ConsumersUnion®
POLICY & ACTION FROM CONSUMER REPORTS

CFA Consumer Federation of America

May 22, 2012

Federal Trade Commission
600 Pennsylvania Ave,
Washington, D.C. 20580

Re: Comments on the Legal Landscape and Dispute Resolution for *Paper, Plastic…or Mobile?* (Project No. 124808)

Consumers Union, the policy and advocacy arm of Consumer Reports, and the Consumer Federation of America (CFA) are pleased to contribute to the discussion on the legal and regulatory framework for consumer protections for mobile payments at FTC workshops such as *Paper, Plastic…or Mobile?* These workshops and convenings are necessary to increase dialogue between stakeholders to help focus on ensuring that consumers are provided with the strongest protections when payments are made with a mobile device. We offer the following comments, which can be found in greater discussion in *Mobile Pay or Mobile Mess: Closing the Gap Between Mobile Payment Systems and Consumer Protections* found at http://www.consumersunion.org/pdf/Mobile-Pay-or-Mobile-Mess.pdf.

The ability to pay with a mobile device is exciting due to its potential ease and convenience, but consumers need to know that they may find themselves at risk for financial loss if a mobile device is lost or stolen or if erroneous charges are incurred due to fraud or mistake. Currently, consumers are left to figure out on their own what types of protections might be provided in the event they discover unauthorized use or an error that resulted from a mobile payment transaction. Consumers are unlikely to know what to do, who to call or what rights they have after discovering unauthorized activity or other errors on their statements or receipts.

What Protections Do Consumers Need?

Consumers should have the strongest guaranteed protections against unauthorized use and other errors regardless of the payment method used for the mobile payment transaction. These protections include:

- Ability to dispute any unauthorized transaction, whether it was a result of a lost or stolen phone or if a merchant error was discovered on a mobile phone statement; and
- Ability to withhold payment of disputed amounts; or
- Ability to obtain recredit in a timely fashion if payment has already paid for the disputed transaction.

Consumer Protections Can Vary Widely for Mobile Payments

Today, the protections a consumer is entitled to receive in the event of an unauthorized transaction or other error *depend upon the payment method* used to fund or linked to the mobile payment transaction. Consumers who link mobile payments to credit cards have the strongest rights, with the greatest caps on liability, the ability to withhold payment of disputed amounts and the right to prompt recredit. Consumers who link their mobile payments to debit cards or bank accounts have the second best set of consumer protections which include limits on liability and the right to recredit within a specified period of time.

West Coast Office
1535 Mission Street • San Francisco, CA 94103-2512
(415) 461-6747• (415) 431-0906 (fax)
www.consumersunion.org

On the other hand, consumers who link their mobile payments to general purpose prepaid cards and gift cards don't have the same guaranteed protections as credit and debit cards. The same applies to mobile payments that are debited directly from a prepaid mobile account or are charged to a mobile phone bill. These payment methods are likely limited to voluntary protections, which may provide no protection at all.

The need to fill the gaps in current regulations is more pressing as mobile phones become ubiquitous and mobile payments rise in popularity. It should not matter to the consumer which payment method is used to make the transaction with a mobile phone. But when a thief uses a stolen mobile phone to pay, or when the wrong amount is billed, or when goods are not delivered as promised, the method of payment can matter a lot because of the disparate protections afforded by each. The payment method the consumer chooses can determine whether, and to what extent, the consumer has a right to get his or her money back.

Mobile Payments Linked to a Credit Card Offer the Strongest Protections
Transactions made with mobile phone payments linked to credit cards are provided the strongest consumer protections.

If a consumer makes a purchase with a mobile phone and the charge goes to the consumer's credit card account, the consumer will receive all of the same protections that apply to a traditional credit card transaction. Federal regulations protect consumers from charges that the consumer did not authorize, whether or not the credit card itself was used in the transaction.[1]

When a consumer links a mobile payment to a credit card, the consumer's liability is limited to no more than $50 for unauthorized credit card charges resulting from a lost or stolen credit card, which in mobile payments can include the phone itself, a chip in the phone or a sticker on the phone.[2] If a billing error appears on a consumer's periodic statement, there is no liability as long as the consumer reports the error within 60 days.[3] With credit card transactions, consumers also have the right to reverse a charge if the goods or services were not delivered as agreed or not accepted by the consumer or his or her designee. Usually this will be for non-delivery, defect, or delivery of the wrong item. This is commonly called a "chargeback" right. Mobile payments linked to credit cards would enjoy these same chargeback rights.

Mobile Payments Linked to Debit Cards or Bank Accounts Have the Second Best Protections
Mobile payments linked to debit cards or bank accounts have mandatory protections but these safeguards are less complete compared to mobile payments linked to credit cards.
The law provides consumers paying with debit cards the right to get their money back but doesn't provide chargeback rights if the goods and services are defective or not delivered as promised. If the mobile phone, chip or other mobile payment device is lost or stolen, the consumer's liability for unauthorized transactions is limited by statute to $50 if the consumer makes a report within two business days from the date the unauthorized transaction occurred.[4]

---

[1] *See* 15 U.S.C. § 1666(b) (2006 & Supp. V), 12 C.F.R. § 226.13(a) (2011) (both defining "billing error" to include unauthorized transactions and transactions that are the subject of a good faith dispute with a merchant about acceptability or delivery of goods and services).
[2] Regulation Z's official staff interpretations state that "credit card" includes a "card or device that can be activated upon receipt to access credit." Official Staff Interpretations, 12 C.F.R. § 226, Subpart G (*see* definition of "credit card," 12 C.F.R. § 226.2(a)(15)). If a mobile phone is set up to access the credit account and then is lost or stolen, the consumer should be liable for no more than $50 in unauthorized transactions.
[3] § 226.13(b)(1).
[4] 12 C.F.R. § 205.6(b)(2). "Access device" is defined as "a card, code, or other means of access to a consumer's account…that may be used by the consumer to initiate electronic fund transfers." § 205.2(a)(1); Regulation E,

If the consumer reports a lost or stolen phone after two days, liability can reach $500 or more.[5] If a consumer finds an unauthorized charge on the bank statement and the phone was not lost or stolen, the consumer won't lose any money as long as the error is reported within 60 days.[6] This time period may be extended for extenuating circumstances.[7] Consumers have another important right when the mobile payment is linked to a debit card or bank account, which is the right to be recredited missing funds from unauthorized transactions within 10 business days.[8]

Mobile Payments Linked to General Use Prepaid Cards Have No Guaranteed Protections
Consumers who use mobile payments that are tied to prepaid cards, or general purpose reloadable prepaid cards,[9] have no guaranteed protections if something goes wrong with the transaction and may have unlimited liability.

Consumers who link mobile payments to prepaid cards do not receive mandatory protections from consumer liability for unauthorized transactions or other errors. Prepaid cardholders do not have a mandatory right of recredit for missing funds, and will likely not get their money back unless the prepaid card company voluntarily provides it.[10] These prepaid cards may have some protections by contract; however, they are voluntary and can be rescinded at any time by the prepaid card issuer.

Additionally, prepaid cardholders may be provided assurances from Visa and MasterCard, two major card networks that their cardholders, including prepaid cardholders, can be worry free and have peace of mind with their zero liability policies. Visa's Zero Liability policy states it will protect cardholders from unauthorized use, and requires financial institutions "to extend provisional credit for losses from unauthorized use within five business days of notification of the loss."[11] MasterCard has a similar Zero Liability policy which will not hold "you responsible for 'unauthorized purchases'."[12]

However, voluntary consumer protections like Visa and MasterCard's zero liability policies are insufficient. For instance, prepaid card holders may be subject to the whims

---

Official Staff Interpretations, 12 C.F.R. § 205, Supplement I. Therefore, a lost or stolen mobile phone will be a lost or stolen "access device" for the purposes of Regulation E.

[5] § 205.6(b)(2). If the consumer reports a lost or stolen access device after two business days, liability is capped at the lesser of: (1) $500, or (2) "[t]he amount of unauthorized transfers that occur after the close of two business days and before notice to the institution, provided the institution establishes that these transfers would not have occurred had the consumer notified the institution within that two-day period." *Id.*

[6] § 205.6(b)(3).

[7] § 205.6(b)(4).

[8] If a consumer reports an error, the consumer's bank must recredit the disputed amount within the lesser of: (1) 10 business days, or (2) one business day after the bank determines that there was an error. 15 U.S.C. §§ 1693f(b-c), 12 C.F.R. § 206.11(c)(1)(i). Consumers Union recommends shortening this period to five days. *See* Consumers Union, Protecting Our Wallets: Consumers Union Recommends Priority Areas for the Consumer Financial Protection Bureau's First Year, http://www.defendyourdollars.org/pdf/Recommended-Priorities-for-the-CFPB.pdf.

[9] General purpose reloadable cards are network branded prepaid cards that can be used to withdraw funds from ATMs, used at a point-of-sale, and have other capabilities similar to debit cards tied to bank accounts. For more information on prepaid cards, *see* Michelle Jun, *Prepaid Cards: Second-Tier Bank Account Substitutes*, Sept 2010, available at http://www.defendyourdollars.org/pdf/2010PrepaidWP.pdf .

[10] Regulation E's official staff interpretations appear to exempt funds in pooled accounts from the definition of "accounts" covered by the regulation. *See* Official Staff Interpretation of 12 C.F.R. § 205.2(b)(3), 12 C.F.R. § 205, Supplement I. This is an accident of history, as prepaid cards are a recent phenomenon.

[11] Visa Zero Liability, http://usa.visa.com/personal/security/visa_security_program/zero_liability.html (last visited June 7, 2011).

[12] MasterCard Zero Liability, http://www.mastercard.us/zero-liability.html (last visited June 7, 2011).

of customer service representatives' knowledge of the policies.[13] Plus, these policies have significant loopholes. Visa's Zero Liability policy does not cover ATM transactions or PIN transactions that are not processed on the Visa network.[14] Card transactions may take place on other networks even if the card has a Visa logo.[15] MasterCard's Zero Liability policy also has loopholes. That policy doesn't give any protection if a consumer reported more than two or more unauthorized events in the past 12 months. It also does not cover ATM or PIN transactions and may not apply if the consumer did not register the card with MasterCard.[16]

Mobile Payments Linked to Gift Cards Are Not Protected From Unauthorized Transactions
Consumers who link mobile payments to gift cards will not likely be able to recover lost funds due to unauthorized transactions or errors. Mobile payments linked to gift cards, which include bank-issued (network-branded) gift cards and single merchant gift cards do not receive protections under federal law or regulation for unauthorized transactions or errors. consumers who use mobile payments applications that are linked to gift cards could lose all their gift card funds if the phone is lost or stolen and a thief uses it to purchase goods with the funds linked to the gift card application. Consumers are then subject to the gift card mobile application's terms and conditions and must comply with the terms in order to possibly redeem any missing funds as a result of unauthorized activity or error.

Federal laws and regulations do not provide protections against unauthorized transactions or other errors for gift cards.[17] While there are consumer protections against expiration dates and many types of fees on gift cards, there are no guarantees that the consumer will be able to recoup gift card funds if they are missing due to theft or as a result of other errors.

Mobile Payments Linked to Phone Bills Offer Unclear Protections:
Consumers who use mobile payment products that debit a prepaid mobile account or send a charge to a mobile phone account will likely only have voluntary protections from the wireless carrier's contract. It is unclear what recourse a consumer has when a payment is linked to a prepaid deposit to a wireless carrier (prepaid) or to a phone bill that the consumer pays at the end of the billing cycle which is usually on a month-to-month basis (postpay). Interstate and international telephone services are regulated by the Federal Communications Commission (FCC), but the FCC does not have regulations on mobile payments ("non-telephone services") charged to a prepaid deposit or phone bill.[18] As a result, consumers making mobile payments

---

[13] "A voluntary policy is subject to the risk of uneven application and to the discretion of employees about how and when to apply the policy, which may disadvantage consumers whose primary language is not English, who are less able to spend time on the phone with customer service due to the nature of their jobs, or who are less able to write a persuasive letter describing the problems—in many cases, the very consumers to whom prepaid debit cards are being marketed as account substitutes." Gail Hillebrand, *Before the Grand Re-thinking: Five Things to Do Today With Payments Law and Ten Principles to Guide New Payments Products and New Payments Law*, 83 Chi.-Kent L. Rev. 769, 790 (2008).

[14] Visa, *supra* note 41.

[15] A merchant's financial institution chooses a network to process debit transactions.

[16] MasterCard, *supra* note 42.

[17] For a more in depth discussion on expanding gift card protections *see* Gail Hillebrand, *Before the Grand Re-thinking: Five Things to Do Today With Payments Law and Ten Principles to Guide New Payments Products and New Payments Law*, 83 Chi.-Kent L. Rev. 769, 790 (2008).

[18] The FCC's authority to write rules protecting consumers against billing errors extends to "telephone-billed purchases," defined as "any purchase that is completed solely as a consequence of the completion of the call or a subsequent dialing, touch tone entry, or comparable action of the caller." 15 U.S.C. § 5724(1) (2006 & Supp. V). It is at best unclear whether text message payments would be covered. The FCC's consumer resources page on "cramming" directs consumers to contact the FCC with complaints regarding interstate or international telephone

linked to a prepaid phone account or to their postpay mobile accounts may have no guaranteed consumer protections in the event of an unauthorized transaction or error. Consumers may be entitled to protections provided by state laws or public utility agency rules, but those safeguards vary from state to state.

So far, only one state agency has taken steps to provide stronger consumer protections for mobile payments linked to mobile phone accounts. The California Public Utilities Commission (CPUC) issued a rule in late 2010 that now provides California residents the right to reverse charges, similar to a chargeback right, for unauthorized charges for goods and services made to prepaid or postpaid mobile phone accounts. Under the CPUC rule, phone companies must give California consumers notice and a chance to opt out of allowing third parties (e.g., a ringtone download store or charitable organization) to put charges on the phone bill.[19] Even if a consumer does allow third party charges, the consumer is not responsible for unauthorized charges. If the consumer disputes a charge, it is presumed unauthorized – the phone company has to prove otherwise before it can hold the consumer responsible for the disputed charge. While an investigation is pending, the consumer does not have to pay the charge. If it has already been paid, the carrier must either verify the charge or recredit the consumer's account within 30 days.

A few simple fixes to existing federal regulations will provide consumers with the strongest protections regardless of what type of payment method is used to make purchases with mobile devices. Regulations E and Z provide consumer protections from unauthorized transactions due to lost or stolen payment devices or other errors, the right of recredit, chargeback rights and limits on liability when they make payments using a credit card, debit card, or funds from their bank accounts. Regulation E ensures that consumers who link mobile payments to debit cards or bank accounts have limited liability for unauthorized transactions and errors, and a right to prompt recredit of missing funds while an investigation in pending. Regulation Z ensures that consumers who link mobile payments to credit cards have limited liability for unauthorized transactions and billing errors, a right to reverse a charge and withhold payment when goods and services are not delivered as agreed or not accepted by the consumer. The Consumer Financial Protection Bureau (CFPB) should clarify that Regulation E covers mobile payments debited against prepaid cards and prepaid phone deposits. The CFPB should also extend Regulation Z protections to mobile payments charged to wireless bills.

States can also play an important role by directly providing their residents with stronger protections for direct to mobile billing. States should follow California's lead by providing consumers with chargeback rights similar to those associated with credit cards. Consumers should be entitled to withhold payment of disputed or "unauthorized" charges. If the disputed charge has already been paid, the consumer should be credited within 30 days. Additionally, consumers should be able to "opt out" of allowing third parties to place charges on the wireless bill.

Until laws and regulations are changed to provide guaranteed protections to all ways to pay by mobile phone, mobile payment service providers can provide stronger protections similar to

---

services, but advises contacting the Federal Trade Commission instead if they find "non-telephone" service charges. *See* Fed. Commc'n Comm'n, Unauthorized, Deceptive or Misleading Charges Placed on Your Telephone Bill, http://www.fcc.gov/cib/consumerfacts/cramming.html.

[19] Cal. Pub. Util. Comm'n, Order Instituting Rulemaking on the Commission's Own Motion to Establish Consumer Rights and Consumer Protection Rules Applicable to All Telecommunications Utilities (Oct. 28, 2010), *available at* http://docs.cpuc.ca.gov/PUBLISHED/FINAL_DECISION/125959.htm (CPUC ORDER).

those described above through contract and product features. For example, consumers should also be able to place a cap on the dollar amount for mobile payments that are directly made to wireless accounts. Wireless companies such as Sprint and CREDO Mobile have an Account Spending Limit, which is a temporary or permanent cap (typically based on credit history, payment history, or to prevent fraud) placed on the amount of unpaid charges that can be accumulated on a consumer's account.[20] Another carrier, Liberty Wireless sets out an established limit of no more than $100 per day to be added to the account and is capped at $250.[21] Consumers should have such additional control over third party transactions that can be made directly to their wireless bills.

Conclusion

We appreciate this opportunity to provide our comments for the need to provide consumers with the strongest protections when making payments with mobile devices. Consumers need consistent and guaranteed protections regardless of the mobile payment method or product used. Whether consumers link their mobile payments to credit cards, debit cards, prepaid cards, gift cards or bill directly to their mobile phones, consumers should have strong guaranteed protections against losing their money if their mobile device is lost or stolen, or used to make unauthorized payments, or for other erroneous charges due to fraud or mistake.

Michelle Jun
Senior Attorney
Consumers Union

Susan Grant
Director of Consumer Protection
Consumer Federation of America

[20] CREDO Mobile Customer Agreement, http://www.credomobile.com/misc/Customeragreement.aspx (last visited June 8, 2011) and Sprint Service Agreement, https://manage.sprintpcs.com/output/en_US/manage/MyPhoneandPlan/ChangePlans/popLegalTermsPrivacy.htm (last visited June 8, 2011).

[21] Liberty Wireless Terms and Conditions, http://www.libertywireless.com/ (last visited June 8, 2011).