRB's assertion of more general authority in respect to unfair and deceptive acts or practices.

[498] CFPB Supervision and Examination Manual, Version 2, Oct. 2012, at UDAAP 5-6. CFPB Bulletin 2012-06, Marketing of Credit Card Add-On Products, July 18, 2012. See Sandra D. Hauser et al., "Lessons Learned from the First Public CFPB Enforcement Action and Bulletin 2012-06," 66 Consumer Fin. L. Q. Rep. 390, 402 (2012).

[499] 12 USC 5531(c).

[500] 12 USC 5531(d).

[501] 12 USC 5531(c).

[502] Carolyn Carter, "Consumer Protection in the States, A 50–State Report on Unfair and Deceptive Acts and Practices Statutes," National Consumer Law Center, Inc., Feb. 2009 at 21.

[503] The states are Arizona, Delaware, Iowa, South Dakota and Wyoming. Ibid.

[504] Carter & Sheldon, supra at 770 (8th ed. 2012). The states are Alabama, Georgia, Iowa, Louisiana, Mississippi, Montana, South Carolina, Tennessee, and Virginia. Carter, supra at 22.

[505] Carter, supra at 22. The states are Florida and Oregon.

[506] Carter & Sheldon, supra at 651-66. The states are Colorado, Georgia, Minnesota, Nebraska, New York, South Carolina, and Washington. Carter, supra at 22; The reliance requirement is clear in the statutes of Indiana, Texas and Wyoming. It is less clear from court decisions in other states. Carter, supra at 22. For example, while Georgia courts require reliance, several trial courts in Virginia, but not all, require it. California courts require reliance for some claims, but not for others. Carter & Sheldon, supra at 225-27.

[507] The states exempting banks are Alabama and Florida. Carter, supra at 14. The states exempting creditors are Alabama, Alaska, Arkansas, Florida, Illinois, Nebraska, Ohio, Oklahoma, Oregon, Tennessee, Utah, Washington, West Virginia, and Wisconsin. Ibid.

[508] Arkansas and Tennessee exempt all regulated industries. Carter, supra at 14. Other states exempt certain industries such as insurance and utilities. The extent of the exemption depends on the precise language of the statute and the relationship between statutes. Carter & Sheldon, supra at 81-102. For example, some states have enacted both a UDAP law and a statute prohibiting unfair and deceptive insurance practices (UNIP statutes). The UNIP laws provide far less protection for consumers. State courts have disagreed on whether their UNIP statute completely replaces their UDAP statute, or whether both apply, the UDAP law providing consumers relief where the UNIP law does not. Ibid, 83-84.

[509] Carter, supra at 17.