Consumers Union
Nonprofit Publisher of Consumer Reports

U.S. PIRG
Federation of State PIRGs

CFA
Consumer Federation of America

July 17, 2007

Committee on Ways and Means
U.S. House of Representatives
Washington, D.C. 20515

RE: Ways and Means Committee Markup of Social Security Number Privacy and Identity Theft Prevention Act of 2007

Dear Representative:

We strongly support H.R. 3046, Social Security Number Privacy and Identity Theft Prevention Act of 2007, and applaud Subcommittee Chairman McNulty and Ranking Member Johnson for their leadership in bringing this important legislation forward. The protections provided by the legislation will go far in deterring widespread and unnecessary sale, purchase, and display of social security account numbers (SSNs) that contribute to the identity theft epidemic victimizing approximately 10 million consumers annually.

We urge you to support this legislation and reject amendments that broaden the legislation's already appropriately tailored and balanced exceptions for public and private sale and purchase of SSNs. Such amendments would undermine the integrity and effectiveness of the legislation.

Social security account numbers provide the key to a consumer's financial identity. As a result, they are commonly used by businesses to both identify a person and authenticate the identity of individuals. The widespread use of SSNs as both authenticators and identifiers is among the chief problems the Committee's many hearings have revealed. SSNs are also widely available on the Internet, in public records, on identification cards, and in mail solicitations, making it easy for thieves to access them. Moreover, SSNs have become a commodity for trade, bought and sold by a wide variety of businesses for both legitimate and suspect purposes. The widespread availability of the SSN coupled with the over-reliance of businesses on this number for identification and authentication makes consumers ever more vulnerable to ID theft.

The Social Security Number Privacy and Identity Theft Prevention Act will go far in remedying these vulnerabilities. The legislation will reduce the widespread availability of SSNs by prohibiting government and businesses from displaying SSNs on the Internet, on checks, on employee ID or benefit cards, on student ID cards, on patient cards, including Medicare cards, and on any other card used to access goods, services or benefits. In addition, the bill imposes new obligations on business and government to safeguard the SSNs left in their care. Appropriately, the legislation leaves in place stronger state laws protecting SSN privacy and leaves open future opportunities for states to enhance privacy protections.

In addition, the bill includes the critical prohibition on the sale and purchase of SSNs, subject to appropriately tailored exceptions to meet law enforcement needs, protect public health and safety and address well-defined, legitimate business needs for the SSN. The exceptions provided for in the bill cover a range of legitimate uses for SSNs that may require their purchase and sale. These existing exceptions address the purported concerns of the data brokers, retailers and the financial services industry. They include: law enforcement, national security, public health and safety, research, certain business transactions, administration of benefits, and tax purposes.

Importantly, the bill provides an exception to the purchase and sale prohibition that will allow consumer reporting agencies (CRAs) to continue to purchase and sell SSNs in connection with legitimate purposes under the Fair Credit Reporting Act (FCRA). The exception ensures that the financial and business community may continue to provide and access SSNs to prevent and detect fraud associated with a credit transaction, including extension, review and collection of accounts; for employment purposes, including background checks; insurance; and in connection with *any* transaction initiated by the consumer so long as there is a legitimate business need for the SSN. Preventing and detecting fraud falls within those business needs. Thus, the FCRA exception ensures that businesses will be able to prevent identity thieves from opening new accounts or committing other fraud while ensuring that SSNs cannot be sold for illegitimate purposes, such as to direct marketers, those who would perpetrate fraud, and others lacking a legitimate need for them. Limiting the exception to sale and purchase by or to a consumer reporting agency will help protect against abuse and misuse of the exception by tying it to the statutory and regulatory framework of FCRA. Proposals to broaden the exception by allowing purchase and sale for *any* FCRA purpose, *even when no CRA is involved* and thus FCRA safeguards are unavailable, eliminates these important anti-abuse protections.

In addition, contrary to assertions that a broad range of important uses are prohibited under the bill, in its current form, the legislation does not prohibit *any* use beyond display, sale and purchase. Thus, the bill does not preclude any business from using SSNs internally for identification, authentication, fraud prevention or detection. The bill also does not prohibit any business from purchasing fraud detection and prevention services so long as the service does not involve sale or purchase of the SSN. By allowing for these uses, the legislation strikes a careful balance by preventing commodity-like sales of SSNs to any willing buyer while allowing for purchase and sale where there are legitimate needs for these numbers.

We urge you to reject efforts by the financial services and data broker industries to include additional exceptions under Section 8(b)(2) to the now strong prohibitions on the sale and purchase of SSNs. In particular, the industry is seeking broad exemptions mirrored after those provided under Section 502(e) of the Gramm-Leach-Bliley Act (GLBA). Such a broad exemption threatens to swallow the rule by allowing sale and purchase for a wide range of vaguely defined purposes. Moreover, the general "fraud prevention and unauthorized transaction" exemption under GLBA has been highly ineffective in preventing identity theft. Since enactment of the GLBA in 1999, the incidence of identity theft has grown dramatically. We urge the committee to be wary of adding any similarly vague and open-ended "fraud prevention" exemptions in this Act. Simply because SSNs are sold or purchased under the guise of fraud prevention does not ensure that they will be used for and limited to that purpose. Indeed, the exceptions proposed by industry provide no such assurances. Instead, they would effectively eliminate the general prohibition since virtually any sale or purchase could be tacitly justified under the guise of fraud prevention.

Likewise, broad exceptions for "verification and identification" would negate the improvements the legislation achieves in reining in commodity sales of SSNs. Note that despite the identity theft vulnerabilities resulting from use of SSNs as both authenticators and identifiers, the bill does <u>not</u> prohibit *use* of SSNs for verification and identification purposes. It merely prohibits the sale and purchase for that purpose if the transaction is not with a consumer reporting agency. Thus, any business, such as a lender, is neither prohibited from buying an SSN from a CRA nor from selling one to a CRA. In addition, no business that already has a customer's SSN is prohibited from using a fraud detection service to verify the identity of the customer with an entity providing that service, so long as the service does not involve actual sale or purchase of an SSN.

In summary, the existing exceptions to the purchase and sale prohibition in the Act are sufficiently tailored to accommodate legitimate needs for the sale and purchase of SSNs and to ensure that, correctly or incorrectly, businesses are still able to *use* SSNs to authenticate or identify. Attempts to expand the exceptions should be rejected.

We offer the following suggestions for improving the legislation:

Prohibit Unnecessary Solicitation of SSNs

We strongly support the addition of a provision prohibiting the unnecessary solicitation of SSNs and urge the Committee to adopt such a prohibition. In addition, businesses should be prohibited from requiring submission of a consumer's SSN as a condition of doing business, except where required by law or where submission is necessary to prevent fraud where no other means of prevention are reasonably available. Contrary to the assertions of the industry, the bill currently contains no such prohibitions. The legislation would be strengthened by including them. Consumers are routinely asked to provide their SSN in connection with routine transactions outside the areas of credit, investment, taxes or employment. Ending the widespread, unnecessary solicitation of SSNs would further protect consumers from identity theft by preventing collection of this sensitive information by businesses that may misuse it or from whom it might be stolen.

Truncation Standard Should Prohibit Display of No More than Three Numbers

The lack of a uniform SSN truncation standard has been identified by the Government Accountability Office and others as contributing to identity theft through use of SSNs. Because some businesses truncate five digits and others truncate only four, thieves are easily able to reassemble a consumer's full SSN. A uniform truncation standard will help mitigate that vulnerability. However, the bill as introduced allows a truncation standard to include the last four digits from the SSN. Unfortunately, display of the last four digits of a SSN leaves consumers open to identity theft since these are the only digits of the number that are uniquely attributable to a single individual. Any truncation standard should explicitly prevent display of the full last four digits.

The Consumer Consent Exception should be Narrowed or Eliminated

The Act permits consumers to allow the sale and purchase of their SSN upon the consumer's affirmative written consent so long as the right to refuse consent is clearly presented to the consumer. However, rarely, if ever, is there an advantage for the consumer to consent to the sale or purchase of their SSN outside of the FCRA context. The very real potential for abusive or misleading practices under the exception warrants greater caution by the Committee. Any consent exception should be limited by a requirement that the SSN is in fact necessary for the requested purpose. And, at a minimum, the legislation should require that consumers give *informed* consent that requires that they be counseled as to the significant risks associated with the sale and purchase of their SSN and that those risks are plainly disclosed to them both orally and in writing. In addition, those seeking consent should be prohibited from offering inducements to consumers for their consent.

In summary, we strongly urge the Committee to report the Social Security Number Privacy and Identity Theft Prevention Act of 2007 as introduced, to adopt amendments that would strengthen the bill, and to reject amendments that would frustrate the Act's fundamental objective to curb the widespread availability, sale and purchase of SSNs or that would undermine the ability of states to protect social security account numbers.

Respectfully,

Gail Hillebrand
Senior Attorney
Consumers Union

Edmund Mierzwinski
Consumer Program Director
U.S. Public Interest Research Group

Travis Plunkett
Legislative Director
Consumer Federation of America