



January 28, 2011

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Room 4725
Washington, DC 20230

Re: Commercial Data Privacy and Innovation in the Internet Economy
A Dynamic Policy Framework

Dear Sir or Madam:

Quicken Loans Inc. (Quicken Loans) is pleased to submit its comments on the Department of Commerce's (DOC) Internet Policy Taskforce's "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework." By way of background, Quicken Loans is an independent Detroit, Michigan-based conventional and FHA retail residential mortgage bank. We have been in business since 1985, and have approximately 4,000 employees. We do business in all 50 states and are one of the nation's five largest retail mortgage lenders, one of the five largest FHA mortgage lenders, and the largest online lender. We closed over \$28 billion in retail mortgages in 2010.

The comments included in this document are the result of internal collaboration with In-House Realty, representing a nationwide network of realtors who align clients with the best agents in their area; One Reverse Mortgage LLC, the nation's third largest provider of reverse mortgage home loans; and Fathead LLC, which includes an eCommerce website for the leading brand in sports and entertainment graphics.

Quicken Loans and its family of companies appreciate the efforts of the Department of Commerce and its Internet Policy Taskforce to reevaluate consumer data privacy protections in the current marketplace. As technology grows and evolves, so must consumer protection. We fully support initiatives that protect sensitive consumer information while bolstering business growth and development. We agree with many of the approaches from the Department of Commerce and agree that companies should provide consumers with the comfort that their information will not be improperly handled. Below, we outline our comments and thoughts on the proposals from the



Department of Commerce, as well as noting some issues that should also be addressed by the Department and other agencies involved in protecting consumer privacy.

General Comments

Quicken Loans agrees that the efforts by the Department of Commerce and the Federal Trade Commission (FTC) have the right intentions in mind as to protecting consumers online. However, we do have concerns about the approach from both the DOC and the FTC. We have read and analyzed the FTC's own report on consumer privacy that was released around the same time as the DOC's own report. In the FTC's report, we see many similarities with what the DOC is hoping to achieve in the online privacy arena. However, we find that this strategy could prove problematic. With two separate agencies approaching revisions to current consumer privacy initiatives, we fear that overlapping regulation and confusion surrounding enforcement could occur. We also note that the DOC goes as far to recommend that that FTC take the lead on online privacy enforcement. However, with the passage of the Dodd-Frank Act this past summer, the Bureau of Consumer Financial Protection (CFPB) will also be granted jurisdiction over certain non-bank financial companies. We fear that the CFPB may also attempt to enter the online privacy arena once again muddying the waters and creating further confusion about who has enforcement authority and who will be drafting and creating new rules.

We can all agree that one thing that is not needed is more confusion—for the consumer or for businesses. We believe that multiple governmental agencies working toward varied goals will only lead to further confusion in the industry. Therefore, we recommend a few things in terms of jurisdiction and enforcement. We believe that either one agency should tackle the creation of rules so that overlapping and holey regulation does not occur. We also recommend that only one organization should take the lead on enforcement. However, if it is decided that multiple agencies must tackle consumer privacy, we believe that a firm and clear line must be drawn between what agency will deal with consumer privacy and which will deal with commercial privacy.

Quicken Loans also appreciates the reserved efforts of the Department of Commerce to closely analyze areas of privacy before plunging head-first into regulation. We understand that a final report will be coming later in the year from the DOC that will include comments from the pending



report. While we understand that these are early steps in the rulemaking process, we believe that much more work and research is needed in the area before issuing proposed rules. We feel that many of the definitions, including those included in the Fair Information Practice Principles (FIPPs) portion of the report (discussed below), are broad and generalized. While we understand that these recommendations are purely talking points right now, we believe that definite and resolute guidance must be provided for the regulation to work properly. We have concerns that an overly-broad rule could cut out companies from tracking information for basic marketing purposes or could create problems in completing simple Internet transactions. The utmost care must be paid to definitions so the DOC can achieve their goals of protecting consumers from harmful and malicious practices without overly burdening companies who are in compliance with existing DOC rules.

Fair Information Practice Principles (FIPPs)

One of the Department of Commerce's main policy initiatives is to create Fair Information Practice Principles (FIPPs). The Department of Commerce hopes that these FIPPs would promote increased transparency with simple notices to consumers about their information, clearly articulated purposes of data collection, commitments to limit data uses to fulfill business purposes, and an expanded use of audit systems to bolster accountability. We believe that if done correctly, these FIPPs could provide a useful service for a consumer and for companies. However, we believe that these FIPPs must be developed with extreme care and caution.

Maybe the greatest obstacle for FIPPs will be the efforts from the FTC in this area. As we have noted above, we believe that multiple agencies working on one issue can create problems with overlapping regulation. We fear that this may be one spot where this is likely to occur. The creation of the CFPB also creates further problems in terms of agency cooperation. We believe that either one regulator should deal with personal consumer privacy or that a strong and concise set of principles must be adopted by all agencies for any online privacy practice to work. A true division between protecting commercial data versus consumer privacy could also work, and we hope that this is the division the FTC and the DOC are seeking currently. We believe that the DOC has shown due diligence in trying to deal with data security breaches and other security concerns. The DOC should stay in this arena and allow the FTC to manage personal consumer privacy.



If the DOC does go ahead with their plans for consumer privacy, we believe that in order for FIPPs to work properly, they must be developed in a clear and concrete way so that there is no confusion for companies as to what is allowed and what is not allowed. We believe that companies should be allowed to voluntarily comply with the Fair Information Practice Principles, and that the proposed FIPPs must allow companies to execute basic marketing tracking for internal purposes. Companies that actively acknowledge and follow the proposed FIPPs should be rewarded accordingly for their commitment to Internet security. We also believe that companies that go out of their way to avoid complying with the FIPPs should be tracked closely and punished accordingly if they explicitly reject the voluntary regulation.

Additionally, we believe that the creation of FIPPs and the execution of them must be done correctly. At the present moment, the FIPPs are too vague. Understandably, they are still being developed, but we do have some recommendations for development. We believe that confusion for the consumer must be eased and the ease of access must also be addressed. A consumer has the right to know how their information is being used on a particular site. However, it does not do the consumer any good to make them constantly confirm what information is being collected and for what purpose. We propose that a clear and concise description of information be provided in a footer of a website as opposed to some solution where a consumer has to opt-in to practices either the first time they visit a site or every time they visit a site. We believe that companies have an ethical standard to live up to in this regard and should not be using consumer information in improper ways or without prior consent. Companies doing this should be rewarded with something of a safe harbor. However, companies who make efforts to skirt regulations or find ways around current law should be sought out by the DOC or the FTC for further investigation.

Additionally, we have concerns about the duration in which companies could be required to keep user data. The DOC is recommending that companies only collect absolutely vital information and that they keep this information for only as long as needed to execute a business transaction. However, databases of consumer information kept by companies can benefit a consumer significantly in saved time and convenience. We believe that companies should be allowed to store information on a consumer if the consumer so wishes. We also believe that forcing companies to dump consumer information within a certain timeframe could be disastrous for companies that need to keep



information stored for a given amount of time. Forcing businesses to constantly re-gather information will not only cost time, but will also cost money that will come from the consumer. We believe that a firm rule about the amount of time companies can store information could prove to be problematic despite the DOC's best intentions.

Lastly, the DOC must keep in mind the distinction between what information being collected is needed for marketing purposes and what information is being used for fraudulent and misleading activities. It is imperative for companies in a marketing sense to understand the activity of the people on their site and the things they are engaged in when on a company's site. This underlines the importance of proposing well-defined regulation so that companies are not punished for tracking simple information used for marketing internally. An all-or-nothing approach in this area could be detrimental to companies that use this information to reach out to consumers visiting a site. Therefore, if regulation is to be proposed, it must be clear so that privacy can be fully protected while still allowing for business activity.

Privacy Policy Office (PPO) within the Department of Commerce

One recommendation the Department of Commerce has for protecting consumer privacy is to create a special Privacy Policy Office (PPO) as a center for commercial data privacy policy expertise. Quicken Loans believes that the PPO could provide a key and much-needed resource in the online privacy world. By convening discussions from various stakeholders about the best ways to approach privacy, the PPO could orchestrate meaningful and resolute changes to the way privacy is used and shared online. However, we must again be cautious that all approaches from the PPO be in consultation with other agencies involved in the privacy arena, and that any regulations and conclusions made by the PPO be made with a thorough analysis of the effect of the regulations on business and business activities.

Do Not Track Technology

One solution being discussed by both the Department of Commerce and the Federal Trade Commission is the possibility of a Do Not Track (DNT) system similar to the Do Not Call system in place from the FTC. We understand that the Do Not Call system has been universally applauded for



helping stop unsolicited telemarketing calls. However, Quicken Loans does not believe that an all-in or all-out approach is the best way to handle privacy online. Other solutions are already being considered in the marketplace so that consumers can choose how their information is used without a complicated and multi-tiered DNT system. Already, certain Internet browsers allow users to prevent the download of tracking cookies. This is easily executed by consumers on their computers today. As technology evolves, so do the solutions for how consumers can protect their information, and we believe an all-or-nothing approach is not the most useful way to approach the protection of information from a technology or consumer standpoint.

A meaningful solution being discussed involves a change to the HyperText Transfer Protocol (HTTP) header that would allow consumers to change tracking settings based on different sites, and would allow them to fully opt-out of specific sites without opting out of all sites. A universal DNT list would be cumbersome to execute and even harder to enforce. We believe the current work being done by companies is on the right track to providing consumers the protection they want. However, we would like to make it clear that any monumental changes to the HTTP system must be thoroughly considered as it pertains to the effect on a company. Significant changes will only hamper business operations and could potentially create even further confusion for companies and consumers when it comes to privacy access. The various solutions surrounding DNT must be further studied and investigated before rules are promulgated.

Security Breach Notification (SBN)

Quicken Loans fully supports the efforts by the Department of Commerce to take the lead in security breach notices. We believe that a common form for Security Breach Notification (SBN) would be advantageous to companies and consumers. As the system stands right now, various states have their own laws, regulations, and forms as it pertains to SBNs. This process can be confusing for consumers and companies when a common form is not available to both. If a common form were developed, consumers would have ample opportunity to review the form and compare it with others online before submitting. As it stands now, consumers may receive a specific state's form with little direction or advice on how to complete it. With a common form, consumers will have the resources needed to fully understand the document. Companies will also benefit in that they will be fully-versed



in the universal form and will not have to juggle various forms and rules for different states while trying to alert consumers of sensitive information that may have been compromised.

Global Initiative

Quicken Loans agrees that the United States is in a unique position and should work to lead the world in data security. We believe that the DOC's approach for the United States to lead the world in privacy protection is worthwhile and substantial. We believe that other countries should look to the U.S. as a model for the way privacy is handled. However, we have concerns that principles practiced in other countries may not always mesh with the principles practiced in the United States. The Department of Commerce should take the lead in helping the U.S. protect sensitive consumer data, but should be cautious to align our consumer privacy online with that of other countries due to significant differences in cultural ideas surrounding privacy protection. What may work in Europe may not necessarily work in the United States. We believe that further investigation must be done before syncing our Internet privacy regulations with those of other countries.

We thank you for this opportunity in allowing us to comment. Should you have any further questions, please feel free to contact me at (313) 373-7474 or at BillEmerson@quickenloans.com.

A handwritten signature in black ink, appearing to read "William Emerson".

William Emerson
CEO
Quicken Loans