napbs
National Association of Professional Background Screeners
The Voice of Screening Professionals

May 17, 2018

Honorable Sam Johnson
Chairman, House Ways and Means
Subcommittee on Social Security
2304 Rayburn House Office Building
Washington, DC 20515

Honorable John Larson
Ranking Member, House Ways and Means
Subcommittee on Social Security
1501 Longworth House Office Building
Washington, DC 20515

RE: Preserving Access to Social Security Numbers in Key Federal Databases to Protect Americans' Health and Safety

Dear Chairman Johnson and Ranking Member Larson:

The National Association of Professional Background Screeners (NAPBS) applauds the Subcommittee for convening today's hearing on the future of the Social Security Number. Our 800 members work to promote the safety and security of our communities and workplaces, and in order to meet that objective access to and usage of identifiers such as the Social Security Number (SSN) is vitally important. Indeed, the use of SSNs is a critical tool for our members to meet the federal statutory obligation imposed on our members by the Fair Credit Reporting Act for "maximum possible accuracy." While the SSN was not designed to serve as a broadly-used identifier when it was created in the 1930s, it nevertheless serves that function in many facets of the American economy and modern society. Curtailing its use in that regard would be highly disruptive and costly, and would just lead to a search for similarly broad identifiers to use in its place.

NAPBS understands and shares the concerns expressed by Members of the Subcommittee and other stakeholders about the potential misuse of SSNs to perpetuate identity theft or other fraud. We recognize that in light of the breaches of consumer data extending back many years have likely exposed most consumers' SSN and other personal identifiable information to risk of misuse. Accordingly, the Subcommittee is appropriately concerned about the future use of SSNs and we welcome the opportunity to share some high-level recommendations:

(1) The use of SSNs as an *identifier* should be preserved.

(2) The use of SSNs as an *authenticator* should be constrained.

(3) Market-based technological solutions for authentication will provide appropriate solutions for consumer authentication

(4) The federal government can establish a leadership role, by eliminating the use of SSNs for authentication purposes when used with data held by the federal government.

The difference between using SSN as an identifier and using it as an authenticator is a key difference – but is frequently overlooked. An identifier is a piece of information used to tag other information as belonging to an individual. An authenticator is a piece of information that tends to confirm that the person you are interacting with is the person that they claim to be.

SSN is an ideal *identifier*. Almost all adult Americans have one, and the number is unique to that individual. That means that a simple 10-digit number can be used as a common index to find data. Employers, schools, banks, health care providers, government agencies, and millions of others can quickly identify their records about an individual using SSN. This has enormous value to both organizations and the individual.

But SSN is a terrible *authenticator*. An ideal authenticator is a piece of information that only the person being authenticated and the person authenticating know, and that is difficult to guess. The very fact that SSN is so useful as an identifier – its common format, its widespread use – make it a terrible authenticator because it is not a secret at all. It is likely that, for most Americans, hundreds of organizations have records of their SSN, and at least thousands of individuals have access to those records.

As technology has evolved, credit card companies, phone companies, and others began using SSNs as *authenticators*, to verify that people are who they claim to be. In effectively treating SSNs as secret information, these institutions have increased the danger of identity theft by both augmenting the power of SSNs, and by sharing the data with their employees. The Federal Trade Commission has acknowledged this issue, noting in a 2008 report that "the SSN may not be well-suited as an authenticator itself, but can be and is used effectively to detect potential fraud by permitting access to other authentication-related information."

With the foregoing in mind, it is important to underscore the critical aspect of SSNs as an *identifier*. Redacting important identifying information such as SSNs from public records greatly impacts the ability of background screeners – which are hired by employers to obtain the critical information needed to make accurate and timely hiring decisions. Having an individual's full DOB and at least the last four digits of his/her social security number are critical identifiers for public records as they help ensure the correct data is matched to an individual. This is particularly important when dealing with common names, as search results can potentially yield hundreds of results. Preserving access to SSNs, therefore, will help ensure the greatest possible accuracy when running background checks for individuals serving in sensitive positions.

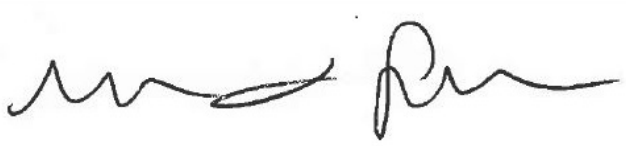
The ultimate solution to authentication will be market-based and technology-focused. But some of the best authentication technology in existence today relies on information that is *identified* using SSN without *authenticating* with the SSN. For example, each of the major credit bureaus uses information from their files about individuals – typically indexed using SSN as a major element – to generate "out of wallet" quizzes to confirm the identity of individuals who request their credit reports. These quizzes ask individuals multiple choice questions regarding matters that the credit files show (such as prior addresses, or the amounts of car or house payments) and

napbs®
National Association of
Professional Background Screeners
The Voice of Screening Professionals

that would be unlikely for another person to know. These questions *authenticate* the person, but the information that leads to the question is *identified* by the SSN.

While the ultimate solution to SSN utilization will be market based and technology focused, the federal government can and should take the lead by restricting agencies' use of SSN as authenticator. Accordingly, NAPBS would like to encourage Congress and Federal agencies to preserve the collection of, use and access to SSNs where appropriate for public safety. Thank you for your time and consideration of these comments.

Sincerely,



Melissa L. Sorenson
Executive Director
National Association of Professional Background Screeners