National Association of Industrial Bankers

60 S. 600 E. SUITE 150
SALT LAKE CITY, UT 84102
(801) 355-2821
INDUSTRIALBANKERS.ORG

March 15, 2019

United States Senate Committee on Banking
Housing and Urban Affairs
Chairman Mike Crapo
Ranking Member Sherrod Brown (D-Ohio)
534 Dirksen Senate Office Building
Washington, DC 20219

Via Email to: submissions@banking.senate.gov

Re: Industry Feedback on Data Privacy, Protection and Collection

To Committee Member Staff:

The National Association of Industrial Bankers[1] is a trade association and we appreciate the opportunity to comment on the important and timely topic of control over personal information and commend the Committee for requesting comments from interested parties.

Our members understand why the focus of your inquiry is companies that acquire and share personal information without the customers' knowledge and in ways the customer does not understand or have an opportunity to opt out of. This emerging business model clearly warrants the attention of Congress and regulators. However, for reasons described below, a good policy needs to distinguish between beneficial and detrimental uses and promote choice when the person will understand the consequences. To the largest extent, consumers don't understand how information is used to enable even the most basic transactions using a card, such as buying groceries.

[1] First chartered in 1910, industrial banks operate under a number of titles; industrial loan banks, industrial loan corporations First, or thrift and loan companies. These banks engage in consumer and commercial lending on both a secured and unsecured basis. They do not offer demand checking accounts but do accept time deposits, savings deposit money market accounts and NOW accounts. Industrial banks provide a broad array of products and services to customers and small businesses nationwide, including some of the most underserved segments of the US economy. Our members are chartered in California, Nevada and Utah.

We note at the outset that most of our members do not share customer information with any party that is not providing services to the bank that are necessary to deliver the bank's products and services. For example, most banks contract with a third party to provide the bank's core processing and accounting systems. A customer using a debit or credit card is most often interacting with a third party operating under a contract with the bank. This type of data sharing has been unrestricted since the current privacy laws were enacted as part of the Gramm-Leach-Bliley Act in 1999. Placing additional restrictions on this type of data sharing would make it impossible for banks to deliver many of their most basic products and services.

The complexity of current payment processing systems is both extensive and largely unknown to people outside the industry. In the past, to get paid a merchant only needed to open a checking account at a bank and deposit cash and checks at the end of each day. Today, in order to accept credit and debit cards, a merchant will usually hire an "independent service organization" (ISO) to install card readers and connect to payment systems that include a processor for the merchant and an "acquiring" bank. The processor receives the payment data from the card reader at the merchant's check out counter and routes it to the acquiring bank. The processor also creates a record of each transaction for multiple purposes. The acquiring bank acts as a gateway to the interbank networks such as Visa and Mastercard. The acquiring bank routes transactions through the network to another processor working for the bank that issued the card to obtain authorization for that transaction. At the end of the day, the merchant processor compiles all of those transactions into batches that are sent to Visa and Mastercard for settlement with the issuing bank.

We believe this background justifies classifying this kind of transaction data as belonging to the merchant. It must control that data to collect for purchases made with a card. It rightly belongs to the merchant as much as a check or cash given for payment. Although like a check, it must be shared through the parties involved in the payment network in order for the merchant to be paid.

Adding to this complexity is a group of banks that partner with merchants to provide in store financing for purchases. A good example is a store that sells furniture and appliances. Many people do not want to use their general purpose credit or debit card for such large purchases. Offering financing options is literally critical to such businesses and beneficial to the customer by enabling purchases when needed by the customer. Most merchants could not survive if they only accepted cash or check or an outside card. In those cases the partner bank finances purchases on the spot and both the merchant and the bank collect information about each purchase. Both parties must collect and retain that information for that sale to occur. This type of financing would not be possible if a consumer could direct the merchant to not share that information with a third party because the bank and its contractors would all be third parties.

Beyond completing these transactions, both merchants and their partner banks utilize information about past purchases to develop marketing plans. It enables merchants in conjunction with their finance partners to provide customers with discounts and product ads designed to meet their individual tastes and financial capabilities. That should be permissible for the partner bank as well as the merchant because the partner bank often has the scale to operate more robust marketing analytics and often has data from multiple merchants to better analyze market trends.

Current laws and regulations require a lender to notify each borrower about how it will use the person's information and to allow the customer to opt out of any use beyond what is needed to provide the original loan or other service. This logical arrangement has worked well for the past nearly 20 years with regard to banks and other financial services providers. In our view, that “ain't broke” and doesn't need fixing.

Issues relating to privacy and control of information have mostly arisen in connection with non financial companies that gather personal information such as Facebook. Its apparently free service as a social network relies on gathering and selling personal information about users to third parties. We understand the concerns about this practice and the difficult task of drawing clear lines between legitimate uses and those uses that policy makers might want to restrict. Defining those lines must be carefully undertaken to avoid giving opt-out or opt-in choices that unduly restrict beneficial uses such as the discounts and tailored offerings described above.

Basically, while it is desirable to let people know and control how their personal information is used, it is also the case that many times people cannot know all the positive ways in which their information is used and so cannot make informed choices about restricting its use. Our members encourage their customers to be informed and make good choices, but choices should be provided only when a person understands what he or she is choosing and the consequences of that choice. By way of analogy, a patient should be able to choose whether to have a surgery but not how to perform the operation, and the hospital should not be prevented from reviewing medical records for the purpose of developing protocols for future care.

Based on the foregoing, we respectfully reply to the Committee's specific questions as follows:

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?***

Answer: Control and protection are different matters.

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?

Answer: We believe the current requirements contained in the Gramm-Leach-Bliley Act are workable and sufficient. As described above, listing all of the parties that must obtain personal information in even a simple transaction would be pointless. The only useful information is whether an entity plans to sell personal information to third parties for reasons having nothing to do with the products and services requested by the consumer. That is already required.

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?

Answer: See foregoing answers.

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?

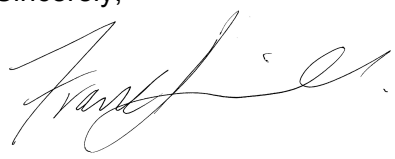
Answer: Our members believe current laws and regulations provide the best method for individuals to access and correct their credit files.

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.

Answer: Our members strongly caution against creating new means for consumers to change the information in their credit reports except if the record contains errors. Lenders, insurers and employers all have legitimate and important reasons for utilizing such reports. Someone who has committed fraud or other imprudent acts should not be able to conceal that from future lenders, insurers or employers. Additionally, this information plays a key role in most fraud control programs. Online lenders, for example, compare information provided by a loan applicant with multiple databases containing personal information such as prior addresses, employers, name spellings, etc. to detect identity theft. Limiting access to this kind of information will make the system less safe, not more secure.

The conundrum is obviously limiting the spread of personal information in ways that would increase the risk of identity theft and unwanted solicitations without limiting these beneficial uses.

Sincerely,



Frank R. Pignanelli
NAIB Executive Director