# Privacy and Information Security Alert:

## Federal Trade Commission Recommendations for Companies Providing Mobile Shopping Applications

AUGUST 11, 2014

FENWICK & WEST LLP

On August 1, 2014, the Federal Trade Commission (FTC) released a report entitled *What's the Deal? An FTC Study on Mobile Shopping Apps* (the *FTC Report*). The *FTC Report* is based on a study the FTC conducted (the FTC Study) to better understand the consumer protection implications of mobile consumer shopping applications that allow consumers to 1) compare prices across retailers, 2) collect and redeem deals, or 3) pay for in-store purchases.[1] Specifically, the FTC Study examined disclosures available to consumers prior to downloading the software onto their mobile devices, including descriptions of how these apps enable consumers to make purchases; how they deal with fraudulent or unauthorized transactions, billing errors or other payment-related disputes; and how the apps handle consumers' personal and purchase data. From the FTC Study, the FTC concluded that mobile shopping apps often do not give shoppers up-front information about their rights and liabilities for erroneous or unauthorized payments. And even though many apps provide links to privacy policies and make strong security promises, the FTC found those policies often use vague language, reserving broad rights to collect, use and share consumer data.

The *FTC Report* identifies three general recommendations to companies that provide mobile shopping apps:

1. Companies should disclose consumers' rights and liability limits for unauthorized, fraudulent or erroneous transactions;
2. Companies should clearly describe how they collect, use and share consumer data; and
3. Companies should ensure that their strong data security *promises* translate into strong data security *practices*.

**Companies should disclose consumers' rights and liability limits for unauthorized, fraudulent or erroneous transactions.**

The FTC Study found that prior to download, apps often fail to provide any information to consumers about their potential liability in the event a payment dispute arises. Consumers are often not aware that while federal laws limit consumers' liability for unauthorized payments in the context of credit or debit card transactions, including where a consumer makes a purchase through an app by placing a charge directly on a credit or debit card ("pass through" apps), statutory protections generally do not apply to purchases involving prepaid, gift or stored-value accounts. The *FTC Report* notes that "stored-value" apps, which usually involve the transfer of consumer funds into an account maintained by the app provider and from which money is later deducted during consumer purchases, may lack the legal protections that are associated with credit or debit card transactions. The FTC Study further found that based on pre-download information, it was often difficult to distinguish whether an app was a pass-through or stored-value app, and thus whether a consumer could rely on statutory protections. Stressing the importance of making information available to consumers pre-download, the *FTC Report* recommends that app developers provide consumers with clear, pre-download disclosures about potential liability for unauthorized transactions, protections available based on method of payment, and dispute resolution mechanisms available. These disclosures should be available to consumers before they begin using the app's services.

**Companies should clearly describe how they collect, use and share consumer data.**

The FTC Study also examined privacy policies associated with the apps to identify shortfalls in disclosures about how the apps collect and share potentially sensitive user information, such as location, interests and affiliations. The FTC Study found that while most apps link to privacy policies and

1 The FTC Study examined 121 apps available on Google Play and the iTunes App Store, but does not specifically identify the apps used.

make strong security promises, the policies often use vague language, reserving broad rights to collect, use and share consumer data. The FTC expressed concern that privacy policies stating that a company may use personal data to "enhance" or "improve" users' shopping experiences make it difficult for consumers to understand how their information is actually being used and the reasonable limits of such use. These practices are of particular concern in light of the FTC's finding that some mobile shopping apps collect highly sensitive personal identifiers, such as Social Security numbers and driver's license numbers. While almost all apps notify consumers of the fact that they share personal data with third parties, many of the apps reserve the right to share consumer data without restriction.

As such, the *FTC Report* recommends that companies clearly describe how their apps collect, use and share consumer data so that consumers may better evaluate and compare apps before downloading them. Referencing the FTC's *March 2012 Privacy Report*, the *FTC Report* further calls for app developers to limit their data collection to the data needed for a requested service or transaction and to make privacy notices clearer, shorter and more standardized to enable better comprehension and comparison.

**Companies should ensure that their strong data security promises translate into strong data security practices.**

Consumer data security has been a focus of FTC enforcement actions in recent years, and in keeping with that focus, the *FTC Report* encourages developers of apps that collect consumer data to provide strong security for that data, especially in light of readily available security features on modern smartphones. The FTC Survey found that many apps promised to implement "technical," "organizational" or "physical" safeguards, such as data encryption, to ensure that consumers' data was secure. Many of the apps stated that they used "industry-standard" or "reasonable" security, and some promised that the service was "more secure than a bank." Although the FTC did not test the accuracy of these claims, it warned that companies must honor the promises they make regarding the security of their apps.

**Consumers should seek information before they download apps.**

In addition to making recommendations to companies providing mobile shopping apps, the *FTC Report* recommends that consumers seek information before they download apps, including looking for dispute resolution procedures and liability limits, considering the payment methods used to fund their purchases, and seeking information about how their data will be collected, used and shared. The *FTC Report* further recommends that if consumers cannot find this information, they should consider downloading an alternative app.

**Conclusion**

While providing guidance, and not legal requirements, the *FTC Report*'s recommendations reflect the FTC's increasing interest in protecting consumers' privacy and information security, and reflect its scrutiny of related company policies. The FTC encourages companies to provide transparent and meaningful pre-download disclosures to consumers regarding their rights and protections, dispute resolution and liability limits, and how their personal data will be used, so that consumers are able to make an informed decision in choosing which apps to download. For mobile shopping app providers, it is important to understand the state and federal laws applicable to mobile apps, including laws governing data privacy and security.

---

*For more information please contact:*

*Jennifer J. Johnson*, 415.875.2391; *jjjohnson@fenwick.com*

*Tyler G. Newby*, 415.875.2495; *tnewby@fenwick.com*

---