The FTC releases staff report on mobile shopping apps

The US Federal Trade Commission ('FTC') has turned its attention to mobile shopping apps, releasing this month a staff report based on a review of the most installed mobile shopping apps across multiple categories. The FTC's focus was not only on how secure a user's personal and payment data is when using these apps, but also on issues such financial liability. Michelle Cohen, Member of Ifrah Law and *E-Commerce Law & Policy* editorial board member, discusses the FTC's study and its findings.

In August, the Federal Trade Commission ('FTC') released a staff report concerning mobile shopping applications ('apps'). FTC staff reviewed some of the most popular apps consumers utilise to comparison shop, collect and redeem deals and discounts, and pay in-store with their mobile devices. In 2012, the FTC conducted a workshop on mobile payments and issued a report that raised concerns about consumer financial liability and the privacy and security of consumers' data in the mobile payment context. This new report[1] follows up on that workshop with a particular emphasis on shopping apps offering price comparison, special deals, and mobile payments.

Popularity of mobile shopping apps and FTC interest in consumer protection and data security

FTC staff recognise that new mobile shopping apps offer consumers many benefits. Shoppers can empower themselves in the retail environment by comparison shopping via their smartphones in real-time. According to a 2014 Report by the Board of Governors of the Federal Reserve System, 44% of smartphone owners report using their mobile phones to comparison shop while in retail stores, and 68% of those consumers changed where they made a purchase as a result[2]. Consumers can also get instant coupons and deals to present at the checkout. With a wave of a phone at the checkout counter, consumers can then make purchases easily.

While shopping apps have surged in popularity, the FTC staff are concerned about consumer protection and data security and privacy issues associated with these apps. The FTC sought to study what types of disclosures and controls are in place in the event of unauthorised transactions, billing errors, or other payment-related disputes. The agency also sought to learn about the disclosures apps provide to consumers concerning data privacy and security.

Methodology of the study

FTC staff conducted an independent review of the most popular new shopping apps, with a particular focus on apps that: (1) allow consumers to compare prices across retailers; (2) collect and redeem deals; and (3) pay for purchases while shopping in brick-and-mortar stores. Staff chose the apps to study based upon the app promotion pages on Google Play and the iTunes App stores, focusing on the 25 most installed apps for each of these three categories.

Next, staff focused on information available to consumers regarding how the apps handle payment disputes and consumer data prior to the download of each app. This review included analysing licence agreements, privacy policies, terms documents, or other developer-provided disclosures. The staff focused particular attention on what the disclosures stated concerning fraudulent or unauthorised transactions, billing errors, and other payment-related disputes.

Interestingly, the report noted (in a footnote) a potential huge shortcoming of the study. That is, there could be disclosures that the FTC staff did not see. This is because, while the FTC staff claim to have carefully analysed the pre-download disclosures and to have opened each app, staff did not actually sign up for any accounts. Thus, '[i]t is possible that the apps provide their users with additional disclosures and information as the user interacts with the service.'[3]

FTC staff find apps lack important information

FTC staff concluded that many of the apps they reviewed failed to provide consumers with important pre-download information. In particular, the report noted that only a few of the in-store purchase apps gave consumers information describing how the app handled payment-related disputes and consumers' liability for charges (including unauthorised charges).

Staff also found that it was difficult for consumers to distinguish between 'pass through' apps (offering payments through credit and debit cards where federal law provided a $50 liability limit for unauthorised charges) and stored value apps - which require users to move money from an external funding source into an account from which the user's charges could be deducted (and where the same protections generally do not apply).

FTC staff determined that 14 out of 30 in-store purchase apps did not disclose whether they had any dispute resolution or liability limit policies prior to download. And, out of sixteen apps that provided pre-download information about dispute resolution procedures or

liability limits, only nine of those apps provided written protections for users. Some apps disclaimed all liability for losses.

FTC staff focused particular attention on data privacy and security, because more than other technologies, mobile devices are personal to a user, always on, and frequently with the user. These features enable an app to collect a huge amount of information, such as location, interests, and affiliations, which could be shared broadly with third parties. Staff noted, 'while almost all of the apps stated that they share personal data, 29 percent of price comparison apps, 17 percent of deal apps, and 33 percent of in-store purchase apps reserved the right to share users' personal data without restriction.'

Staff concluded that while privacy disclosures are improving, they tend to be overly broad and confusing. In addition, staff have concerns that app developers may not be considering whether they even have a business need for all the information they are collecting. As to data security, staff noted it did not test the services to verify the security promises made. However, FTC staff reminded companies that it has taken enforcement actions against mobile apps it believed to have failed to secure personal data (such as Snapchat and Credit Karma, stating: 'Staff encourages vendors of shopping apps, and indeed vendors of all apps that collect consumer data, to secure the data they collect. Further those apps must honor any representations about security that they make to consumers.'

FTC staff recommend better disclosures and data security practices, and consumer responsibility

The report urges companies to disclose to consumers their rights and liability limits for unauthorised, fraudulent, or erroneous transactions. Staff cautioned that consumers should understand what their liability is for purchases and unauthorised transactions before they make purchases. Organisations offering these shopping apps should also explain to consumers what protections they have based on their methods of payment, and what options are available for resolving payment and billing disputes. Companies should provide clear, detailed explanations for how they collect, use and share consumer data. And, apps must put promises into practice by abiding by data security representations.

Importantly, the FTC staff report does not place the entire burden on the companies offering the mobile apps. Rather, FTC staff urge consumers to be proactive when using these apps

Importantly, the FTC staff report does not place the entire burden on the companies offering the mobile apps. Rather, FTC staff urge consumers to be proactive when using these apps. The staff report recommends that consumers look for and consider the dispute resolution and liability limits of the apps they download. Consumers should also analyse what payment method to use when purchasing via these apps. If consumers cannot find sufficient information, they should consider an alternative app, or make only small purchases.

While a great 'deal' could be available with a click on a smartphone, the FTC staff urges consumers to review available information on how their personal and financial data may be collected, used and shared while they get that deal. If consumers are not satisfied with the information provided regarding data privacy and security, then staff recommend that they choose a different app, or limit the financial and personal financial data they provide (though that last piece of advice may not be practical considering most shopping apps require a certain level of personal and financial information simply to complete a transaction. In this author's view, the key would be how the company secures the information and if the company asks for more information than is typical in a retail transaction).

Deal or no deal? The FTC will be watching new shopping apps

The FTC staff report makes clear that the staff have concerns about mobile payments and will continue to focus on consumer protections - both from financial liability perspectives and concerning the security of the data collected, used and shared through the new apps. The agency has taken several enforcement actions against companies for failing to secure personal and payment information and it does not appear to be slowing down. While the FTC recognises the benefits of these new shopping and payment technologies, it is also keenly aware of the enormous amount of data obtained by companies when consumers use these services. Thus, companies should anticipate that the FTC will continue to monitor shopping and deal apps with particular attention on disclosures and data practices.

Michelle W. Cohen, CIPP-US Member
Ifrah Law PLLC, Washington DC
michelle@ifrahlaw.com

1. The August report is available at http://www.ftc.gov/system/files/documents/reports/whats-deal-federal-trade-commission-study-mobile-shopping-apps-august-2014/140801mobileshoppingapps.pdf
2. See Board of Governors of the Federal Reserve System Report, Consumers and Mobile Financial Services 2014, at 2 (2014).
3. 'What's the Deal? An FTC Study on Mobile Shopping Apps,' August 2014, Federal Trade Commission Staff Report, at n. 15.