April 16, 2019

The Honorable Michael Crapo
The Honorable Sherrod Brown
Senate Committee on Banking, Housing, and Urban Affairs
534 Dirksen Senate Office Building
Washington, D.C. 20510

Re: Response to Request For Information Regarding Feedback on Data Privacy, Protection and Collection

Dear Chairman Crapo and Ranking Member Brown:

Thank you for the opportunity to provide information regarding the feedback on the collection, use and protection of sensitive information by financial regulators and private companies. As the representative of a highly-regulated industry, the National Association of Professional Background Screeners ("NAPBS") seeks to address the three questions posed in your request and we look forward to working with the Committee as it explores various policies related to protecting consumers.

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 Fair Credit Reporting Act (FCRA) and Various State Corollary Statutes Currently Provide Extensive Consumer Safeguards To Control the Use of Data.

As an initial matter, we would like to discuss the role of today's consumer in the background screening process as regulated by various federal and state statutes. It is important to note at the outset that an employer may not procure or cause a consumer report to be procured for employment purposes unless (1) "a clear and conspicuous disclosure has been made in writing to the consumer" and (2) "the consumer has authorized in writing the procurement of the report…" 15 U.S. C. 1681(b). Thus, in the context of employment-related consumer reports, the FCRA preserves the right of the consumer to control whether such a report can be compiled on his/her behalf.

110 Horizon Drive, Suite 210 • Raleigh, NC 27615
Phone: 919.459.2082 • Fax: 919.459.2075 • Email: info@napbs.com

Again, within the context of employment screening, before beginning to prepare a consumer report, NAPBS members must receive certifications from their clients, i.e. employers, that they have both disclosed to the consumer and received authorization from the consumer to procure a consumer report. They must further certify to the consumer reporting agency that they have a permissible purpose under the FCRA, such as employment screening, to request such reports. The information is then compiled into a consumer report and shared with the prospective employer as authorized by the consumer.

In order to prepare the report NAPBS members use information provided by the consumer to obtain public record information - some of which is only available through databases and verify provided information such as education credentials and employment history. The information is then evaluated and compiled into a consumer report within the limited scope as required by the law and further defined by their client. Consumers are entitled to a copy of the report upon request, and are provided the opportunity to dispute the completeness or accuracy of the report.

During this entire process, NAPBS members adhere to statutory and industry standards regulating the use and storage of personal information such as the Gramm-Leach-Bliley Act (GLBA) and the Fair Credit Reporting Act. It is from this unique, experienced perspective that NAPBS respectfully submits its comments on developing the Committee's approach to data collection by financial regulators and private financial companies.

NAPBS would encourage Congress to promote uniform consumer disclosures to promote greater consumer clarity.

As noted in the Committee's Request for Feedback, some consumers are concerned about the collection of sensitive information by financial regulators, private financial companies, and third parties. This type of data collection offers a unique challenge because of the nature of the sharing of data and access to it. With vertical sharing arrangements, consumers must either provide information to background screening companies at the request of their prospective employer or provide information to a prospective employer who in turn provides that information to a background screening company. In addition, in the frequent case where a consumer has or may have resided in multiple states, an employer will typically provide the consumer or prospective employee multiple disclosure forms for each state. While these forms are similar, they also contain slight nuances in terminology from each other and the required FCRA disclosure serving little to no benefit to the consumer.

Ultimately, consumers are best served by a front-end, single consent solution for the collection, use, storage, and sharing of personal information over an appropriate and contextual life cycle. Without a front-end, single consent solution, consumers are confronted with a lengthy, often confusing list of legal privacy policies in order to make a single transaction – the preparing of a

consumer report for evaluation of employment - and companies unnecessarily face additional costs and burdens to prepare a report that was authorized by the consumer from the outset.

A consumer currently subjected to multiple consent forms with exhaustive terms and conditions, may actually make less-informed decisions than a consumer faced with a front-end overview of the access, sharing, and storage of their data. To improve consumers' ability to provide informed consent, NAPBS envisions a brief, universal consent form that a consumer would sign at the outset of the background screening process.

This consent form would provide a high-level overview of which companies are accessing certain data, why such access is necessary, and how the data will be shared and protected. Moreover, the consent form would still be required to comply with existing statutory and regulatory notification requirements by including necessary information and detailed, actionable information for consumers who wish to learn the details of data use and privacy.

For background screening companies, a universal consent form would reduce the regulatory burden, which would allow companies to focus more resources on the continued protection of consumer data.

As Congress considers policies to improve consumer control over their information, we would encourage Congress to take action to streamline the consumer consent process for consumer reports and help give consumers greater awareness of how their data is used in the context of preparing a consumer report.

NAPBS encourages Congress to review and eliminate Federal and state statutes that impose unnecessary data collection and retention requirements

One fundamental approach to protecting consumer data is to reduce its collection and retention. To that end NAPBS encourages Congress to review and eliminate unnecessary statutory data collection and retention requirements. Existing state and federal law sometimes prevent Consumer Reporting Agencies (CRAs) from disposing of consumer data, which is the most effective method of protecting it. For example, the California Investigative Consumer Reporting Act requires consumer reporting agencies to retain a copy of consumer reports for 2 years. A federal statute could usefully identify any retention period over a year as being potentially excessive, and the FTC could be authorized to take action to limit retention periods to one year (e.g., by a suit for a declaration against excessive state laws).

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?

While mindful that this question appears to be directed towards credit bureaus (as defined in Section 603(p) of the FCRA), NAPBS like to offer for the Committee's consideration a proposal that would help promote accuracy of consumer reports more generally. Specifically, Congress can help promote greater accuracy of searches performed on the federal court repository system by directing the Judicial Conference to modernize PACER through the use of certain identifiers, such as dates of birth, as done by every state court.

NAPBS encourages Congress to take action to improve the accuracy of searches performed on the federal court repository, PACER.

Often as employers run background checks on prospective employees, the process includes a check for federal criminal records, all of which are held in the Public Access Court Electronics Records (PACER). Because searches on PACER are limited to name-only, the systems returns an abundance of irrelevant search results, which makes it difficult to determine whether a criminal record relates to an applicant. The absence of identifiers in PACER leaves the CRA vulnerable to reporting false positives and impeding an applicant's ability to get a job, as well as risking an employer's ability to maintain a safe workplace.

PACER's failure to utilize key identifiers, even minimally, is unlike state and county court repositories around the country. It is important to remember that employers and background screeners already have the date of birth (DOB) and social security number (SSN) and may enter this data into their search criteria to ensure accuracy in the search results without publicly displaying this information. That is often the model employed by state courts. Therefore, in order to enable the public to accurately identify the parties in federal court proceedings (including, civil, criminal and bankruptcy proceedings), Congress should direct the Judicial Conference to establish such rules as are necessary to require the submission of personal identifiers.

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.

Currently, the FCRA provides extensive consumer control and safeguards over the use of data for credit, insurance, employment and other purposes.

The FCRA currently governs precisely the scenario laid out in this question, whereby data is collected and shared for the purposes outlined in 15 U.S.C. 1681(b). As discussed elsewhere in our response, consumers have direct authority over the initiation of a consumer report and employers using consumer reports and CRAs each have their respective obligations under the FCRA, including consumer disclosure and authorization, accuracy, and consumer disputes. Similarly, furnishers of this information also have obligations, including duties to accuracy,

correction/updating, and various notifications. To the extent that parties or individuals act as CRAs but do not comply with the statutory obligations, they are subject to federal/state enforcement actions and/or private rights of action.

NAPBS encourages Congress to harmonize the FCRA with respect to statutory damages.

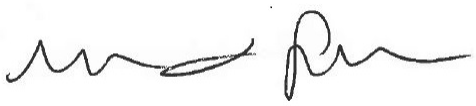
While not asked in your questions, we would be remiss if we failed to point out the need to harmonize the FCRA with other federal consumer protection statutes. Unlike every other major federal consumer protection statute, the FCRA does not impose a cap on statutory damages for civil actions. NAPBS encourages Congress to cap statutory damages under the FCRA. Very often, cases are brought with no harm but result in the imposition of significant statutory damages for technical violations. The FCRA is a very technical statute presenting CRAs and users with numerous technical compliance obligations. Mere technical violations, as opposed to violations causing actual harm, should not be subject statutory damages.

Conclusion:

NAPBS thanks the Committee on Banking, Housing and Urban Affairs for the opportunity to share its comments, and sincerely hopes its comments are beneficial to the development of the Committee's approach to consumer data privacy. The Fair Credit Reporting Act provides a robust regulatory framework addressing a number of the questions raised in your letter. We hope the incremental changes that could be enacted outside the context of the FCRA could also help promote great consumer protection while also mindful not encroach on constitutionally protected free speech. Please know that NAPBS and its members are available and prepared to discuss any questions regarding our industry or the aforementioned concerns.

Thank you for accepting our comments and we look forward to working with you further.

Sincerely,



Melissa Sorenson, Esq.
Executive Director

About NAPBS

The National Association of Professional Background Screeners (NAPBS) is the trusted global authority for the screening profession. In pursuit of their mission to advance excellence in the

screening profession, NAPBS promotes and advocates for ethical business practices and fosters awareness of privacy rights and consumer protection issues. NAPBS is an international trade association of over 900 member companies. Its members provide employment and tenant background screening and related services to virtually every industry around the globe. The reports prepared by NAPBS's background screening members are used by employers and property managers every day to ensure that workplaces and residential communities are safe for all who work, reside or visit there.

NAPBS members range from large background screening companies to individually-owned businesses, each of which must comply with applicable law, including when they obtain, handle, or use public record and private data. NAPBS members also include suppliers of background screening information such as court-record retrieval services and companies that provide access to public record data to background screeners.

The majority of NAPBS's members are consumer reporting agencies ("CRAs") who provide consumer reports (also known as background checks) for employment or tenant screening purposes to employers and property managers.

110 Horizon Drive, Suite 210 • Raleigh, NC 27615
Phone: 919.459.2082 • Fax: 919.459.2075 • Email: info@napbs.com