National Pawnbrokers Association®

March 14, 2019

The Honorable Mike Crapo, Chair
Committee on Banking, Housing, and Urban Affairs
United States Senate
534 Senate Dirksen Office Bldg.
Washington, D.C. 20510

The Honorable Sherrod Brown, Ranking Member
Committee on Banking, Housing, and Urban Affairs
United States Senate
534 Senate Dirksen Office Bldg.
Washington, D.C. 20510

Transmitted via: submissions@banking.senate.gov

Re: Collection, Use, and Protection of Sensitive Information by Financial Regulators and Private Companies

Dear Chairman Crapo and Ranking Member Brown:

The National Pawnbrokers Association appreciates the opportunity to comment on the collection, use, and protection of sensitive information by financial regulators and private companies. Collection and use of transaction data by state and local law enforcement agencies, and in a few cases by federal agencies, has been a concern of NPA members for more than 15 years. Our members believe that protections for transaction data collected and used by state and local agencies is inadequate and needs improvement through federal legislation and regulation. Additionally, more robust oversight of collection and use by federal agencies could reveal the need for enhanced regulation.

The National Pawnbrokers Association (NPA), founded more than 30 years ago, is the only nationwide trade association for the pawn industry, which has approximately 10,000 locations. The pawn industry has been regulated in many states since World War I (and, in states such as New York, back to the 1890's) and is governed by 15 federal statutes and regulations.

National Pawnbrokers Association
PO Box 508
Keller, TX 76244
Tel: (817) 337-8830 ~ Fax: (817) 337-8875
www.NationalPawnbrokers.org
Info@NationalPawnbrokers.org

The NPA aids members in bringing their views before local, state, and federal agencies and educates industry members about their compliance responsibilities. Our board, staff and consultants also advocate for protections of pawn consumers, particularly with respect to privacy protections that apply to all consumers of financial services under the Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (GLBA), and under the Fair Credit Reporting Act (FCRA).

Some NPA members operate more than one store; most of these owners and many others in the industry qualify as "small businesses" serving members of local communities. Pawnbrokers generally know the needs of their communities because they live in or nearby the same communities. Recent reports from the Federal Reserve Board and the FDIC suggest that pawnbrokers serve part of the nearly 40 million unbanked or underbanked adults who may need safety-net credit.

Our comments on the issues outlined in your February 13, 2019 invitation for feedback are limited to the issues with which our members have expressed concerns. We start with two generic comments and then proceed with more specific comments.

Generally, we believe that privacy protections for consumers who obtain safety-net credit from pawnbrokers licensed by state and local governments are not sufficiently strong. This remains the case following the consumer financial privacy protections in GLBA's Title X. The emergence of data brokers that are not governed under GLBA or the FCRA is a factor in our conclusion that privacy protections are not what they should be.

We also believe that many consumers are not aware of the extent of data collected about their daily transactions by data brokers even after the revelations about Facebook and others, and media coverage about high-profile data breaches such as experienced by Starwood Hotels prior to its acquisition by Marriott, Equifax, Anthem, Target and Home Depot, not all of which are covered by either GLBA or the FCRA. The FTC or CFPB could use their authority to flesh out the privacy and safeguards regulations they have ability to write and enforce.

Our second general observation is that legislating the implementation of "best practices" across the consumer financial services, consumer credit reporting, or data broker industries is not a wise idea. Practices are changing at a rapid pace in cyber-security, cyber-resilience, and recovery from data breaches. What was a "best practice" one day may not be applicable by the end of the next day – just as companies in the past that were declared to be PCI-compliant one day then were no longer PCI-compliant the nanosecond after a breach occurred. Thus, our view is that "best practices" is not a useful way to express Congress' expectations about consumer data protection because a "best" practice can be so easily outdated and then lead to unmanageable compliance expectations and undue enforcement actions by regulators. For these reasons, the responses we offer to your questions will focus on legislative solutions, rather than on "regulation" or "best practices."

The sub-question of what improvements might be achieved by regulation under existing statutes requires a willing regulator that is not overzealous in its interpretations. Although we recognize that some federal statutes grant more generous regulatory powers to federal agencies than others, our sense is the issues

the Committee on Banking is reviewing may require new grants of authority to deal with emerging issues or industries that arose since Congress enacted the FCRA over 45 years ago and the GLBA some 20 years ago.

Question 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?

The NPA's major concerns are with data collected by entities not governed by GLBA's Title X or by the FCRA. We believe that these "data brokers" are a fast-growing sub-industry and pose risks to individuals' financial data that they have no power to oversee or prevent.

Every person should have the right to know who is collecting, maintaining, using, or marketing data about them. Some data collection in the United States is transparent – data collected by consumer credit reporting agencies is one such example. Information collected by "data brokers," on the other hand, may take place without individuals' knowledge. Individuals should be informed when their personal information is being collected for use by a state or local government or by a business other than the one the individual dealt with, including those that sell data to candidates for public office. Congress should extend Title X or the FCRA to cover this broad range of data collectors and brokers who do not have direct contact with individual consumers and may not have had direct contact with the business owners that consumers dealt with. These data brokers are deriving business opportunities from the data without obtaining individuals' or business owners' consent.

Data breach notification laws enacted by the states often only require notification if the individual's Social Security number is in the database that was hacked. We believe that other sensitive data, including state drivers' license or identification card numbers, and passport numbers when combined with other personal information (birthdate, home address, cell or land phone numbers) and biometric identifiers (photos of consumers or fingerprints) enable identity theft and that reliance on Social Security numbers as triggers in any future federal data-protection laws or in current or future state data protection laws should not suffice.

Every provider of consumer or business financial products and services should be responsible for using best practices applicable to the types of data they obtain – or are required to obtain to comply with federal, state, or local laws – from their customers without legislation that mandates use of such practices. Rather than being the subject of legislation, using best practices should just be good business and implemented according to the size of the business and nature of the data involved.

Agencies of federal, state, and local governments that obtain individuals' personally identifiable information should be held to high standards of responsibility for the protection of that data. Agencies and their employees should not be allowed to share individuals' personally identifiable information obtained in the course of official duties with members of the general public unless the data sharing is pursuant to duly authorized warrants or administrative subpoenas so that the data are protected properly from subsequent sharing or misuse. Federal agencies should not be allowed to use services provided by data brokers to avoid responsibilities under the federal Privacy Act of 1974.

We recognize that there are cases in which obtaining consumers' consent would not be in the public interest. Agencies, for example, should not be required to alert individuals when doing so would violate standards set by Congress, such as when they are subject to reports covered by specific financial "suspicious activity" reporting under Title 31 of the United States Code or are the subjects of duly authorized "national security letters," administrative subpoenas or Foreign Intelligence Surveillance (FISA) court-authorized warrants, or are covered by one of the statutory exceptions set forth in the Right to Financial Privacy Act of 1978.

Except for cases involving national security or specific, highly sensitive criminal investigations, non-consensual collection of consumers' personal information by government agencies or through unregulated data brokers infringes protections afforded by the Fourth Amendment and is bad public policy. Recent decisions from the Supreme Court have limited government collection of information without due process, including in United States v. Carpenter, 585 U.S. _; 138 S. Ct. 2206 (2018) and City of Los Angeles v. Patel, 576 U.S. –; 135 S. Ct. 2443 (2015).

We also believe that breach-notification requirements should be imposed on the entity that caused the breach, not on a provider of consumer financial services like NPA members who did not cause the breach. In other words, the liability to consumers and the expenses related to data-breach notification should be borne by the data broker if that is whose practices or a lack thereof allowed a breach to occur. Neither liability nor breach notification should be imposed on someone who is remote from the situs of the breach.

The pawn industry presents a special case that compels us to mention how liability and notification expenses ought to be positioned. Specifically, many states and, increasingly, local governments require transaction reporting to local law enforcement authorities; the laws that contain these reporting requirements either specify a method of delivery that is not as secure as it might be, authorize a senior law enforcement official to determine the method of delivery, or require delivery to a third-party vendor as an agent of law enforcement and the third-party vendor sets the method of delivery. If the breach occurs during transmission from the consumer financial services provider or while in the hands of the local government agency or its third-party vendor, pursuant to state or local requirements, then that vendor, not the consumer financial services provider should bear the breach-notification responsibility. We also suggest that a safe harbor or presumption be enacted to protect the consumer financial services provider from data-breach liability to consumers if the provider is required by law to make the transaction report and transmit it using a method over which the provider has no choice or control. This would help the consumer financial services provider reduce litigation expenses for breaches over which they have no control.

To the extent your Committee determines that the Fair Credit Reporting Act should be amended to reach data brokers, we recommend the legislation include related rulemaking authority for the Federal Trade Commission because of its history of responsibility for enforcement of that Act.

Question 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 disclosures to citizens and consumers about the information that is being collected about them and for what purposes?

Both the Fair Credit Reporting Act and the Equal Credit Opportunity Act contain requirements intended to help consumers understand how personally identifiable information and credit histories are used by private financial companies and how consumers may improve their chances of obtaining credit, insurance, or employment. We urge the Committee not to alter these requirements.

Third-party vendors – data brokers -- that obtain consumers' personally identifiable information and transaction records from financial regulators or private financial companies should not be allowed to re-use that information for purposes other than the reasons for which (a) the consumer originally shared the information with the company, or (b) the regulator originally required the third party or the private financial company to obtain it – without disclosure to the individuals whose information they propose to re-use. Such disclosures should not be permitted to be made at the outset of the transaction or account relationship under which the information is originally collected because it is too easy to lose sight of such disclosures while engaged in that original transaction.

Third party vendors that obtain consumers' personally identifiable information and transaction records without the consent of the consumer or of the business with which the consumer dealt should be required to hold those data separately from other data they maintain, and respond to inquiries from affected consumers about the scope of the information and records and requests to correct any errors.

Question 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?

The term "financial regulators" is not defined in your Invitation to Provide Feedback, but we infer that the Committee intended responses to cover all agencies having inspection, supervision, examination, licensure, or enforcement authority over private financial services companies in the United States. In this connection, the term extends to state agencies and departments that charter commercial banks and credit unions or license non-depository providers of consumer financial services. It also should include state and local governments and their law enforcement agencies who have similar powers over licensed non-depository providers.

As mentioned above, a few states and many local governments require pawnbrokers to report transactions with the general public on a wholesale, no-threshold basis.[1] The reports contain personally identifiable

[1] The NPA is aware of two ongoing lawsuits challenging the constitutionality under state laws of local governments' no-threshold data-collection requirements, both of which are in New York State. Our members generally maintain that no-threshold data-collection requirements violate due process protections embedded in the Fourth Amendment to the United States Constitution on grounds much like those articulated by the Supreme Court in City of Los Angeles v. Patel, 576 U.S. – , 135 S. Ct. 2443 (2015) (hotel operators required to collect and maintain records on guests for specified period and to make them available to any police officer for "inspection").

information about all consumers to whom the pawnbroker has advanced monies, as well as details about the consumers' personal property delivered into the pawnbroker's possession and even the proprietary business information of the pawn transaction's amount. The types of information required to be reported has grown over the three decades since these wholesale, suspicion-less reporting requirements began to be required.

It has become popular for many local governments to use third-party vendors to collect these transaction records from pawnbrokers. These providers are not as clearly subject to the FCRA as we believe they should be – given the numbers of transaction records we estimate they hold (running to hundreds of millions in the case of one such third-party provider) and the sensitivity of the information these records contain. In other words, to the extent the information obtained by unregulated data brokers, directly or indirectly from pawnbrokers, is being used without consumers' permission, substantive protections equivalent to the FCRA should govern and limit data brokers re-use of this information.

We are deeply concerned about the emergence of for-profit, for-hire data brokers and their insatiable appetites for data. Over the past two years, these data brokers have tried to get state and local governments to require adding photos of borrowers and the property they deliver to pawnbrokers as collateral to the transmitted pawn transaction records. Beyond the excessive intrusion into the consumer financial transactions governed by GLBA, pawnbrokers have no control over the resulting records the data brokers have or what they do with it. Consumers have no greater control.

Additionally, because government agencies use their data brokers to collect, store, and report back to them the data collected, we have seen evidence that these consumer financial transaction records are being merged into law enforcement databases, which raises questions about use and consumer consent.

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

The definition of credit furnishers in the FCRA should be expanded to include data brokers, including those hired by or providing data collection, storage or reporting services to government agencies for any credit, insurance, background check, security clearance or other employment-related reason. Requirements for safe disposal of consumer information and regular purging when it becomes outdated by current standards should be included. These two protections would reduce longer-term risks to consumers of uses of out-of-date information in the hands of data brokers.

Question 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?

Many of the comments we have offered above also respond to Question 5.

In conclusion, we submit that individuals whose data gets into the hands of for-profit data brokers should enjoy the same privacy, safeguarding, and disposal protections that Congress enacted for individuals who use consumer financial products and services offered by others types of "financial institutions" covered by the GLBA and the Regulation "P" requirements promulgated to implement those requirements.

Consumers whose information ends up in data brokers' databases should enjoy comparable protections from being perused by private financial companies and government agencies that data held by consumer reporting agencies has under the FCRA and GLBA.

Thank you for this opportunity to share views on this important topic. Please contact Fran Bishop, the NPA's Government Relations Liaison, at fbishopdp1@gmail.com for any follow-up information requests.

Sincerely,

Tim Collier
President