December 23, 2019

Social Security Administration, OLCA
ATTN: Reports Clearance Director
3100 West High Rise
6401 Security Blvd.
Baltimore, MD 21235

Via Electronic Mail

Re: Draft eCBSV User Agreement and Related Materials

Dear Ms. Lipsky:

The undersigned associations appreciate the opportunity to comment on the Social Security Administration's ("SSA") draft user agreement (and related documents) for participants in the SSA's electronic Consent Based Social Security Number ("SSN") Verification ("eCBSV") Service ("Draft User Agreement"), issued for notice and comment under the Paperwork Reduction Act ("PRA").[1] We appreciate the SSA's willingness to engage with us and our member firms as it develops the system and implements Section 215 of the Economic Growth, Regulatory Relief, and Consumer Protection Act of 2018 ("Banking Bill").

This letter reflects our initial list of problematic issues in the Draft User Agreement and related documents. As discussions with our members are ongoing, we expect our positions to evolve. To that end, we plan to submit additional comments which will supplement, and possibly substitute, the comments in this letter. While this letter identifies many of the material issues, we expect to identify additional issues in the coming weeks, and we also plan to develop more detailed proposed revisions to the issues we identify.

Our comments are grounded in the Banking Bill and other legal authority for SSA to develop the eCBSV and this Draft User Agreement. At its core, the Banking Bill requires SSA to do the following: (1) Build eCBSV and ensure its proper use through audits; (2) Certify compliance with the Gramm-Leach-Bliley Act ("GLBA"); (3) Effectuate consumer consent, including electronically; and (4) Recover costs. Congress did not contemplate that SSA would enter into a User Agreement with Financial Institutions or Permitted Entities for any purpose beyond those specifically enumerated in the Banking Bill. Consequently, the issues we will address in this letter exceed SSA's legal authority. As such, SSA cannot demonstrate that its proposed information collection is "necessary for the proper performance of the functions of the agency"[2] or that they provide "utility" to the federal government or the public, as SSA is required to demonstrate under the PRA.[3]

In this letter, we address the following: (1) The SSA's proposed regulation and examination of personally identifiable information ("PII"); (2) legal and operational issues

[1] Unless otherwise noted, the terms used in this letter are as defined in the Draft User Agreement.
[2] 44 U.S.C. § 3506(c)(3)(A).
[3] *Id.* § 3501(2) & (4).

related to electronic consent; (3) concerning language regarding audits; and (4) misstatements regarding the SSA's legal authorities. As discussed in more detail below, we have identified many provisions in the draft documents published by SSA that are beyond the scope of the agency's legal authorities and therefore should be removed or substantially redrafted.

SSA's Proposed Regulation and Examination of PII

The Draft User Agreement contains several provisions that would grant SSA regulatory and examination authority with regards to a Permitted Entity's treatment of PII. There is no legal authority for these provisions. Moreover, if these provisions are included in the final User Agreement, undue burdens will be placed on Permitted Entities. These provisions need to be removed or substantially rewritten to focus only on SSA's statutory authority and to minimize the burden on Permitted Entities.

The Banking Bill clearly delineates SSA's authority to oversee Permitted Entities, and that is limited to the use of the database and information related to the database. Specifically, subsection (e) of the Banking Bill requires a Permitted Entity to submit a certification to the SSA Commissioner every two years that includes the following:

> (1) the entity is a permitted entity;
> (2) the entity is in compliance with this section;
> (3) the entity is, and will remain, in compliance with its privacy and data security requirements, as described in title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) **with respect to information the entity receives from the Commissioner pursuant to this section**; and
> (4) the entity will retain sufficient records to demonstrate its compliance with its certification and this section for a period of not less than 2 years. (emphasis added)

Additionally, the Banking Bill permits the SSA Commissioner to conduct audits and monitoring for only two purposes: (1) to ensure proper use by permitted entities of the eCBSV; and (2) to deter fraud and misuse by permitted entities with respect to the eCBSV. These two provisions represent the full extent of SSA's oversight authority.

In contrast and in conflict with this statutory authority, several provisions of the Draft User Agreement attempt to expand the SSA's authority in regards to Permitted Entities maintenance of PII and other confidential information. We have identified the following non-exhaustive list of problematic provisions that do not align with the authorities granted in the Banking Bill or are not necessary as they are not part of process defined in the Banking Bill:

(1) **Definition and Use of the Term PII (Sections I.B p.3; V.B p.12; V.C p.13; IX.A.1. p.17; and IX.A.3 p.17) and use of term "confidential information" (Sections III.A.11 p.6; V.A.3 p.11):** Defining PII exceeds SSA's statutory authority as the Banking Bill does not grant any additional authorities to SSA with respect to PII. Additionally, the term "confidential information" is frequently used but undefined, but would also appear to be out of scope. By contrast, the terms "SSN Verification," "Written Consent" and "Consent Form" are useful and align with SSA's authority in the Banking Bill. Those are

the terms that should be the focus of the User Agreement, not the more expansive definition of PII which includes data completely unrelated to the eCBSV and SSA's authority.

(2) **Scope of On-Site Inspections:** "SSA reserves the right to conduct on-site visits to review the Permitted Entity's and each of its Financial Institution's, if any, documentation and in-house procedures for protection of and security arrangements for confidential information and adherence to terms of this user agreement." (Section III.A.16 p.7). Separately, "SSA may make onsite inspections of the Permitted Entity's or Financial Institution's site, including a systems review, to ensure that the Permitted Entity or Financial Institution has taken the above-required precautions in sections III A and IV B to protect the Written Consent and the information contained therein and to assess overall system security." (Section IV.C p.10).

These provisions do not align with the Banking Bill or any other law related to Permitted Entities' data security and privacy. As discussed above, SSA may only monitor and audit to ensure proper use of the eCBSV and to deter fraud and misuse of the eCBSV. These provisions must reflect that narrow scope.

(3) **Breach Notification (Section V.B.2 p.12):** It appears SSA is trying to implement their own breach notification requirement which is an authority not granted by the Banking Bill. "When the Permitted Entity, including any Financial Institution(s) it services, if any, becomes aware or suspects that PII has been lost, compromised, or potentially compromised, the Permitted Entity or the Financial Institution, in accordance with its incident reporting process, shall provide immediate notification of the incident to the primary SSA contact. If the primary SSA contact is not readily available, the Permitted Entity or the Financial Institution shall immediately notify an SSA alternate, if the name of the alternate has been provided."

This directly conflicts with the Banking Bill and GLBA. The Banking Bill explicitly states that "Notwithstanding any other provision of law, including the matter preceding paragraph (1) of section 505(a) of the Gramm-Leach-Bliley Act (15 U.S.C. 6805(a)), any violation of this section and any certification made under this section shall be enforced in accordance with paragraphs (1) through (7) of such section 505(a) by the agencies described in those paragraphs." Further, GLBA and its implementing regulations govern Permitted Entities' data security and breach notification requirements. This breach notification provision should be removed from the User Agreement.

Electronic Consent

Electronic Signature Requirements

As a foundational issue, the Draft User Agreement and Electronic Signature Requirements document prescribe electronic signature requirements that are beyond the SSA's authority in the Banking Bill and do not align with the Electronic Signatures in Global and National Commerce Act ("E-SIGN Act").

The Banking Bill alone governs the terms of the consumer consent needed to access eCBSV. "Notwithstanding any other provision of law or regulation, a permitted entity may submit a request to the [eCBSV] only (A) pursuant to the written, including electronic, consent received by a permitted entity from the individual who is the subject of the request; and (B) in connection with a credit transaction or any circumstance described in section 604 of the Fair Credit Reporting Act (15 U.S.C. 1681b)." Further, the Banking Bill requires that in order for a Permitted Entity to use the consent of an individual received electronically, the Permitted Entity "must obtain the individual's electronic signature, as defined in section 106 of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7006)." Finally and most notably, "no provision of law or requirement, including section 552a of title 5, United States Code, shall prevent the use of electronic consent for purposes of this subsection or for use in any other consent based verification under the discretion of the Commissioner."

The User Agreement must align with these consent-related provisions of the Banking Bill. However, as currently drafted, the Agreement and the Electronic Signature Requirements document include provisions that are not based in the Banking Bill and are beyond the scope of SSA's authority. It also appears that the Electronic Signature Requirements document includes details and requirements that are not related to obtaining an electronic signature under the E-SIGN Act.

There is no need for the Electronic Signatures Requirement document, and as currently drafted, it erroneously conflates the requirements of E-SIGN Act that are applicable to other circumstances (e.g., obtaining a consumer's consent to receive disclosures electronically). In short, to ensure compliance with the Banking Bill's electronic consent provisions, the User Agreement need only state that to obtain electronic consent, a Permitted Entity must obtain an electronic signature as defined in the E-SIGN Act.

Operational Challenges

In initial discussions with our members, some have raised significant operational concerns with the electronic consent that is the alternative to Form SSA-89. First, it is unclear whether SSA is claiming that there needs to be two check boxes – one for the standard terms and conditions for a credit application (or other FCRA permissible purpose), and one for the SSA verification, or if the SSA language can be appended to the terms and conditions with a single consent check box. A single consent is vastly preferred as it is extremely unlikely that an application would be allowed to go through if a user did not consent to both standard terms and conditions *and* the eCBSV consent. Stated differently, requiring separate consent or dual consents would frustrate the clear purpose of the Banking Bill. Further, a single consent would be consistent with SSA's stated intent to allow the capture of consumer consent to be consistent with existing business and regulatory practices across the financial industry (see SSA FAQs 3.01 and 3.02).

Second, the requirements of Section IV.A.2 (p.8) of the Draft User Agreement are an operational challenge (if not impossibility). For example, the requirement to display all of the

information listed in Section IV.A.2.b (p.9) is impossible for mobile applications or at retail point-of-sale environments.

Thirdly, our members are concerned that the requirement to list the SSN holder's name, SSN, and date of birth on the screen potentially makes sensitive information vulnerable.

Fourth, the last paragraph on page 2 of the Electronic Signature Requirements Document states "…the verification response provided by SSA should not be used as the sole basis of identity proofing and/or authenticating the signer…." It is beyond the scope of SSA's authority under the Banking Bill to dictate how financial institutions factor SSN Verifications into their identity and risk programs. As discussed above, we believe the whole of the Electronic Signature Requirements is unnecessary and should be removed. Further, this concept is already addressed in clearer, more appropriate language in the last paragraph of Section II (p.4) of the Draft User Agreement.

Lastly, we want to ensure that the proposed language meets other applicable legal and regulatory requirements, including providing customer notifications are in plain language and easy for a consumer to understand. The prescriptive language as drafted may be in conflict with current regulatory guidance. Some flexibility in the prose used to comply with existing guidance would be helpful. We are obtaining additional feedback from our members regarding operational challenges and plan to provide that feedback to the SSA in the coming weeks.

Audit Language

The language in Section VIII.A.2 is unclear and incomplete as drafted. It seems that Section VIII.A.2.a (p.16) is meant to encompass depository institutions and credit unions who have no Type I or Type II violations, but as drafted it is unclear. If the reference is meant to be depository institutions and credit unions, one possible solution would be: "If the Permitted Entity is subject to supervision by a Prudential Regulator as defined in 12 U.S.C. § 5481(24), and has no Type I or Type II violations…".

Additionally, the language of Section VIII.A.2.c further muddies the intent of this section. If the intent is for SSA to reserve authority to conduct additional audits based on suspicious activity, it should be stated as such (rather than "random audits") as currently drafted.

Legal Authorities

The Draft User Agreement does not accurately delineate the legal authorities under which the User Agreement and the eCBSV are to operate. For example, Section I.C. (p.3) states that the "legal authority for providing SSN Verifications to the Permitted Entity or Financial Institution is the SSN holder's written, including electronic, consent as authorized by the Privacy Act at 5 U.S.C. § 552a(b), section 1106 of the Social Security Act, codified at 42 U.S.C. § 1306, and SSA regulation at 20 C.F.R. § 401.100, and the Banking Bill." This statement fails to acknowledge that, for purposes of consumer consent, the Banking Bill is the sole legal authority, and specifically overrides the Privacy Act and any other law or requirement – including existing SSA requirements. As discussed above in regards to electronic consent, the statutory language is clear

that the Banking Bill, and only the Banking Bill, is determinative for how to obtain a consumer's consent to access eCBSV. This section should be redrafted to recognize such authority.

Section VIII.D (p.17) similarly fails to acknowledge that the Banking Bill supersedes the Privacy Act. That section states:

> "If the results of the CPA's review indicate that the Permitted Entity and/or Financial Institution has not complied with any term of this user agreement or the Banking Bill, SSA, in addition to referring the matter to the appropriate regulatory enforcement agency in accordance with the Banking Bill, may:
>
> A. Perform its own onsite inspection, audit, or compliance review;
> B. Refer the report to its Office of the Inspector General for appropriate action, including referral to the Department of Justice for criminal prosecution;
> C. Suspend eCBSV services;
> D. Terminate this user agreement; and/or,
> E. Take any other action SSA deems appropriate."

This language in the Draft User Agreement must be amended to recognize the enforcement language in the Banking Bill. Subsection (g)(2) of the Banking Bill states: "Notwithstanding any other provision of law, including the matter preceding paragraph (1) of section 505(a) of the Gramm-Leach-Bliley Act (15 U.S.C. 6805(a)), any violation of this section and any certification made under this section shall be enforced in accordance with paragraphs (1) through (7) of such section 505(a) by the agencies described in those paragraphs." The Draft User Agreement must be clear that violations of the Banking Bill and the certification are solely enforced by the regulatory agencies listed in the GLBA.

In conclusion, we thank you for the opportunity to raise these critical issues and look forward to working with you to address them. As discussed above, this is a preliminary list of issues and recommendations, and is not exhaustive.

Sincerely,

American Bankers Association

Consumer First Coalition