

To the Point!

legal, operations, and strategy briefs for financial institutions February 22, 2013



Mobile Privacy Disclosures: Building Trust Through Transparency Federal Trade Commission Staff Report

The Federal Trade Commission (“FTC”) released a staff report titled Mobile Privacy Disclosures: Building Trust Through Transparency (the “Report”) advising industry participants on best practices to inform consumers of how their personal information is collected, used and shared. The Report notes the “unique privacy challenge” posed by mobile devices including geolocation capabilities, limited screen space for privacy disclosures and the large number of entities involved in providing the mobile service that may collect and use data from mobile devices. The Report is important for banks that offer mobile banking services as it establishes minimum industry standards which can be used by banking regulators and consumers to compare a bank’s treatment of its customers who use mobile apps provided by the bank to receive bank services.

The Report divides the mobile industry into four (4) categories: mobile platforms; app developers; advertising networks; and app developer trade associations. While not specifically identified by the FTC in its Report, banks that offer mobile banking services fit within the app developer category. Although banks do not offer or sell mobile apps through mobile platforms, they do provide mobile apps to customers that subscribe to their mobile banking services and such mobile apps are susceptible to the same types of information gathering, use and sharing as are mobile apps offered by app developers on mobile platforms addressed by the FTC in the Report.

The Report provides four (4) recommendations for mobile app developers:

- Have a privacy policy and make sure it is easily accessible through the app stores;
- Provide just-in-time disclosures and obtain affirmative express consent before collecting and sharing sensitive information (to the extent the platforms have not already provided such disclosures and obtained such consent);
- Improve coordination and communication with ad networks and other third parties, such as analytics companies, that provide services for apps so the app developers can provide accurate disclosures to consumers. For example, app developers often integrate third-party code to facilitate advertising or analytics within an app with little understanding of what information the third party is collecting and how it is being used. App developers need to better understand the software they are using through improved coordination and communication with ad networks and other third parties.
- Consider participating in self-regulatory programs, trade associations and industry organizations, which can provide guidance on how to make uniform, short-form privacy disclosures.

In the mobile banking context, the first recommendation that an app developer offer a privacy policy through the “app stores” it uses to distribute its mobile apps should be viewed as a recommendation that the bank offer a privacy disclosure at the time the consumer enrolls in the mobile banking services. It is noteworthy that the FTC identified the model privacy notice used by financial institutions to comply with the Gramm Leach Bliley Act (that was developed by the federal financial institution regulatory agencies and the FTC) as an example of how an app developer could create a privacy policy for consumers that is simple to read and understand.

The actions that may be necessary to implement the recommendations on disclosures to consumers on data collection, use and sharing depend upon a careful examination of the bank's mobile app and mobile banking service including identification of the following: what information is collected; how such information is used; is the information shared; is information retained; and what are the consumer's expectations regarding data collection?

Banks all have privacy notices required by the Gramm Leach Bliley Act. Each bank should consider whether that notice is also an accurate and complete statement of the treatment of personal information for its mobile banking customers. Each bank should also consider whether additional disclosures specific to mobile banking would be beneficial for its customers both at the time the customer enrolls in the mobile banking service and later when information is collected, as suggested by the FTC.



Corporate Account Takeover

Corporate account takeover is a form of identity theft affecting business customers. Cyber thieves obtain control of a business account by stealing user passwords, IDs and other security credentials that are then used to initiate fraudulent wire and ACH transactions. It is a risk for all businesses but seems to affect small business customers more frequently. Losses to small businesses have been recently estimated at \$2 billion with more than 10% of small businesses experiencing such losses.

The Conference of State Bank Supervisors ("CSBS") and the Federal Financial Institution Examination Council ("FFIEC") have provided guidance for banks regarding best practices to reduce the risk of electronic theft. Each bank should review these guidelines and consider additional steps it could implement to help prevent this type of theft.

Banks can also mitigate the risk of corporate account takeovers by educating their customers regarding security. Both the CSBS and the FFIEC recommend such educational initiatives. Information can be made available in statement stuffers or other direct mail communications, at branch offices and on websites. The bank can monitor customer clicks on information security links to identify which are effective and for which customers may welcome additional information. In addition to helping prevent these losses such initiatives can establish the bank as a source of expertise to its customers.

Finally, banks should review their contractual agreements with customers to ensure that they offer protection for the bank if the customer experiences a loss due to a corporate account takeover. Banks should consider including the following topics in their agreements: roles and responsibilities for processing transaction requests; dispute resolution processes; minimum security standards; disclaimer and acknowledgment that no security procedures can be foolproof and the customer agrees that the procedures chosen are commercially reasonable for the type, size and frequency of transfers they originate; responsibility for designating authorized users; and transaction limits.

We recommend that each bank review the regulatory guidance to consider what, if any, of the best practices can be implemented; review its customer education program to enhance security awareness; and review and revise its contractual agreements to provide the broadest protection for the bank if a customer experiences a loss.



CFPB Issues Guidance on Mortgage Servicing Transfers

The Consumer Financial Protection Bureau (the "CFPB") continues its focus on mortgage servicing and recently issued Bulletin 2013-1 (the "Bulletin") to mortgage servicers identifying the CFPB's current expectations regarding mortgage servicing transfers. The guidance applies now and will be enforced by CFPB examiners prior to the January 10, 2014, effective date of the Mortgage Servicing Rule. The CFPB guidance is based on consumer complaints and supervisory work related to servicing transfers and identifies specific areas of focus for these examinations.

Areas of Focus for All Servicing Transfers

The CFPB advises servicers that it will focus on the servicer's policies, procedures, systems and controls in servicing transfers to ensure timely, accurate and complete transfer of information that ensures compliance with the mortgage loan and applicable law. The CFPB also emphasizes that transferees should have policies and procedures to identify necessary documents or information not transferred and to obtain such required information. Areas of focus for examinations identified by the CFPB include:

- Transferor servicer's transfer preparation, including steps taken to ensure information transferred is compatible with the transferee's system, adequate information is provided to the transferee to provide service without unnecessary interruption, and how the transferor intends to respond to inquiries from the transferee or consumers.
- Transferee's handling of transferred files, including due diligence to ensure accurate information is conveyed to customers, procedures in place to identify customers in the loss mitigation process, indication that the servicing platform accurately reflect account information, and post-transfer audits to ensure data was properly and accurately transferred.
- Transferors' and transferees' policies and procedures to ensure the transferee receives any loss mitigation status prior to the transfer, the transferor sends and the transferee receives related documentation, and the transferee is properly applying payments.

The Bulletin reminds servicers that current law applies to servicing transfers including the Real Estate Settlement Procedures Act, the Fair Credit Reporting Act and the Fair Debt Collection Practices Act. In addition, the CFPB noted that servicers will be examined for potential UDAAP violations, in particular as they may relate to a failure to honor loan modifications that are in process during the servicing transfer.

Written Plan for Significant Servicing Transfers

The CFPB stated that it will require servicers that engage in significant servicing transfers to prepare and provide written plans to the CFPB on how they will manage associated consumer risks.

New Servicing Rules

The Bulletin also reminds servicers of the new servicing rules issued by the CFPB that will take effect January 10, 2014. The CFPB also stated it plans to work with mortgage servicers directly to support implementation of new rules and to issue plain language summaries of the rules and other materials to help servicers understand supervisory expectations.

Based on guidance provided in the Bulletin, the CFPB appears focused on the specifics of how mortgage servicing transfers are handled at the operational level with emphasis on having policies and procedures in place and adequate employee training. Mortgage servicers should review, develop or modify their policies and procedures for servicing transfers with attention to the areas noted by the CFPB, especially the loan modification process. Furthermore, mortgage servicers engaged in significant servicing transfers shall be prepared to provide their written plans for transfers to the CFPB. Mortgage servicers are encouraged to work with industry groups and raise questions during any interface with the CFPB to address issues and concerns before the formal effective date of the new rules.

Chapman and Cutler LLP

Attorneys at Law • Focused on Finance®

To the Point! is a summary of items of interest and current issues for financial institutions with primary focus on regulatory, consumer, and corporate issues. Chapman and Cutler LLP maintains a dedicated practice group with expertise to counsel on these issues and other enterprise risk management matters facing financial institutions. If you would like to discuss any of the items contained in these briefings or other legal, regulatory, or compliance issues facing your institution, please contact one of the partners in our Bank Regulatory Group:

Marc Franson • 312.845.2988

Scott Fryzel • 312.845.3784

Heather Hansche • 312.845.3714

Doug Hoffman • 312.845.3794

John Martin • 312.845.3474

David Worsley • 312.845.3896

Dianne Rist • 312.845.3404

This document has been prepared by Chapman and Cutler LLP attorneys for informational purposes only. It is general in nature and based on authorities that are subject to change. It is not intended as legal advice. Accordingly, readers should consult with, and seek the advice of, their own counsel with respect to any individual situation that involves the material contained in this document, the application of such material to their specific circumstances, or any questions relating to their own affairs that may be raised by such material.

© Chapman and Cutler LLP, 2013. All Rights Reserved. Attorney advertising material.

Chapman and Cutler LLP | 312.845.3000 | 111 West Monroe Street | Chicago | IL | 60603