

United States Senate

WASHINGTON, DC 20510

February 12, 2018

Nancy A. Berryhill
Acting Commissioner of Social Security
U.S. Social Security Administration
6401 Security Boulevard
Baltimore, MD 21235-0001

Dear Acting Commissioner Berryhill:

We write regarding the growing problem of synthetic identity fraud. The Government Accountability Office describes synthetic identity fraud as involving "...the creation of a fictitious identity, typically by using a combination of real data from multiple individuals and fabricated information."^[1] This type of fraud most often impacts vulnerable populations – particularly children, given that their Social Security Number (SSN) is not yet associated with any live borrowers – and is estimated to result in losses of \$6 billion per year.^[2]

The data points often used by criminals to commit synthetic identity fraud are stolen, but valid. The SSNs are paired with fabricated identity information, such as names and dates-of-birth (DOB). Criminals are able to exploit these data points because there is no efficient, modern method to confirm that a name, SSN, and DOB belong to a real person. This issue has been exacerbated as consumers' expectations around "instant" delivery of financial products and services have evolved.

The Social Security Administration (SSA) recognized the need to address this issue when, in 2002, it created the Social Security Number Verification Pilot for Private Business program. The creation of this program acknowledges that the private sector – particularly financial institutions – needed the ability (with the individual's consent) to verify whether a given name, DOB, and SSN match a government-derived source of truth in order to fight fraud. That pilot program has since evolved into today's Consent-Based Social Security Number Verification system (CBSV), which serves the same role. The CBSV can and should serve as a powerful tool to protect vulnerable populations from identity theft. However, the SSA requirement that users of the CBSV system first obtain the written, physical signature of the individual prior to accessing the database unnecessarily impedes CBSV's usefulness in preventing identity theft. While some financial transactions, such as mortgage applications, are still paper-intensive, rapid technological change has made access to many financial products and services increasingly digital with instant access. In situations, where consumers expect - and financial institutions often make - quick determinations, the physical signature requirement negates the utility of CBSV to combat synthetic identity fraud.

Given the push by SSA and the broader federal government to modernize IT infrastructure, we strongly believe that SSA should make provisions to accept the consent of an individual electronically in order to access CBSV. It is within your authority to make this reasonable and overdue change to accept consent electronically without new legislation. The Social Security Act provides authority and flexibility for the head of SSA to determine appropriate parameters surrounding requests for information and services by private entities.^[3]

^[1] "Identity Theft Services: Services Offer Some Benefits but Are Limited in Preventing Fraud," Government Accountability Office, GAO-17-254. March, 2017.

^[2] "Synthetic Identity Fraud Cost Lenders \$6 Billion in 2016," Auriemma Consulting Group. August, 2017. Accessed at: <http://www.acg.net/synthetic-identity-fraud-cost-banks-6-billion-in-2016-auriemma-consulting-group/>

^[3] 42 U.S.C § 1306(b) reads, in part: "Requests for information...may, subject to such limitations as may be prescribed by the head of the applicable agency to avoid undue interference with his functions under this chapter,

It has long been government policy to encourage electronic signatures. Two relevant federal statutes - the Electronic Signatures in Global and National Commerce Act (E-SIGN) and the Government Paperwork Elimination Act (GPEA) – encourage acceptance of e-signatures. For example, as the Office of Management and Budget (OMB) points out, GPEA “...specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form, and encourages Federal government use of a range of electronic signature alternatives.”^[5] In our view, a consumer’s consent given electronically and received by a financial institution in order to access the CBSV is clearly in the spirit of both of these laws.

We are very sensitive to privacy concerns, particularly when SSNs and other personally identifiable information of consumers are involved. We are pleased, therefore, that the only information provided to users of the CBSV system are machine-to-machine numerical responses corresponding to “yes,” “no,” or, “deceased.” We would not expect SSA to provide users of the CBSV any information on individuals beyond this. Also, as you look to modernize the hardware and software of the CBSV system, we encourage you to ensure the security and integrity of the system are maintained.

The operational costs of the CBSV are funded through enrollment fees and per-transaction fees paid by end-users of the system. In fact, to fund initial start-up costs to build the original system, SSA asked participating private sector firms to: 1) pay an initiation fee and 2) pay upfront for their estimated annual transactions.^[6] Since private sector end-users of CBSV seem willing to maintain and support this funding structure, we see no budgetary concerns that should negatively affect your decision to upgrade and modernize this system to handle expanded demand and ensure near-continuous availability.

Thank you for your attention to this critical issue and interest in fighting synthetic identity fraud. We look forward to working with SSA to better protect our constituents against this crime.

Sincerely,



Bill Cassidy, M.D.
United States Senator



Claire McCaskill
United States Senator



Tim Scott
United States Senator



Gary Peters
United States Senator

be complied with if the agency, person, or organization making the request agrees to pay for the information or services requested....”

^[5] “Implementation of the Government Paperwork Elimination Act,” Office of Management and Budget. Accessed at https://www.whitehouse.gov/omb/fedreg_gpea2.

^[6] Office of the Inspector General, Social Security Administration. “Audit Report of the Consent Based Social Security Number Verification Program.” A-03-08-18067. July, 2009.