

THE FINANCIAL SERVICES ROUNDTABLE



1001 PENNSYLVANIA AVE., NW
SUITE 500 SOUTH
WASHINGTON, DC 20004
TEL 202-289-4322
FAX 202-628-2507

E-Mail info@fsround.org
www.fsround.org

Financing America's Economy

August 30, 2011

Ms. Claire Stapleton

Chief Privacy Officer

Consumer Financial Protection Bureau

1801 L Street, NW

Washington, DC 20036

<http://www.regulations.gov>

Re: Docket Numbers: **CFPB-2011-0010**
 CFPB-2011-0011
 CFPB-2011-0012
 CFPB-2011-0013
 CFPB-2011-0014
 CFPB-2011-0015

Dear Ms. Stapleton:

The Financial Services Roundtable (“Roundtable”)¹ respectfully submits these comments in response to the six Consumer Financial Protection Bureau’s (“CFPB”) notices of proposed Privacy Act Systems of Record listed above. We ask that the CFPB:

- limit routine uses of data to those listed by other Federal banking agencies;
- limit the collection of personally identifiable information to what is necessary to carry out statutory duties; and
- implement a robust security system.

Limit Routine Uses

As an initial matter, the Federal banking agencies have historically created a confidential environment with the industry in carrying out their examination and enforcement activities. In the context of the contemplated “routine uses” listed in the six Notices, the CFPB should mirror the routine uses that the Federal banking agencies have included in similar SORs, except to the extent required by law.

The list of routine uses is more extensive in the CFPB notices than it is in the most recent notice published by the OCC in the Federal Register on July 11, 2008. The list of routine uses seems overbroad and should be limited.

¹ The Financial Services Roundtable represents 100 of the largest integrated financial services companies providing banking, insurance, and investment products and services to the American consumer. Member companies participate through the Chief Executive Officer and other senior executives nominated by the CEO. Roundtable member companies provide fuel for America’s economic engine, accounting directly for \$92.7 trillion in managed assets, \$1.2 trillion in revenue, and 2.3 million jobs.

Limit the Collection and Maintenance of Personally Identifiable Information

One threshold question each Federal agency must address is what types of personally identifiable information that it collects ultimately will be maintained in an SOR. The Privacy Act provides that an agency that maintains an SOR shall “maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President.” 5 U.S.C. 552a(e)(1). It is unclear from the descriptions of the SORs the extent to which CFPB intends to collect personally identifiable information about individuals. We urge the CFPB to limit the collection of personally identifiable information about individuals only to that information it actually needs to conduct its statutorily required duties.

We specifically note with concern that the Directory Database Notice (Docket No. CFPB–2011–0015) identifies a wide variety of types of personally identifiable information that may be contained in the contemplated SOR. In particular, the Notice indicates that the SOR may include, among other things, the gender and ethnicity of individuals. On its face, it is not clear how information regarding gender and ethnicity would support the stated purpose of the SOR relating to maintaining “identifying and registration information concerning entities and their affiliates” that offer consumer financial products and services. 76 Fed. Reg. 45,763, 45,764 (Aug. 1, 2011). In light of the sensitivity of this information, we believe that, absent a compelling justification, the CFPB should not collect and maintain in the Directory Database SOR information about the gender and ethnicity of individuals.

Also, information with respect to individuals associated with smaller (total assets of \$10 billion or less) depository institutions, or service providers to such institutions under Section 1026 of Dodd-Frank Wall Street Reform and Consumer Protection Act should be excluded from the scope of the databases. Supervision and enforcement of consumer financial protection for small insured depository institutions and insured credit unions remains with the prudential regulator.

We urge the CFPB to limit collection of personally identifiable information to the minimum necessary for the agency to perform its statutorily required duties. The Office of Management and Budget (“OMB”) has made it clear that if a Federal agency is not maintaining personally identifiable information about individuals, the agency would have no obligation to protect, and would not have to expend resources to protect, such information. As noted by the OMB, “[b]y collecting only the information necessary and managing it properly, agencies can often reduce the volume of information they possess, the risk to the information, and the burden of safeguarding it.” OMB Memorandum M-07-16 at 5 (May 22, 2007). Moreover, the OMB has clarified that “[a]gencies must now also review their current holdings of all personally identifiable information and ensure, to the maximum extent practicable, such holdings are accurate, relevant, timely, and complete, and *reduce them to the minimum necessary for the proper performance of a documented agency function.*” *Id.* at 6.

In addition, as noted above, the CFPB should have flexibility to collect and then properly dispose of information without actually maintaining it. In this regard, if the CFPB needs a particularly sensitive type of information in order to perform its duties, the CFPB could collect such information, use it for the performance of its duties and then appropriately return or dispose of it, without maintaining such information for an extended period of time in an SOR or otherwise. If the CFPB determines later that it needs access to the information that it previously obtained and then later returned or

disposed of, the cost of re-obtaining information likely would be far less than the cost associated with maintaining the security of information that is retained.

As indicated above, it is realistic to expect a strong demand for this information. As a result, the risks associated with unauthorized access to such information (*e.g.*, a hacking incident) will increase. If the CFPB were to suffer a breach of sensitive personally identifiable information, the costs associated with addressing that breach, including the costs associated with investigating the breach, notifying individuals, providing credit monitoring and even embarrassment for the agency, could be great. This reaffirms the point made above; if the CFPB does not maintain information, it has no risk of a breach with respect to that information. To the extent that CFPB needs sensitive personally identifiable information to perform its supervisory activities, the CFPB should strongly consider collecting the information, using it for its supervisory purposes and then appropriately returning or disposing of the information, rather than maintaining the information in an SOR.

Implement a Robust Data Security System

While we recognize that the CFPB is a new agency with many other priorities and deadlines, the protection of personally identifiable information is very important. As described in the Notices, the types of data that the CFPB contemplates maintaining in the SOR are particularly sensitive, including, for example, Social Security numbers. This information would present an attractive target to cyber criminals and others who would seek to obtain large quantities of data stored by the CFPB that could be used to commit identity theft or other fraud.

The CFPB must be alert and pro-active about the wide variety of information security requirements to which it is subject. In this regard, each Federal agency that maintains personal information regarding individuals is subject to a number of detailed information security requirements with respect to that information, including, requirements under the Privacy Act, the Federal Information Processing Standards and guidance from the OMB and National Institute of Standards and Technology. For example, agencies must establish comprehensive written information security programs that include administrative, technical and physical safeguards to ensure the security and confidentiality of information about individuals that is maintained by the agency and to protect against anticipated threats to the integrity of those records that could result in “substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained.” 5 U.S.C. § 552a(e)(10). Moreover, agencies must categorize information and information systems based on level of impact and implement minimum security requirements and controls based on those impact levels. *See, e.g.*, FIPS 199 and 200.

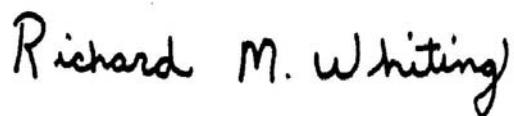
The Notices, however, include only a cursory description of the safeguards that the CFPB will maintain to protect the personally identifiable information maintained in the contemplated SOR. Specifically, the Notice states that “[a]ccess to electronic records is restricted to authorized personnel who have been issued non-transferrable access and passwords” and that “[o]ther records are maintained in locked filing cabinets or rooms with access limited.” 76 Fed. Reg. at 45,765. While we do not believe that a public notice regarding an SOR should include a detailed description of an agency’s information security controls, we do believe it is important that the Notice highlight that the agency has implemented and continues to maintain a comprehensive information security program that contains robust and risk-based information security controls and standards to protect the information stored in the SOR.

Federal agencies are known to be repositories of large quantities of information, and, as a result, Federal agencies have not avoided the scrutiny of criminals seeking to obtain such information. In fact, Federal and state governments have suffered a number of reportable security incidents in which unauthorized third parties obtained access to highly sensitive information about individuals. The threat is real. We believe it is critical that the CFPB address these serious risks in a detailed and comprehensive manner.

It is also important to note that the routine use section of the Notices highlight a wide variety of potential disclosures of information from the contemplated SOR to third parties. As a result, it is critical that the CFPB ensure that it only disclose information to third parties that are capable and actually will protect the information received from the CFPB. In fact, in the interim final rule that establishes procedures for the disclosure of information by the CFPB to third parties, the CFPB indicates that confidential information the CFPB discloses to third parties generally will “remain the property of the CFPB.” 12 C.F.R. 1070.47(a)(1). As a result, when a third party receives confidential information from the CFPB, that information is owned by the CFPB, and it is the CFPB’s obligation to protect that information, as well as to provide notice of any unauthorized access to, or misuse of such information. This is a potential burden that cannot be overstated. As a result, we believe the CFPB should be guided by these information security concerns in determining whether to make a disclosure of information to a third party and also in determining the types of information security controls and requirements the CFPB will impose on any potential recipient of information (as well as how to monitor third-party compliance with these requirements).

Thank you again for the opportunity to share our views with you on this subject. If you have any questions, please feel free to contact me at 202-589-2413 or Rich@fsround.org, or William Henley, the Senior Vice President of Regulation at BITS² at 202-589-2402 or William@fsround.org.

Sincerely,

A handwritten signature in black ink that reads "Richard M. Whiting". The signature is written in a cursive, slightly slanted style.

Richard Whiting
Executive Director and General Counsel

² BITS is the technology division of the Roundtable. BITS fosters the growth and development of electronic financial services and e-commerce for the benefit of financial institutions and their customers.