FTC staff recommendations for mobile financial services

Consumer protection concerns highlighted in CFPB response

In September, the staff of the Federal Trade Commission's ('FTC') Bureau of Consumer Protection submitted comments to the Consumer Financial Protection Bureau ('CFPB') in response to the CFPB's 'Request for Information' ('RFI') issued in June 2014. The RFI sought comment on the use of mobile financial services by consumers and 'economically vulnerable populations' to access products and services, manage finances, and achieve their financial goals. The FTC staff asserts that mobile technologies can benefit consumers in many ways, most notably by making financial transactions convenient. With ease, consumers can check their bank balances and make purchases. For 'unbanked' consumers, having charges placed on their mobile phone bills can be especially helpful.

Consumer protection concerns

However, mobile financial services present consumer protection concerns, according to FTC staff. The key concerns are:

- potential liability for unauthorised charges using prepaid or stored value products;
- unfair billing practices on mobile carrier bills;
- privacy and security of consumers' personal and financial data, and
- potential use of consumers' information by data brokers and others.

Unauthorised charges using prepaid/stored value products

As the FTC has noted in its reports, transactions made using prepaid or stored value accounts generally do not have the same statutory and/or contractual liability limits applicable to other forms of payment such as credit cards. When consumers use a prepaid/gift card or a stored value account within the app to make an m-payment transaction, they are at the mercy of whatever protections are voluntarily provided by the prepaid card or mobile app provider. Here, the FTC staff reiterates its concerns regarding these modes of payment, noting that 'unbanked' consumers and other vulnerable groups, such as students, tend to use these forms of payment for mobile transactions. Thus, it is critical for these groups to receive disclosures regarding the scope of their potential liability.

Billing practices on mobile telephone bills

Some consumers charge a good or service directly to a mobile phone account. Mobile carrier billing may be beneficial for consumers who do not have or want to use credit cards. Unbanked consumers may find that mobile carrier billing fits their needs by allowing purchases without incurring interest or not being able to make the purchases. However, the FTC and the Federal Communications Commission ('FCC'), among other agencies, have found a persistent problem known as cramming - unauthorised, usually third party charges on consumers' bills. Recently, the FTC and the FCC announced a $105 million dollar settlement with AT&T Mobility for unauthorised charges on consumers' mobile phone bills[1]. The FTC staff's comments reiterate their concerns with cramming. Staff also continue to recommend that:

- mobile carriers offer consumers the option to block all third-party charges;
- market participants obtain consumers' express, informed consent to charges before they are billed;
- mobile carriers disclose all charges for third-party services clearly and conspicuously;
- carriers implement effective dispute resolution processes; and
- consumers check their mobile bills carefully.

Personal and financial data privacy and security

Mobile technologies raise unique privacy concerns because many different companies are involved in the m-payments system and large amounts of sensitive data are collected. Involved parties may have access to more data than is typically present in a traditional payment scenario. The FTC staff's suggestions include having app developers provide 'just-in-time' disclosures and obtain affirmative express consent prior to collecting sensitive information about consumers or sharing that information. Further, while 'end-to-end' encryption is available throughout the entire m-payment chain, not all industry participants are utilising this. The FTC has taken enforcement action against Fandago and Credit Karma for failing to ensure their apps were secure[2].

Data brokers' and other use of consumer information

Finally, the FTC staff note that data brokers can buy and sell sensitive consumer information without interacting directly with consumers. The FTC has authority under the Fair Credit Reporting Act and the FTC Act to take actions against companies utilising consumer information improperly.

What's next?

FTC staff's comments make clear that the agency will continue to support the CFPB in protecting consumers as they navigate mobile financial transactions. For companies involved in the m-payment ecosystem, this means that disclosures should be clear, back-up for charges should be maintained, and privacy and data practices should be conspicuous and secure.

Michelle W. Cohen Member
Ifrah PLLC, Washington DC
michelle@ifrahlaw.com

1. http://www.ftc.gov/news-events/press-releases/2014/10/att-pay-80-million-ftc-consumer-refunds-mobile-cramming-case
2. http://www.ftc.gov/news-events/press-releases/2014/03/fandango-credit-karma-settle-ftc-charges-they-deceived-consumers