



March 15, 2019

The Honorable Mike Crapo
Chairman, U.S. Senate Committee on Banking, Housing, and Urban Affairs
534 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Sherrod Brown
Ranking Member, U.S. Senate Committee on Banking, Housing, and Urban Affairs
534 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Senators Crapo and Brown:

On behalf of Credit Karma, I write in response to the Senate Committee on Banking, Housing and Urban Affairs' ("Committee") request for comments regarding the collection, use, and protection of sensitive information by financial regulators and private companies. We appreciate the opportunity to respond to the Committee's request, and we commend the Committee for its leadership on this important issue.

As a leading consumer-centric personal finance technology company with more than 85 million members in the United States and Canada, including almost half of all U.S. millennials, Credit Karma, in partnership with its lending partners, has facilitated more than \$40 billion in credit lines across financial products including credit cards, personal loans, mortgage refinancing, automotive financing, and student loan refinancing. Credit Karma's services also include Credit Karma Tax, a completely free, DIY tax preparation service.

As the Committee continues to consider legislative proposals during this ongoing debate, we believe that four (4) core principles should form the basis of any privacy, data security and data breach notification legislation, which serve as a backdrop for all of our responses:

- Any federal effort should produce a clear federal privacy, data security, and breach notification regime that preempts all analogous state laws;
- Public enforcement from the relevant state regulators and state attorneys general strikes the appropriate balance between ensuring that the relevant federal and state consumer protection regulators are monitoring and responding to privacy and data security risks while also creating an enforcement regime that regulated entities of all sizes can reasonably manage and comply with;

- One of the best ways to encourage the kinds of internal privacy and data security practices or “cyber-hygiene” necessary to adequately protect consumer data is by incorporating into any legislative proposals clear safe harbors that encourage regulated entities to pursue certifications for their data security practices and information technology infrastructure that goes beyond Gramm-Leach-Bliley and its implementing regulations and state data security and privacy laws; and,
- Any federal privacy, data security, and breach notification regime should be technology-neutral, flexible to fit various business models, risk-based, and be accompanied by FTC rulemaking such that the regime can evolve along with a constantly-evolving threat and risk landscape.

1) What could be done through legislation, regulation, or by implementing best practices that would give consumers more control over and enhance the protection of consumer financial data, and ensure that consumers are notified of breaches in a timely and consistent manner?

We believe that these are three discrete issues – consumer control, enhancing protection of consumer data, and timely notification of breaches – that all require distinct approaches.

Consumer Control: Credit Karma fully supported the Consumer Financial Protection Bureau’s Authorized Financial Data Sharing and Aggregation Principles (“Principles”), and as a member of the Consumer Financial Data Rights Group¹, we fully support data portability and believe the Principles should be codified legislatively and incorporated into any federal privacy legislation.

Credit Karma is a member-driven organization, and our members’ data is only shared at the instruction of our members and under no other circumstance, so we firmly believe that empowering consumers begins and ends when they have full control of their personal information. We give our members full control of their data, and we believe that codifying consumer-authorized financial data sharing and aggregation consistent with the CFPB’s Principles would be the best way to enshrine consumer control into federal law.

Enhancing Protection of Consumer Data: We believe the best way to encourage the kind of “cyber-hygiene” for companies that enhances the protection of consumer data is to develop proposals that create clear safe harbors for companies to obtain security certifications that go above and beyond existing data security requirements. Building safe harbors that encourage regulated entities to go the extra mile in creating the technological and data security infrastructure that effectively monitors, detects, and responds to safety threats is the best legislative approach for encouraging the kind of data security practices we all want to see moving forward. Doing so creates clear standards for compliance that give regulated entities clear incentives for incorporating best practices into their privacy programs.

¹ Consumer Financial Protection Bureau, “Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation.” (October 18, 2017). Available at: https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf.

Timely Notification of Breaches: Data breaches do not recognize state boundaries, and our regime for notifying consumers should not either. Credit Karma supports a clear, national standard for the timing and method of disclosing any breach notification, and a clear, single definition for what constitutes a breach that acknowledges the practical reality of how businesses detect and process potential unauthorized access of sensitive consumer information.

Credit Karma has members in every state and the District of Columbia. Accordingly, we currently comply with 55 unique data breach notification regimes across the states, territories and the District of Columbia.²

For us, this means competing and occasionally inconsistent key operational definitions of what constitutes a breach, inconsistent notice requirements where simply pegging our compliance practices to what is considered the most comprehensive state statutes does not necessarily constitute compliance in every state or meet regulators' expectations. Of particular importance for Credit Karma, is ensuring that any national data breach notification requirement is triggered when it is confirmed a breach has actually occurred and that the time period to disclose begins only upon the identification of a substantial harm. Finally, any data breach notification regime must ensure that disclosures are meaningful and only issued when there has been a substantial data breach of national implications where there is clear and substantial harm. Otherwise, there is a risk of consumer confusion or disclosure fatigue.

2) What could be done through legislation, regulation, or by implementing best practices to ensure that financial regulators and private financial companies (including third-parties that share information with financial regulators and private financial companies) provide adequate disclosure to citizens and consumers about the information that is being collected about them and for what purposes?

Based off our experiences in the industry, we feel best suited to focus on our response on the practices of private financial companies. At the onset of a consumer relationship, we believe consumers should be given a clear disclosure that clearly sets forth how a consumer's information will be used. And, we believe that this disclosure should be made readily available through the companies' website.³ A useful legislative or regulatory exercise would be to extend GLBA's model disclosure policies to financial institutions and non-financial institutions alike.⁴

We would caution against legislative approaches that would seek to require disclosure every time a consumer's data is used pursuant to a comprehensive privacy policy. As previously stated, consideration should be given to any requirements that may cause consumer confusion or run the risk of disclosure fatigue. We believe that re-disclosures should only occur if there are material

² Foley & Lardner LLP, "State Data Breach Notification Laws" (last accessed March 8, 2019). Available at: https://www.foley.com/files/Publication/c31703ac-ee93-40a5-b295-7e1d9fe45814/Presentation/PublicationAttachment/903a95c5-0154-4091-88c7-b6438fed6127/18.MC12803%20Data%20Breach%20Chart%20012019%20V2_edit.pdf.

³ Credit Karma, Privacy Policy (effective date May 31, 2018). Available at: <https://www.creditkarma.com/about/privacy-20180531/>.

⁴ Federal Trade Commission, Model GLBA Privacy Form, (last accessed March 8, 2019). Available at: https://www.ftc.gov/system/files/documents/rules/privacy-consumer-financial-information-financial-privacy-rule/privacymodelform_optout.pdf.

changes in a firm’s privacy policy, and compliance should be permitted if the amended privacy policy is shared electronically either via email or on a link prominently provided for on the firm’s website.

3) What could be done through legislation, regulation, or by implementing best practices to give citizens and consumers control over how financial regulators and private financial companies (including third-parties that share information with financial regulators and private financial companies) use consumer data?

As noted above, Credit Karma fully supports consumer financial data portability and the CFPB’s Principles, including codifying the Principles legislatively or formally adopting them through a GLBA-related rulemaking. This is a step we believe gives consumers meaningful control of their data. Additionally, we believe that any control regime should require that regulated entities provide consumers the ability to opt-out of their data being sold, the right to know what information is being collected and how their information is being used (provided through a clear privacy policy, *supra*, and/or upon a reasonable request), and the right to request their data be deleted (with appropriate exceptions⁵). But, any such requirements should define the term “consumer” such that it does not include employees, and any such standards should be a part of a single, national standard that affirms consumer portability and consumer control at every phase of a consumer relationship for account creation to account termination.

4) What could be done through legislation, regulation, or by implementing best practices by credit bureaus to protect consumer data and to make sure that information contained in a credit file is accurate?

Credit Karma is not a credit bureau as the term is defined in the Fair Credit Reporting Act. As a general matter, we describe above the steps we believe Congress should take to create legislative safe harbors that incent covered entities to pursue data security certifications that extend beyond compliance with GLBA and its implementing regulations and relevant state data security standards.

We are also aware of general principles regarding FTC rulemaking, civil penalties, and federal regulator and state attorneys general enforcement that gives regulated entities further incentive to comply with relevant laws to protect consumer data. We also believe that these principles incorporated into a single, national standard that includes clear safe harbors for entities that secure the requisite security certifications will go a long way in ensuring that all financial institutions – including credit bureaus – are adequately protecting consumer data.

⁵ Two examples where we believe appropriate concessions should be made regarding the right to delete information concerns human resources information and the steps that Credit Karma takes to retain a members’ information after they terminate an account for security purposes. Regarding the former, the California Consumer Privacy Act currently defines a “consumer” so broadly that it includes employees who now have a right to request that any personal information (as defined in the CCPA) be shared or deleted upon which includes personnel-related matters (e.g. internal investigations). Regarding the latter, we retain some information once an account has been terminated for identifying purposes only to ensure that fake accounts are not re-opened in a members’ name. We believe that any legislative proposals should be mindful of the kinds of unintended consequences created by unnecessarily broad definitions of terms like “consumer” and “personal information.”

Finally, regarding the accuracy of information contained in credit reports, Credit Karma has developed what we believe to be an industry-leading, consumer-centered dispute function through TransUnion that allows consumers to dispute errors easily on website on our app.⁶ Since its inception, Direct Dispute™ has removed more than \$10.2 billion in mistaken debt from TransUnion reports. Legislatively, the Committee could explore requirements that credit reporting agencies must establish direct dispute mechanisms with third-party providers like to develop consumer-friendly, direct dispute features modeled after Direct Dispute™.

In terms of legislative proposals to improve furnisher accuracy, one is not readily apparent from our vantage point. We believe that the Fair Credit Reporting Act (FCRA's) standards regarding accuracy requirements of data furnishers is sufficient, and as a practical matter, it is impossible to legislate a solution whereby millions of data points being shared between furnishers and credit reporting agencies daily becomes error free. Therefore, we believe that technological solutions like our Direct Dispute™ function that empowers consumers to easily fix credit reporting errors is the most practical solution to address errors in credit reports.

5) What could be done through legislation, regulation, or by implementing best practices so a consumer can easily identify and exercise control of data that is being (a) collected and shared by data brokers and other firms and (b) used as a factor in establishing a consumer's eligibility for credit, insurance, employment, or other purposes.

Data brokers: First, we believe it is important to clearly define what constitutes a “data broker.” Credit Karma believes that a data broker is an entity that that collects personal information about consumers and sells that information to other organizations without a consumers’ knowledge and consent. As an entity that never sells our members’ information – but whose members’ information is bought and sold by data brokers – we believe that setting clear parameters for who is and who is not a data brokers is vital in mapping out any legislative or regulatory approach seeking to regulate data brokers.

The FTC’s May 2014 study, “Data Brokers: A Call for Accountability” sets forth a set of reasonable policy recommendations that we believe could form the basis of a legislative proposal.⁷ Key in any legislative proposal, however, is clearly defining data brokers so that only those entities that are collecting, packaging, and selling this information to other organizations without a consumers’ knowledge and consent are the ones that would be subject to any new requirements.

Consumer control of data used for credit, insurance, and employment purposes: Consistent with the comments above, consumers should generally know when their information is being used for credit, insurance, and employment purposes. Regarding credit, credit transactions almost always require that the consumer apply for credit, so they should generally be aware that the information they furnish is being used for credit purposes. In cases like that, any proposal should exclude

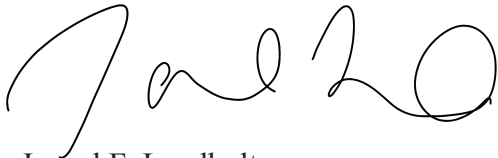
⁶ Credit Karma, “How to dispute errors on your TransUnion credit report with Credit Karma’s Direct Dispute™ feature,” (updated December 4, 2018). <https://www.creditkarma.com/advice/i/credit-karma-direct-dispute/>.

⁷ Federal Trade Commission, “Data Brokers: A Call for Accountability” (May 2014). Available at: <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf>.

from additional obligations instances where the information in question is being shared by the consumer themselves (or at the consumers' instruction). This is likely also the case with insurance where, in cases where the consumer is sharing information, or their information is being shared by a third party at the consumers' direction, they should not be subject to additional requirements given that the consumer is aware of the information being shared and its intended purpose. In cases where a consumer is unaware that their information may be sold or shared with a third party for any of these purposes, this information should be disclosed with clear explanations for how the information will be used.

Credit Karma appreciates the opportunity to submit comments, and we look forward to continuing to engage with Committee staff on privacy, data security and breach notification matters throughout the 116th Congress. Should you have any questions about the submission, please contact me directly at jarrod.loadholt@creditkarma.com.

Respectfully,

A handwritten signature in black ink, appearing to read "Jarrod F. Loadholt". The signature is fluid and cursive, with the first name "Jarrod" being the most prominent part.

Jarrod F. Loadholt
Director, Legislative and Regulatory Affairs