

**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**

**Comments of the Staff of the Bureau of Consumer Protection\***

**September 10, 2014**

---

**\*These comments represent the views of the staff of the Bureau of Consumer Protection. They are not necessarily the views of the Commission or any individual Commissioner. The Commission has, however, voted to authorize the staff to submit these comments.**

## I. INTRODUCTION

Federal Trade Commission (FTC or Commission) staff files this comment in response to the Consumer Financial Protection Bureau's (CFPB) June 12, 2014 Request for Information (RFI) seeking comment on the use of mobile financial services by consumers and economically vulnerable populations to access products and services, manage their finances, and achieve their financial goals.<sup>1</sup> In its RFI, the CFPB also seeks information about barriers to low-income, underserved, or economically vulnerable customers accessing mobile technology for financial services, as well as any potential consumer protection issues associated with the use of such technology.<sup>2</sup> The CFPB seeks this information to inform its consumer education and empowerment strategies in these areas.<sup>3</sup>

Over the past two decades, one of the FTC's top priorities has been to address consumer protection issues raised by new technologies, including mobile products and services. Since the emergence of the mobile marketplace, the FTC has brought law enforcement actions, written reports, conducted surveys, and issued consumer and business guidance in this area. FTC staff supports the CFPB's efforts to explore the impact of mobile financial services on traditionally underserved communities, and provides this comment to highlight the consumer protection issues and to make recommendations based on the FTC's experience in this topic area.

Mobile technologies provide consumers with unprecedented efficiency and convenience to conduct financial transactions.<sup>4</sup> Consumers can check their bank balances on the go, make purchases using their mobile devices, and even receive discounts based on their location. Some mobile technologies, such as mobile carrier billing, may be especially beneficial for unbanked and underbanked consumers. At the same time, consumers using mobile financial services may be at risk for liability for unauthorized charges or unfair billing, as well as the increased collection, use, and sharing of consumers' personal and financial data. These issues may raise particular concerns for the underserved or economically vulnerable consumers using these services.

This comment highlights five potential consumer protection concerns raised by mobile financial services and discusses steps the FTC has taken to address them. They are: (1) the potential liability for unauthorized charges using prepaid or stored value products; (2) the unfair billing practices on mobile carrier bills; (3) the privacy of consumers' personal and financial data; (4) the security of consumers' personal and financial data; and (5) the potential use of consumers' information by data brokers and other third parties.

---

<sup>1</sup> *Request for Information Regarding the Use of Mobile Financial Services by Consumers and Its Potential for Improving the Financial Lives of Economically Vulnerable Consumers*, 79 Fed. Reg. 33731 (June 12, 2014).

<sup>2</sup> *Id.* The CFPB limits its request to mobile financial services and seeks comment on mobile point of sale payments only as they relate to low-income and underserved consumers. *See id.* at 33731.

<sup>3</sup> *Id.* at 33731.

<sup>4</sup> FED. TRADE COMM'N, WHAT'S THE DEAL? A FTC STUDY ON MOBILE SHOPPING APPS, at 3 (Aug. 2014), available at <http://www.ftc.gov/system/files/documents/reports/whats-deal-federal-trade-commission-study-mobile-shopping-apps-august-2014/140801mobileshoppingapps.pdf>.

## II. FTC AUTHORITY AND ACTIVITY IN THE AREA OF MOBILE COMMERCE

Beginning in 2002, the FTC has examined the benefits and consumer protection challenges associated with consumers' increasing use of mobile commerce. Through workshops,<sup>5</sup> reports,<sup>6</sup> and law enforcement actions,<sup>7</sup> the FTC has worked to ensure that consumer protections keep pace as mobile commerce transitions from concept to reality.<sup>8</sup> More recently, at its April 2012 workshop addressing mobile payments, *Paper, Plastic...or Mobile*, FTC staff convened experts with a range of perspectives to explore the consumer protection issues that arise in connection with mobile payments.<sup>9</sup> Following the workshop, FTC staff released a report in March 2013 (Mobile Payments Report) that highlighted the key areas for consumer concern discussed at the workshop, including the importance of clear disclosures about dispute resolution and liability limits and the need for mobile payment companies to provide greater transparency surrounding their data practices.<sup>10</sup> In particular, the report recognized the comparatively heavy use of mobile financial products by underbanked consumers.<sup>11</sup>

---

<sup>5</sup> See *Mobile Cramming: An FTC Roundtable*, FED. TRADE COMM'N (May 2013) (Workshop), available at <http://www.ftc.gov/bcp/workshops/mobilecramming/>; *Paper, Plastic...or Mobile*, FED. TRADE COMM'N (April 2012) (Workshop), available at <http://www.ftc.gov/bcp/workshops/mobilepayments/>; *Pay on the Go: Consumers and Contactless Payment*, FED. TRADE COMM'N (July 2008) (Workshop), available at <http://www.ftc.gov/bcp/workshops/payonthego/index.shtml>; *Protecting Consumers in the Next Tech-ade*, FED. TRADE COMM'N, (Nov. 2006) (Workshop), available at <http://www.ftc.gov/bcp/workshops/techade/what.html>; *The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues*, FED. TRADE COMM'N (Dec. 2000) (Workshop), available at <http://www.ftc.gov/bcp/workshops/wireless/index.shtml>.

<sup>6</sup> See FED. TRADE COMM'N, WHAT'S THE DEAL? A FTC STUDY ON MOBILE SHOPPING APPS (Aug. 2014), available at <http://www.ftc.gov/system/files/documents/reports/whats-deal-federal-trade-commission-study-mobile-shopping-apps-august-2014/140801mobileshoppingapps.pdf>; FED. TRADE COMM'N, MOBILE CRAMMING: AN FTC STAFF REPORT (July 2014), available at <http://www.ftc.gov/system/files/documents/reports/mobile-cramming-federal-trade-commission-staff-report-july-2014/140728mobilecramming.pdf>; FED. TRADE COMM'N, PAPER, PLASTIC...OR MOBILE (Mar. 2013), available at [http://www.ftc.gov/sites/default/files/documents/reports/paper-plastic-or-mobile-ftc-workshop-mobile-payments/p0124908\\_mobile\\_payments\\_workshop\\_report\\_02-28-13.pdf](http://www.ftc.gov/sites/default/files/documents/reports/paper-plastic-or-mobile-ftc-workshop-mobile-payments/p0124908_mobile_payments_workshop_report_02-28-13.pdf); FED. TRADE COMM'N, RADIO FREQUENCY IDENTIFICATION: APPLICATIONS AND IMPLICATIONS FOR CONSUMERS (Mar. 2005), available at <http://www.ftc.gov/sites/default/files/documents/reports/rfid-radio-frequency-identification-applications-and-implications-consumers-workshop-report-staff/050308rfidrpt.pdf>.

<sup>7</sup> See *Credit Karma, Inc.*, FTC File No. 1323091 (F.T.C. Mar. 28, 2014), available at <http://www.ftc.gov/enforcement/cases-proceedings/132-3091/credit-karma-inc>; *Fandango, LLC*, FTC File No. 1323089 (F.T.C. Mar. 28, 2014), available at <http://www.ftc.gov/enforcement/cases-proceedings/132-3089/fandango-llc>; *Apple, Inc.*, FTC File No. 1123108 (F.T.C. Mar. 25, 2014), available at <http://www.ftc.gov/enforcement/cases-proceedings/112-3108/apple-inc>; *FTC v. Wise Media, LLC*, No. 1:13-cv-1234 (N.D.Ga. Apr. 16, 2013), available at <http://www.ftc.gov/enforcement/cases-proceedings/122-3182/wise-media-llc-et-al>; *FTC v. Tatto, Inc.*, No. 2:13-cv-08912-DSF-FFM (C.D.Ca. Dec. 16, 2013), available at <http://www.ftc.gov/enforcement/cases-proceedings/112-3181/tatto-inc-also-dba-winbigbidlow-tatto-media-et-al>; *FTC v. Jesta Digital, LLC*, No. 1:13-cv-01272-JDB (D.C. Aug. 21, 2013), available at <http://www.ftc.gov/enforcement/cases-proceedings/112-3187/jesta-digital-llc-also-dba-jamster>.

<sup>8</sup> Additional information about the FTC's consumer protection mission, enforcement actions, and outreach initiatives is accessible for desktop and mobile devices in English at <http://www.consumer.ftc.gov/> and Spanish at <http://www.consumidor.ftc.gov/>.

<sup>9</sup> *Paper, Plastic...or Mobile* Workshop, *supra* note 5.

<sup>10</sup> PAPER, PLASTIC...OR MOBILE, *supra* note 6 at 5-7, 11-15.

<sup>11</sup> *Id.* at 4 (citing BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, CONSUMERS AND MOBILE FINANCIAL SERVICES (Mar. 2012), available at <http://www.federalreserve.gov/econresdata/mobile-device-report-201203.pdf>).

FTC staff has continued to make emerging mobile technology issues a priority by hosting additional workshops on topics such as mobile cramming, mobile security, and mobile location services, as well as pursuing enforcement actions under Section 5 of the FTC Act alleging deceptive and unfair practices in the mobile marketplace.<sup>12</sup> The sections below address various topics raised by the CFPB's RFI and share the FTC's expertise from over a decade of working in this area.

### **III. CONSUMER PROTECTION ISSUES WITH THE USE OF MOBILE FINANCIAL SERVICES**

#### **A. Concerns About Potential Liability for Unauthorized Charges Using Prepaid or Stored Value Products<sup>13</sup>**

Many transactions on mobile devices – notably, those made using prepaid or stored value accounts – are generally not protected by the statutory and/or contractual liability limits that consumers might expect. Consequently, it is imperative that consumers be able to learn about their rights and protections before using a service to make a payment via their mobile device.

Federal laws limit consumers' liability for unauthorized charges in many contexts, but protections can vary based on how consumers fund or process their mobile payment transactions or purchases.<sup>14</sup> In particular, when a consumer makes a purchase through a mobile payment app by placing a charge directly on a credit or debit card that is associated with that app, the consumer is protected by the same federal liability limits applicable to physical credit or debit cards.<sup>15</sup> However, these statutory protections generally do not apply 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.<sup>16</sup> Instead, for these transactions, consumers must rely on whatever protections, if any, are voluntarily provided by the prepaid card or mobile app provider.<sup>17</sup>

In a recent report, *What's the Deal? An FTC Report on Mobile Shopping Apps*, (Mobile Shopping Apps Report), FTC staff looked at the information available to consumers, prior to download, about liability limits and dispute procedures when using apps that permit in-store

---

<sup>12</sup> A full list of the FTC mobile technology initiatives and enforcement matters can be found at <http://www.ftc.gov/news-events/media-resources/mobile-technology>.

<sup>13</sup> The RFI seeks comment on the use of prepaid products by low-income consumers for their daily financial transactions as well as the opportunities and risks of such products. RFI, *supra* note 1, at 33733.

<sup>14</sup> See PAPER, PLASTIC... OR MOBILE, *supra* note 6, at 5-7 (cited in *WHAT'S THE DEAL? A FTC STUDY ON MOBILE SHOPPING APPS*, *supra* note 4, at 11).

<sup>15</sup> *Id.*

<sup>16</sup> *Id.*

<sup>17</sup> See *id.* See also FED. TRADE COMM'N, Staff Comments, *In the Matter of Request for Comment on Advance Notice of Proposed Rulemaking Electronic Fund Transfers (Regulation E) and General Purpose Reloadable Prepaid Card*, Docket No. CFPB-2012-0019, at 2-3 (July 23, 2012), available at [http://www.ftc.gov/sites/default/files/documents/advocacy\\_documents/ftc-staff-comment-consumer-financial-protection-bureau-concerning-electronic-fund-transfers/120730cfpbstaffcomment.pdf](http://www.ftc.gov/sites/default/files/documents/advocacy_documents/ftc-staff-comment-consumer-financial-protection-bureau-concerning-electronic-fund-transfers/120730cfpbstaffcomment.pdf) (highlighting some of the consumer protection issues surrounding general purpose reloadable accounts, including liability limits for fraudulent or unauthorized transactions).

mobile payments.<sup>18</sup> FTC staff examined the disclosures of those apps that allowed consumers to pass charges to prepaid and gift cards, as well as apps that allowed consumers to use their credit or debit cards to fund stored value accounts within the app to make subsequent purchases.<sup>19</sup> Almost half of the 30 in-store purchase apps did not disclose whether they had any dispute resolution or liability limits policies prior to download.<sup>20</sup> Further, of the 16 apps that provided pre-download information about dispute resolution procedures or liability limits, only nine offered any written protections for their users and seven disclaimed all liability.<sup>21</sup> Given the lack of alternative remedial avenues for stored-value service users, the report encourages consumers to look for those mobile payment services that disclose upfront how the payment service works and what consumers can do if they encounter a problem.<sup>22</sup> Staff also reiterated its recommendation from the Mobile Payments Report that companies provide clear dispute resolution and liability limits information to their customers, particularly when using a stored value method to process payments.<sup>23</sup>

Similarly, in its comment to the CFPB's advance notice of proposed rulemaking relating to prepaid cards,<sup>24</sup> FTC staff highlighted the lack of specific liability limiting protections for unauthorized use of general purpose reloadable (GPR) prepaid accounts. The FTC comment maintained that students and the unbanked are among the greatest users of GPR accounts, and more mobile service providers are focusing services on the unbanked, who tend to use GPR prepaid accounts as substitutes for bank accounts.<sup>25</sup> Therefore, it is important for these groups to receive adequate information on the scope of their potential liability.<sup>26</sup>

---

<sup>18</sup> WHAT'S THE DEAL? A FTC STUDY ON MOBILE SHOPPING APPS, *supra* note 4, at 11.

<sup>19</sup> *See id.* at 13.

<sup>20</sup> *Id.* at 11.

<sup>21</sup> *Id.*

<sup>22</sup> *See id.* at 15; *see also, Is your shopping buddy app-y?*, Fed. Trade Comm'n (Aug. 1, 2014), available at <http://www.consumer.ftc.gov/blog/your-shopping-buddy-app-y>.

<sup>23</sup> WHAT'S THE DEAL? A FTC STUDY ON MOBILE SHOPPING APPS, *supra* note 4, at 14-15 (citing PAPER, PLASTIC... OR MOBILE, *supra* note 6, at 5-7).

<sup>24</sup> *Advance Notice of Proposed Rulemaking (ANPR) for Electronic Fund Transfers (Regulation E)*, 77 Fed. Reg. 30923 (May 24, 2012).

<sup>25</sup> FED. TRADE COMM'N, Staff Comments, *In the Matter of Request for Comment on Advance Notice of Proposed Rulemaking Electronic Fund Transfers (Regulation E) and General Purpose Reloadable Prepaid Card*, Docket No. CFPB-2012-0019, at 2, n. 22-24 (July 23, 2012), available at [http://www.ftc.gov/sites/default/files/documents/advocacy\\_documents/ftc-staff-comment-consumer-financial-protection-bureau-concerning-electronic-fund-transfers/120730cfpbstaffcomment.pdf](http://www.ftc.gov/sites/default/files/documents/advocacy_documents/ftc-staff-comment-consumer-financial-protection-bureau-concerning-electronic-fund-transfers/120730cfpbstaffcomment.pdf).

<sup>26</sup> The Mobile Shopping Apps Report also noted that even if the CFPB were to extend Regulation E protections to GPR cards, it is not clear whether such protections would fully cover consumers using all types of prepaid cards or stored value items, including, for example, closed loop prepaid gift cards or closed loop stored-value apps. To the extent that any prepaid items are not ultimately covered, these consumers still may only receive the contractual protections, if any, provided in their gift card or app contracts. Therefore, it is important for consumers to get information about their potential liability. WHAT'S THE DEAL? A FTC STUDY ON MOBILE SHOPPING APPS, *supra* note 4, at n. 34.

## B. Concerns About Unfair Billing Practices on Mobile Carrier Bills<sup>27</sup>

“Mobile carrier billing” – the ability to charge a good or service directly to a mobile phone account – is a payment method that offers many potential benefits for consumers who want to use their mobile phones to pay for goods and services.<sup>28</sup> In particular, carrier billing may be useful for consumers who do not have credit cards, or do not want to use them, especially for small transactions. In this way, carrier billing may be especially beneficial for unbanked and underbanked consumers.<sup>29</sup>

As carrier billing has developed, however, fraud has become a problem for consumers. In particular, mobile cramming – the unlawful practice of placing unauthorized third-party charges on mobile phone accounts – is a significant concern.<sup>30</sup> Mobile cramming occurs when consumers are signed up and billed for third-party services, such as ringtones and recurring text messages containing trivia or horoscopes, without their knowledge or consent. In six recent enforcement actions, the Commission has alleged that such practices have cost consumers millions of dollars,<sup>31</sup> and in three of these actions alone, defendants have agreed to orders imposing judgments totaling more than \$160 million.<sup>32</sup>

In addition to the agency’s enforcement actions, the Commission has engaged in policy and outreach initiatives to address mobile cramming issues. Specifically, the Commission convened a roundtable of interested stakeholders to discuss strategies to eliminate mobile

---

<sup>27</sup> The RFI seeks comment on the use of prepaid phones and carrier billing by underserved communities. RFI, *supra* note 1, at 33733.

<sup>28</sup> MOBILE CRAMMING: AN FTC STAFF REPORT, *supra* note 7, at i.

<sup>29</sup> *Id.*

<sup>30</sup> *Id.*

<sup>31</sup> *FTC v. T-Mobile USA, Inc.*, No. 2:14-cv-00967-JLR (W.D. Wash. July 1, 2014), available at <http://www.ftc.gov/enforcement/cases-proceedings/132-3231/t-mobile-usa-inc>; *FTC v. Wise Media, LLC*, No. 1:13-cv-1234-WSD (N.D. Ga. Apr. 17, 2013), available at <http://www.ftc.gov/enforcement/cases-proceedings/122-3182/wise-media-llc-et-al>; *FTC v. Jesta Digital, LLC*, No. 1:13-cv-01272-JDB (D.D.C. Aug. 21, 2013), available at <http://www.ftc.gov/enforcement/cases-proceedings/112-3187/jesta-digital-llc-also-dba-jamster>; *FTC v. Tatto, Inc.*, No. 2:13-cv-08912-DSF-FFM (C.D. Cal. Dec. 16, 2013), available at <http://www.ftc.gov/enforcement/cases-proceedings/112-3181/tatto-inc-also-dba-winbigbidlow-tatto-media-et-al>; *FTC v. Acquinity Interactive, LLC*, No. 0:14-cv-60166-RNS (S.D. Fla. July 29, 2013) (amended complaint filed June 16, 2014), available at <http://www.ftc.gov/enforcement/cases-proceedings/122-3161/acquinity-interactive-llc-et-al>; *FTC v. MDK Media, Inc.*, No. 2:14-cv-05099-JFW-SH (C.D. Cal. July 29, 2014), available at <http://www.ftc.gov/enforcement/cases-proceedings/132-3225-132-3224-132-3223/mdk-media-inc>.

<sup>32</sup> See Press Release, Fed. Trade Comm’n, Operator of Mobile Cramming Scheme Will Pay More Than \$1.2 Million in FTC Settlement (Aug. 5, 2014), available at <http://www.ftc.gov/news-events/press-releases/2014/08/operator-mobile-cramming-scheme-will-pay-more-12-million-ftc>; Press Release, Fed. Trade Comm’n, Operators of Massive Mobile Cramming Scheme Will Surrender More Than \$10M in Assets in FTC Settlement (June 13, 2014), available at <http://www.ftc.gov/news-events/press-releases/2014/06/operators-massive-mobile-cramming-scheme-will-surrender-more-10m>; Press Release, Fed. Trade Comm’n, Mobile Crammers Settle FTC Charges of Unauthorized Billing (Nov. 21, 2013), available at <http://www.ftc.gov/news-events/press-releases/2013/11/mobile-crammers-settle-ftc-charges-unauthorized-billing>; Press Release, Fed. Trade Comm’n, Jesta Digital Settles FTC Complaint it Crammed Charges on Consumers’ Mobile Bills Through ‘Scareware’ and Misuse of Novel Billing Method (Aug. 21, 2013), available at <http://www.ftc.gov/news-events/press-releases/2013/08/jesta-digital-settles-ftc-complaint-it-crammed-charges-consumers>.

cramming,<sup>33</sup> and FTC staff recently issued a report that recommends certain best practices for industry participants to protect consumers against mobile cramming.<sup>34</sup>

The report recommends that: (1) mobile carriers give consumers the option to block all third-party charges on their phone accounts; (2) market participants take appropriate action so that advertisements for products or services charged to a mobile bill are not deceptive; (3) market participants obtain consumers' express, informed consent to charges before they are billed to a mobile account, and maintain reliable records of such authorizations; (4) mobile carriers disclose all charges for third-party services clearly and conspicuously to consumers in a non-deceptive manner; and (5) carriers implement an effective dispute resolution process.<sup>35</sup>

Finally, the Commission has issued education materials on this topic encouraging consumers to check their mobile carrier bills carefully.<sup>36</sup>

### C. Concerns About the Privacy of Consumers' Personal and Financial Data<sup>37</sup>

Another concern in the mobile environment is consumer privacy. The FTC has been the primary federal agency involved in privacy enforcement and policy since the 1970s, when it began enforcing one of the first federal privacy laws – the Fair Credit Reporting Act (FCRA). Since then, rapid changes in technology have raised many new privacy challenges, and the FTC has expanded its efforts to address them. The Commission uses a variety of tools to protect consumers' personal and financial information, including workshops, reports, surveys, testimony, law enforcement, and consumer and business education.

During the past few years, a key focus at the Commission has been to address the privacy concerns raised by the rapid expansion of mobile technologies and connected devices. As part of this effort, the FTC held three roundtables in 2009-2010,<sup>38</sup> followed by a preliminary and final report setting forth a framework for addressing privacy in today's marketplace.<sup>39</sup> The report urges companies to: (1) adopt privacy by design by building in privacy at every stage of product

---

<sup>33</sup> *Mobile Cramming: An FTC Roundtable*, *supra* note 5.

<sup>34</sup> MOBILE CRAMMING: AN FTC STAFF REPORT, *supra* note 6.

<sup>35</sup> *Id.* at i-ii.

<sup>36</sup> See, e.g., *Mystery Phone Charges*, Fed. Trade Comm'n (Dec. 2013), available at <http://www.consumer.ftc.gov/articles/0183-mystery-phone-charges>; *Hiding in Plain Sight?*, Fed. Trade Comm'n (July 1, 2014), available at <http://www.consumer.ftc.gov/blog/hiding-plain-sight>; *Top Billing: 5 Best Practices for the Mobile Industry*, Fed. Trade Comm'n (July 28, 2014), available at <http://business.ftc.gov/blog/2014/07/top-billing-5-best-practices-mobile-industry>.

<sup>37</sup> The RFI acknowledges that a significant percent of low-income consumers use their mobile devices as their primary means to access the internet and go online. Accordingly, the RFI seeks comment as to whether the privacy and security considerations differ when consumers access services online via a computer or via a phone or mobile application. RFI, *supra* note 1, at 33733-34.

<sup>38</sup> *Exploring Privacy – A Roundtable Series*, FED. TRADE COMM'N (Dec. 7, 2009, Jan. 28, 2010, Mar. 17, 2010) (Workshops), available at <http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml>.

<sup>39</sup> FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, at 1 (2012) available at <http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf> (Commissioner Ohlhausen and Commissioner Wright were not members of the Commission at that time and thus did not participate in the vote on the report).

development; (2) offer more streamlined choices to consumers by providing choices at key decision-making moments and eliminating choices about obvious or expected data uses; and (3) make information collection and use practices more transparent.<sup>40</sup>

The Commission's work in this area has shown that mobile technologies raise unique privacy concerns due to the high number of companies involved in the mobile payments ecosystem and the large volume of data being collected. In addition to the banks, merchants, and payment card networks present in traditional payment systems, mobile payments often involve new actors such as operating system manufacturers, hardware manufacturers, mobile phone carriers, application developers, and coupon and loyalty program administrators.<sup>41</sup> When a consumer makes a mobile payment, any or all of these parties may have access to more detailed data about a consumer and the consumer's purchasing habits as compared to data collected when making a traditional payment.<sup>42</sup>

In its report, *Mobile Privacy Disclosures: Building Trust Through Transparency*,<sup>43</sup> FTC staff made a number of recommendations to improve transparency in the mobile environment, including recommendations that app developers provide "just-in-time" disclosures and obtain affirmative express consent from consumers prior to collecting sensitive information about consumers or sharing such sensitive data with third parties.<sup>44</sup>

FTC staff built on these recommendations in its recently-issued Mobile Shopping Apps Report. In addition to examining disclosures about the apps' liability and dispute procedures, discussed above, that report reviewed the privacy disclosures of mobile shopping apps, which included 30 in-store payment apps.<sup>45</sup> While most of the apps reviewed had privacy policies, staff found that those policies often used vague terms, reserving broad rights to collect, use, and share consumer data without explaining how the apps actually handled the information.<sup>46</sup> Staff recommended that companies clearly describe how they collect, use and share consumer data so that consumers can make informed choices about the apps they use.<sup>47</sup> Staff further recommended that consumers seek information before they download apps about how their data will be collected, used, and shared.<sup>48</sup> If consumers cannot find this information, or are uncomfortable with what they find, they should look for a different app or consider taking steps to minimize their exposure by limiting the personal and financial data they provide.<sup>49</sup>

---

<sup>40</sup> *Id.* at vii-viii.

<sup>41</sup> *Paper, Plastic...or Mobile Workshop*, *supra* note 5 (J. Anderson, Mastercard, session 1 transcript, at 37).

<sup>42</sup> *Id.* (H. Geiger, Center for Democracy & Technology, session 4 transcript, at 4).

<sup>43</sup> FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY (2013), available at <http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf> (Commissioner Wright did not participate).

<sup>44</sup> *Id.* at 22-23.

<sup>45</sup> WHAT'S THE DEAL? A FTC STUDY ON MOBILE SHOPPING APPS, *supra* note 4, at 15.

<sup>46</sup> *Id.* at 2.

<sup>47</sup> *Id.*

<sup>48</sup> *Id.*

<sup>49</sup> *Id.*



Law enforcement and education also have been critical to the FTC's efforts in this area. In the past several years, the FTC has brought a number of enforcement actions alleging deceptive and unfair conduct by mobile app developers in the collection or sharing of consumers' data,<sup>50</sup> including children's data.<sup>51</sup> Further, the FTC's website features many materials educating consumers about potential concerns related to mobile privacy.<sup>52</sup>

#### **D. Concerns About the Security of Consumers' Personal and Financial Data**

Mobile technologies also may raise security concerns. Indeed, consumers cite security concerns as one key reason for reluctance to use mobile devices for financial transactions.<sup>53</sup> As discussed at the FTC's workshop and report on mobile payments, technological advances in the mobile payment marketplace actually offer the potential for *increased* data security for financial information.<sup>54</sup> For example, mobile payment technology allows for encryption throughout the entire payment chain, often referred to as "end-to-end encryption."<sup>55</sup> However, as shown by FTC enforcement in this area, some industry players are not taking full advantage of the enhanced security features of mobile technologies.

The FTC is addressing mobile security through enforcement, policy initiatives, and consumer and business education. For example, in two recent cases against Fandango and Credit Karma, the FTC alleged that, despite their security promises, the companies failed to take reasonable steps to secure their mobile apps, leaving consumers' sensitive personal information at risk.<sup>56</sup> The complaints charged that Fandango and Credit Karma disabled a critical default process, known as SSL certificate validation, which would have verified that the apps' communications were secure. The FTC staff also issued educational material discussing how such apps may fail to provide security for their customers' data.<sup>57</sup>

---

<sup>50</sup> See e.g. *Snapchat, Inc.*, FTC File No. 132-3078 (F.T.C. May 8, 2014), available at <http://www.ftc.gov/enforcement/cases-proceedings/132-3078/snapchat-inc-matter>; *Goldenshores Technologies*, FTC File No. 132-3087 (Dec. 5, 2013), available at <http://www.ftc.gov/enforcement/cases-proceedings/132-3087/goldenshores-technologies-llc-erik-m-geidl-matter>; *FTC v. Frostwire, LLC*, No. 1:11-cv-23643 (S.D. Fla. Oct. 11, 2011), available at <http://www.ftc.gov/enforcement/cases-proceedings/112-3041/frostwire-llc-angel-leon>.

<sup>51</sup> See *US v. Path, Inc.*, No. 3:13-cv-00448 (N.D. Cal. Feb. 1, 2013), available at <http://www.ftc.gov/enforcement/cases-proceedings/122-3158/path-inc> (alleging violations of the Children's Online Privacy Protection Act); and *US v. W3 Innovations, LLC*, No. 5:11-cv-03958 (N.D. Cal. Aug. 15, 2011), available at <http://www.ftc.gov/enforcement/cases-proceedings/102-3251/w3-innovations-llc-dba-broken-thumb-apps-justin-maples-us> (alleging violations of the Children's Online Privacy Protection Act).

<sup>52</sup> *Consumer Information- Privacy & Identity*, Fed. Trade Comm'n, available at <http://www.consumer.ftc.gov/topics/privacy-identity>.

<sup>53</sup> See, e.g., BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM, CONSUMERS AND MOBILE FINANCIAL SERVICES, at 2 (2014) ("Among consumers who do not use mobile financial services, the principal reasons cited for not using the services are perceptions of limited usefulness and benefits, and concerns about security."), available at <http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201403.pdf>.

<sup>54</sup> PAPER, PLASTIC...OR MOBILE, *supra* note 6 at 11.

<sup>55</sup> *Id.* at 12.

<sup>56</sup> *Credit Karma, Inc.*, *supra* note 7; *Fandango, LLC*, *supra* note 7.

<sup>57</sup> *How Secure is that Mobile App?*, Fed. Trade Comm'n (Mar. 28, 2014), available at <http://www.consumer.ftc.gov/blog/how-secure-mobile-app>.

In addition, last year, mobile device manufacturer HTC agreed to settle charges that the company failed to take reasonable steps to secure the software it developed for its smartphones and tablet computers, introducing security flaws that placed at risk the sensitive information of millions of consumers.<sup>58</sup>

The Commission has also hosted a workshop on mobile security threats<sup>59</sup> and is currently reviewing additional information in response to detailed questions posed about mobile security.<sup>60</sup> Moreover, FTC staff has released guidance directed to businesses operating in the mobile arena to help educate them on best practices to handle sensitive information. FTC staff published a guide, *Marketing Your Mobile App: Get It Right from the Start*, to help mobile app developers observe truth-in-advertising and basic privacy and security principles when marketing new apps.<sup>61</sup> Likewise, because mobile apps and devices often rely on sensitive consumer data, FTC staff has developed, *Mobile App Developers: Start with Security*, a guidance piece that provides tips to help mobile app developers approach mobile apps security. Among other things, the piece suggests that developers take stock in the data their apps collect and store, generate password credentials securely, and use encryption to transmit important data.<sup>62</sup>

#### **E. Concerns About the Potential Use of Consumer Information by Data Brokers and Others<sup>63</sup>**

The mobile marketplace also has relevance for data brokers and companies that buy and sell consumer data largely without directly interacting with consumers. The Commission has focused on the practices of data brokers since the enactment of the FCRA, which imposes obligations on consumer reporting agencies that provide data for credit, employment, insurance and other defined eligibility determinations.<sup>64</sup> As mobile services have grown in capabilities and popularity, so has the potential for new companies operating in this environment to violate traditional laws governing collection and use of consumer data, such as the FCRA. Indeed, the FTC has taken action against a number of mobile apps under the FCRA.

---

<sup>58</sup> *HTC America, Inc.*, FTC File No. 1223049 (F.T.C. Feb. 22, 2013), available at <http://www.ftc.gov/enforcement/cases-proceedings/122-3049/htc-america-inc-matter>.

<sup>59</sup> *Mobile Security: Potential Threats and Solutions*, FED. TRADE COMM'N (June 2013) (Workshop), available at <http://www.ftc.gov/news-events/events-calendar/2013/06/mobile-security-potential-threats-solutions>.

<sup>60</sup> Press Release, Fed. Trade Comm'n, FTC Invites Further Public Comment on Mobile Security (April 17, 2014), available at <http://www.ftc.gov/news-events/press-releases/2014/04/ftc-invites-further-public-comment-mobile-security>.

<sup>61</sup> *Marketing Your Mobile App: Get It Right from the Start*, Fed. Trade Comm'n, (April 2013), available at <http://www.business.ftc.gov/documents/bus81-marketing-your-mobile-app>.

<sup>62</sup> *Mobile App Developers: Start with Security*, Fed. Trade Comm'n (Feb. 2013), available at <http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security>.

<sup>63</sup> The RFI seeks comment on the use of consumer financial data and the role of third parties in mobile financial services. See RFI, *supra* note 1, at 33732-34.

<sup>64</sup> FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY, at 4 (2014), available at <http://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>.

In 2012, the Commission issued warning letters to marketers of six mobile applications that provided background screening apps that they may be violating the FCRA.<sup>65</sup> The FTC warned the apps' marketers that, if they have reason to believe the background reports they provided were being used for employment screening, housing, credit, or other similar purposes, they must comply with the FCRA.<sup>66</sup> Further, the FTC settled charges last year with one enterprise that marketed its mobile apps as employment screening tools, alleging that the company operated as a consumer reporting agency without taking consumer protection measures required by the FCRA.<sup>67</sup>

In addition to raising issues under traditional data privacy laws like the FCRA, mobile services raise other data broker-related concerns. As noted above, the mobile ecosystem is unique in that there are many different entities and types of entities with the ability to access large volumes of potentially sensitive data. When data is sold to these entities, often outside the protections of specific privacy laws, questions arise regarding how this data may be used to either benefit or disadvantage low-income and underserved communities.

These concerns were discussed in a detailed study of the data broker industry that the FTC recently concluded. In May, the FTC issued *Data Brokers: A Call for Transparency and Accountability*, a report detailing staff's in-depth study of the practices of nine data brokers representing a cross-section of the industry.<sup>68</sup> The report notes that data brokers combine and analyze information about consumers to make inferences that can help companies prevent fraud, improve product offerings, and deliver tailored advertisements to consumers.<sup>69</sup> Further, data brokers make inferences about consumers and create data segments that group consumers based on the information they collect.<sup>70</sup> The inferences made about consumers can involve potentially sensitive information.<sup>71</sup> Indeed, the report found potentially sensitive categories to include those that primarily focus on ethnicity and income levels, such as "Urban Scramble" and "Mobile Mixer," both of which include a high concentration of Latinos and African Americans with low incomes.<sup>72</sup>

On September 15, 2014, the FTC will host a public workshop, *Big Data: A Tool for Inclusion or Exclusion?*, to examine the use of big data and its impact on consumers, including low-income consumers and underserved communities.<sup>73</sup> Among the issues, the workshop will

---

<sup>65</sup> Press Release, Fed. Trade Comm'n, FTC Warns Marketers That Mobile Apps May Violate Fair Credit Reporting (Feb. 7, 2012), available at <http://www.ftc.gov/news-events/press-releases/2012/02/ftc-warns-marketers-mobile-apps-may-violate-fair-credit-reporting>.

<sup>66</sup> *Id.*

<sup>67</sup> *Filiquarian LLC, et. al*, FTC File No. 1123195 (F.T.C. May 1, 2013), available at <http://www.ftc.gov/enforcement/cases-proceedings/112-3195/filiquarian-publishing-llc-choice-level-llc-joshua-linsk>.

<sup>68</sup> See A CALL FOR TRANSPARENCY AND ACCOUNTABILITY, *supra* note 64, at 48.

<sup>69</sup> *Id.* at iv-v.

<sup>70</sup> See *id.* at 19-21.

<sup>71</sup> *Id.* at 20.

<sup>72</sup> *Id.* Some other data broker segments focus on minority communities, ethnicity, health, income level, and education level.

<sup>73</sup> *Big Data: A Tool for Inclusion or Exclusion?*, FED. TRADE COMM'N (Sept. 2014) (Workshop), available at <http://www.ftc.gov/news-events/events-calendar/2014/09/big-data-tool-inclusion-or-exclusion>.

explore the potential uses of big data as well as the potential benefits and harms for particular populations of consumers.<sup>74</sup>

#### **IV. CONCLUSION**

FTC staff will continue to protect consumers in the mobile environment to ensure that this medium continues to grow and realize its full potential to benefit all consumers, including the economically vulnerable. Staff also supports the CFPB's effort to consider these issues, and looks forward to a continued partnership in our shared goal to protect American consumers. If any other information would be useful regarding these matters, please contact Jessica Rich, Director, Bureau of Consumer Protection at 202-326-2148 or Patricia Poss, Attorney, Bureau of Consumer Protection at 202-326-2413.

---

<sup>74</sup> *Id.*