January 17, 2020

Social Security Administration, OLCA
ATTN: Faye I. Lipsky
Director, Office of Regulation and Reports Clearance
3100 West High Rise
6401 Security Blvd.
Baltimore, MD 21235

Office of Management and Budget
ATTN: Desk Officer for SSA

***Via Electronic Mail***

**Re: Draft eCBSV User Agreement and Related Materials, Docket No: SSA-2019-0052**

Dear Director 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, 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 (the "Banking Bill").[2]

Fundamentally, our comments are grounded in the following: Implementation of the Banking Bill must adhere to the plain text of that statute and the clear intent of Congress. The Banking Bill was not ambiguous in describing the full range and limits of the authority granted to the SSA. That authority comprises: (1) Building eCBSV and ensuring its proper use through audits and monitoring; (2) certifying compliance with the Gramm-Leach-Bliley Act ("GLBA"); (3) enabling consumer consent, including by use of an "electronic signature," as that term is defined in the Electronic Signatures in Global Electronic Signatures in Global and National Commerce Act ("E-SIGN Act"); and (4) recovering 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.

Many of the elements of the Draft User Agreement and related documents we address in this letter are ones in which SSA goes beyond what the Banking Bill legally authorized it to do.

---

[1] *Agency Information Collection Activities: Proposed Request*, 84 Fed. Reg. 66704 (Dec. 5, 2019). Our comments respond to the topics on which the SSA is soliciting feedback, including SSA is soliciting comments on the accuracy of the agency's burden estimate; the need for the information; its practical utility; ways to enhance its quality, utility, and clarity; and ways to minimize burden on respondents, including the use of automated collection techniques or other forms of information technology.

[2] Unless otherwise noted, the terms used in this letter are as defined in the Draft User Agreement.

As such, SSA cannot demonstrate that these elements of its proposed information collection are "necessary for the proper performance of the functions of the agency,"[3] or that they provide "utility" to the federal government or the public, as SSA is required to demonstrate under the PRA.[4]

We oppose approval of this proposed collection request in its current form and urge SSA to make revisions, as described below, prior to submitting the request to the Office of Management and Budget for approval. In this letter, we address the following issues and provide recommendations for each that will ensure the creation of the eCBSV system does not exceed SSA's authority under the Banking Bill and adheres to the intent of Congress: (1) The SSA's proposed regulation and examination of personally identifiable information ("PII"); (2) legal and operational issues related to electronic consent; (3) concerning language regarding audits; (4) overstatements regarding the SSA's legal authorities; (5) technical specifications of the eCBSV system; (6) the opportunity for unilateral changes by SSA; and (7) concerns regarding costs and burdens.

## A. 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 imposed on Permitted Entities without providing commensurate benefit to the public or to the government.

The Banking Bill clearly delineates SSA's authority to oversee Permitted Entities, which is limited to the use of the database and information related to the database. Specifically, subsection (g) of the Banking Bill clearly articulates the full extent of SSA's oversight authority by defining the narrow purposes for such audits and monitoring, which are to:

(1) Ensure proper use by permitted entities of the eCBSV; and
(2) Deter fraud and misuse by permitted entities with respect to the eCBSV.

In other words, SSA may audit and monitor for those purposes only to ensure Consent Forms and SSN Verifications are received, processed and retained properly, and to ensure proper systems integration to the eCBSV by Permitted Entities.

Any requirements related to PII, confidential information, or matters outside the scope of the Banking Bill are beyond SSA's statutory authority. Other federal and state laws govern the use and protection of consumers' PII. For example, GLBA governs the use, protection and security of information held by Financial Institutions and their service providers. Certain federal and state agencies, including the Federal banking agencies and Consumer Financial Protection Bureau, are tasked with the oversight authority to ensure compliance with these standards.

[3] 44 U.S.C. § 3506(c)(3)(A).
[4] 44 U.S.C. § 3501(2) & (4).

SSA's only authority in regards to the treatment of PII and data security is to ensure Permitted Entities certify compliance with GLBA with respect to information received from SSA. Specifically, subsection (e) of the Banking Bill requires a Permitted Entity to submit a certification to the SSA Commissioner every two years that includes a statement of compliance with title V of GLBA "with respect to information the entity receives from the Commissioner pursuant to this section…."

Further, the only information received by a Permitted Entity from the Commissioner pursuant to the Banking Bill is the "SSN Verification" as defined in the Draft User Agreement; that is, the response provided by SSA to a Permitted Entity in response to an SSN Verification request. While other pieces of data are required to effectuate an SSN Verification (i.e., the SSN holder's name, SSN and date-of-birth, as described in the term "Fraud Protection Data"), those items are outside the scope of SSA's authority to regulate. As SSA notes, Fraud Protection Data is "data provided by the Permitted Entity…,"[5] rather than the SSN Verification, which is data provided by SSA. Furthermore, as discussed above, the security and privacy of the elements of Fraud Protection Data are protected by the implementing regulations of the GLBA, which is enforced and overseen by federal and state financial regulators. It is also worth noting that none of these data elements are unique to the Banking Bill or eCBSV: These and many other data elements are already required to be collected for regulatory purposes including customer identification requirements under anti-money laundering laws.[6]

Additionally, nowhere does the Banking Bill grant SSA the authority to implement its own data breach notification requirement. Yet, the Draft User Agreement contains significant new requirements on this issue that are, in some respects, inconsistent with existing breach notification requirements under GLBA and state laws.

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 the maintenance of PII and other confidential information by Permitted Entities.

*Recommendations*

To align the User Agreement with SSA's statutory authority, we recommend the following modifications:

(1) Remove the definition and use of the term "PII," (p.3) and use of the term "confidential information," throughout all draft materials. The terms "SSN Verification," "Written Consent" and "Consent Form" are useful and align with SSA's authority in the Banking Bill. Those terms should be the focus of the User Agreement, not the more expansive terms such as PII, which includes data unrelated to the eCBSV and SSA's authority. Therefore:

- The entirety of Section IV.B (p.9) should be rewritten as follows in order to focus on SSN Verifications and recognize existing regulatory obligations:

[5] *See* Draft User Agreement, Paragraph III.A.12 (p 6).
[6] *31 U.S.C. § 5318; see e.g., 31 C.F.R. § 1020.220.*

*The Permitted Entity must retain the signed Written Consent for a period of five (5) years from the date of the SSN Verification request, either electronically or on paper. The Permitted Entity must protect each completed Written Consent and the information therein, as well as the associated record of SSN Verification, consistent with existing requirements under the Gramm-Leach-Bliley Act with regards to confidentiality, protection from loss or destruction, limiting access, and storage of sensitive data.*

*In accordance with section III.A.17, the stored data must not be reused. However, the Permitted Entity can mark its own records as "verified" or "unverified" (or in a similar manner) for future reference. The Permitted Entity cannot reuse a Written Consent to submit another SSN Verification request or for different purposes.*

(2) Paragraphs III.A.9-10(p.6) misrepresent the nature of financial institutions' third-party vendor management regulatory obligations, and III.A.11 exceeds SSA's authority with regards to data security. Therefore:

- Paragraph III.A.9 should be rewritten as follows in order to comport with established regulatory expectations for vendor management:

  *The principal Permitted Entity originating a request and directly receiving consent from SSN holders will be responsible for all SSN Verification requests made, and for complying with the requirement to maintain an audit trail to track all eCBSV activities of itself, whether directly through eCBSV's real-time client application or if operating through a service provider, subsidiary, affiliate, agent, subcontractor, or assignee to effectuate SSN Verification requests.*

- The entirety of Paragraphs III.A.10 and 11 of the Draft User Agreement should be removed and replaced with one item addressing existing regulatory expectations, such as:

  *The Permitted Entity acknowledges that certification of compliance with the GLBA, as required for use of the eCBSV, attests to a Permitted Entity's compliance with that statute's privacy and data security requirements, with respect to information the entity receives from the Commissioner pursuant to the Banking Bill. Additionally, the Permitted Entity acknowledges its obligations to comply with vendor management expectations established by a Federal banking agency, as defined in 12 U.S.C. § 1813(q), the Board of the National Credit Union Administration, or the Bureau of Consumer Financial Protection, as applicable. Therefore, it is the expectation of SSA that the Permitted Entity will handle SSN Verifications and Consent Forms in the same manner as other sensitive data is required to be treated under the GLBA.*

- Relatedly, the Draft User Agreement does not sufficiently distinguish the roles and responsibilities of the different types of Permitted Entities. In particular, both the Draft User Agreement and Banking Bill define the term "Permitted Entity" to include both Financial Institutions *and* firms that are service providers, subsidiaries, affiliates, agents, subcontractors, or assignees of a Financial Institutions. Contracts, as well as existing

regulatory obligations, specify the duties of each party. The Draft User Agreement must recognize these distinctions, particularly with regard to consent. Therefore, we recommend the following new paragraph be added to Section I:

*D. Clarification*
*While the term "Permitted Entities" includes both Financial Institutions and service providers, subsidiaries, affiliates, agents, subcontractors, or assignees of a Financial Institution, SSA recognizes that the roles and responsibilities of each may be different, depending on their chosen method of integration with eCBSV. Therefore, in the case of a Permitted Entity servicing a Financial Institution(s), the ultimate responsibility of receiving and retaining Consent Forms is that of the principal Financial Institution originating an SSN Verification request, not that of the service provider, subsidiary, affiliate, agent, subcontractor, or assignee contracted by the principal Financial Institution to submit such an SSN Verification request.*

(3) In Section IX.A (p.17-18) and Paragraph XV.A.3 (p.20), the term "PII" should be replaced with "SSN Verification."

(4) Audits must be limited to the purposes specified in the Banking Bill. As discussed above, the Banking Bill grants SSA the authority to monitor and audit for the narrow purposes of ensuring proper use of eCBSV and to deter fraud and misuse of the system. SSA does not have the authority to examine the privacy or data security practices of Permitted Entities. Therefore:

- The following language should be deleted from Paragraph III.A.16 (p.7) of the Draft User Agreement: "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 IV.C (p.10), "Onsite and other Reviews," should be deleted and replaced with language consistent with the Banking Bill, such as:

  *SSA may conduct audits and monitoring of the Permitted Entity to ensure proper use of the eCBSV and/or to deter fraud and misuse, specifically (1) the proper use and retention of SSN Verifications and Consent Forms, and (2) appropriate technical integration into the eCBSV system.*

  *As necessary to ensure compliance with the Banking Bill and this User Agreement, SSA may make periodic reviews of the Consent Forms to confirm that Consent Forms have been properly completed.*

(5) The following language in Paragraph V.A.3 (p.11) should be deleted: "The Permitted Entity shall process all confidential information under the immediate supervision and control of Authorized Users in a manner that will protect the confidentiality of the records; prevent the

unauthorized use of confidential information; and prevent access to the records by Unauthorized Users."

(6) The entirety of Sections V.B.1 (p.12) of the Draft User Agreement should be deleted. As discussed, regulating the manner in which Permitted Entities manage and secure data exceeds the authorities granted to SSA by the Banking Bill.

With regard to Paragraph V.B.2, as discussed above, SSA does not have authority under the Banking Bill to establish additional breach notification requirements for Permitted Entities. As such, the entirety of this paragraph should be deleted and replaced with the following:

> *2. Reporting Lost, Compromised, or Potentially Compromised SSN Verifications*
>
> *When the Permitted Entity becomes aware or suspects that SSN Verifications have been lost or compromised, the Permitted Entity, in accordance with its incident reporting process, shall provide immediate notification of the incident to the primary SSA contact, or alternate SSA contact (See Section XV for the phone numbers of the designated primary and alternate SSA contacts).*

(7) Section V.C (p.13) should be rewritten as follows to reflect existing regulatory obligations:

> *The Permitted Entity and all Financial Institutions it services, if any, shall process all SSN Verifications and Consent Forms under the immediate supervision and control of an Authorized User in a manner consistent with the Permitted Entity's certification of compliance with the Gramm-Leach-Bliley Act.*

(8) The following changes should be made to Paragraph IX.A.1. (p.17):

- Item 1.A should be rewritten as follows: *Multiple failures to comply with this user agreement.*
- Item 1.C should be deleted; and
- Item 1.D should be rewritten as follows: *A violation of retaining Written Consents.*

(9) The following language should be removed from Paragraph IX.A.3: "either unauthorized disclosure of PII or…."

**B. Legal and Operational Issues Related to Electronic Consent**

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 E-SIGN Act. The Banking Bill alone, and in particular three provisions, govern the terms of the consumer consent needed to access eCBSV. They are:

1. Paragraph (f)(1), which states: "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)."

2. Paragraph (f)(2), which 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)."

3. Finally and most notably, paragraph (f)(3), which states: "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."

As currently drafted, the Draft User 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 unrelated to obtaining an electronic signature, as that term is defined in the E-SIGN Act. The Banking Bill is clear that the only nexus to the E-SIGN Act with regards to eCBSV is that, for electronic consent, a Permitted Entity must obtain an individual's Electronic Signature, as defined in the E-SIGN Act. Only the cross-referenced definition should be reflected in the User Agreement. The manner of obtaining consent and other requirements in the Electronic Signatures Requirement document is extraneous, unnecessary, and introduces requirements that contradict the law.

Further, the requirements enumerated in the Draft User Agreement pose technical and operational challenges that could significantly compromise the utility of the eCBSV to combat fraud. Customers of financial institutions expect access to products and services across a myriad of platforms (e.g., retail point-of-sale) and digital channels (e.g., mobile applications). Attempting to comply with the burdensome and lengthy requirements called for in the Draft User Agreement in many of these customer channels would not only be operationally impossible, but also highly inadvisable. For example, meeting many of the requirements of section IV.A.2.b (p.9), including the requirements related to the SSA Written Consent Template, may be a violation of financial privacy rules. Specifically, the Draft User Agreement would require a Permitted Entity to list the individual's name, SSN, and date of birth on an electronic screen that may, in many cases, be visible to multiple people. To ensure PII remains protected, it is common practice to protect at least some of that information.

Finally, the Draft User Agreement prohibits the use of electronic consent by certain individuals, and such prohibition is not based on applicable law. Specifically, the Draft User Agreement prohibits electronic consent by legal guardians of adults and parents or legal guardians of children under age 18. For those individuals, the SSA will only accept a SSA-89 signed with a wet signature by the parent or legal guardian. The Banking Bill makes no distinction on who may consent electronically, and therefore these prohibitions should be removed. Furthermore, this prohibition frustrates the stated purpose of the Banking Bill – "to reduce the prevalence of synthetic identity fraud, which disproportionately affects vulnerable

populations, such as minors and recent migrants…."[7] Not permitting electronic Consent Forms to be filed on behalf of minors and other vulnerable populations is directly counter to the purpose of the Banking Bill and the eCBSV.

*Recommendations*

(1) There is no need for the Electronic Signatures Requirement document and it, along with any reference to it in the Draft User Agreement, should be removed. 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) and therefore does not comport with the Banking Bill. The User Agreement must only include a requirement that an individual's electronic signature, as defined in the E-SIGN Act, is obtained for a valid electronic consent.

- Paragraph III.A.6 (p. 5) should be rewritten as follows:

  *The Permitted Entity will obtain an Electronic Signature on an electronic Consent Form.*

- In Paragraph III.A.7 (p. 5), the phrase "meeting SSA requirements" which appears after "Electronic Signature" should be removed.

- Paragraph IV.A.1.b (p. 8) should be revised to remove the reference to the Electronic Signature Requirements document, and therefore the sentence should end after the phrase "with an Electronic Signature."

- Paragraph IV.A.1.c (p. 8) should be revised to remove the phrase "that meets SSA's requirements" after "Electronic Signature."

- Paragraph IV.A.5 (p. 9) should be revised to remove the phase "meeting SSA's requirements" after "Electronic Signature."

- In its entirety, Section IV.E (p. 10) should be revised to read as follows:

  *The Permitted Entity or any Financial Institution(s) it services, if any, will obtain an Electronic Signature for electronic Consent Forms.*

- Section XVI (p. 21) references "by using an approved electronic signature process" which is undefined. This should be revised to read "by using an Electronic Signature."

- Exhibit C (p. 26) the last line should be revised to remove the phrase "that meets SSA's electronic signature requirements."

[7] Subsection (a) of the Banking Bill.

(2) Additional language must be added to clarify that consumer consent for an eCBSV verification does not require its own separate and distinct 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.[8] Thus, while the Draft User Agreement states that written, including electronic, consent can be incorporated into existing electronic workflows or business processes, an explicit statement regarding single consent is critical. Therefore, Section IV.A.1.c (p.8) of the User Agreement should be rewritten as follows:

> *An electronic form of consent, which can be incorporated into the Permitted Entity's or Financial Institution's electronic workflow or business process, including any existing process to capture an individual's consent, signed electronically by the SSN holder with an Electronic Signature. See SSA's Written Consent Template…."*

(3) Paragraph IV.A.2 (p.8-9) of the Draft User Agreement should be deleted. The requirements of this section impose operational challenges (if not impossibilities) and are wholly inconsistent with SSA's stated intent of allowing Permitted Entities to effectuate electronic consent as part of existing consent workflows and business processes. Further, as described above, many of these requirements may run counter to existing financial privacy rules.[9]

Ensuring informed consumer consent that is both consistent with obtaining an Electronic Signature under the E-SIGN Act and that can be incorporated into existing workflows or processes can be achieved via the recommended language we offer in #2 above, and is all that is needed to meet the objectives of the Banking Bill.

(4) In order to ensure that Permitted Entities can incorporate consent for eCBSV into existing workflows and business processes, we recommend the following modifications to Exhibit C:

- Delete the requirement to include the headline "Authorization for the Social Security Administration to Disclose Your Social Security Number Verification."

- SSA should provide flexibility to Permitted Entities with regard to eCBSV-specific consent language. In addition to the language offered in the Draft User Agreement, additional options for the main consent text should be available that achieve the requisite consent but are more compatible with commonly used consent processes, such as:

---

[8] The intent of Congress, as articulated by the Banking Bill's primary author, is relevant: *"Nothing in this provision would require consumers to fill out extra forms, provide extra signatures, or do anything that would significantly alter their expectations for a seamless application experience. The goal is to inform consumers of the possible inquiry to the SSA and allow them to provide consent via the chosen method by the creditor, which now includes electronic signature."* (*See* 164 Cong. Rec. S1714 (2018) (statement of Sen. Tim Scott).)

[9] See, for example, the Interagency Guidelines Establishing Standards for Safeguarding Customer Information set forth pursuant to sections 501 and 505 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 and 6805) which requires, in part, that financial institutions "ensure the security and confidentiality of customer information." Meeting the proposed requirements of the Draft User Agreement to present certain data on a screen is neither secure nor confidential.

*I authorize [name of Financial Institution/Permitted Entity] to verify whether the name, Social Security number, and date-of-birth I have provided match with records maintained by the Social Security Administration.*

- Add language to the User Agreement providing Permitted Entities the ability to make non-substantive, conforming modifications to the language to ensure its clarity and conformity with existing workflows and business processes.

(5) In the event recommendation #4 above is incorporated by SSA, Section IV.E (p.10) of the Draft User Agreement would become redundant and should be deleted.

(6) The first paragraph of Section IV.D (p. 10) should be removed and replaced with the following:

*If the SSN holder is a minor child (under age 18), the Written Consent must be signed by the child's parent or legal guardian. If the SSN holder is a legally incompetent adult, the Written Consent must be signed by the individual's legal guardian.*

**C. Audit Language**

The language in Paragraph VIII.A.2 (p.16) is unclear and incomplete as drafted. It seems that Paragraph VIII.A.2.a is meant to encompass depository institutions who have no Type I or Type II violations, but as drafted it is unclear and excludes credit unions. Additionally, the language of Section VIII.A.2.c further muddies the intent of this section.

*Recommendations*

(1) Paragraph VIII.A.2.a should be rewritten as follows:

*If the Permitted Entity is subject to supervision by a Federal banking agency, as defined in 12 U.S.C. § 1813(q), the Board of the National Credit Union Administration, or the Bureau of Consumer Financial Protection, and has no Type I or Type II violations…."*

(2) Section VIII.A.2.b should be rewritten as follows:

*If the Permitted Entity is not subject to supervision by a Federal banking agency, as defined in 12 U.S.C. § 1813(q), the Board of the National Credit Union Administration, or the Bureau of Consumer Financial Protection,…."*

Further, the word "or" should be deleted from the end of this section.

(3) Section VIII.A.2.c should be rewritten to reflect SSA's intent to conduct additional audits based on suspected violations of the terms of the User Agreement, such as:

*SSA reserves the right to conduct additional audits of a Permitted Entity if SSA has reason to believe the Permitted Entity is in material violation of the terms of the User Agreement.*

**D. Legal and Enforcement Authorities**

The Draft User Agreement does not accurately reflect the plain language of the Banking Bill with regards to legal authorities for consent and enforcement. For example, Section I.C (p.3) fails to acknowledge that, for purposes of consumer consent, the Banking Bill is the sole legal authority, and explicitly overrides the Privacy Act and any other law or requirement – including existing SSA requirements. Specifically, subsection (f)(3) of the Banking Bill states:

*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.*

Further, the Draft User Agreement contemplates an enforcement regime that far exceeds the clear language of the Banking Bill. Specifically, subsection (g)(2) of the Banking Bill states:

*(A) IN GENERAL.—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****.*

*(B) RELEVANT INFORMATION.—Upon discovery by the Commissioner, pursuant to an audit described in paragraph (1), of any violation of this section or any certification made under this section,* ***the Commissioner shall forward any relevant information pertaining to that violation to the appropriate agency described in subparagraph (A) for evaluation by the agency for purposes of enforcing this section****.* [Emphasis added]

*Recommendations*

(1) Section I.C. (p.3) should be deleted and rewritten as follows:

*Legal authority for providing SSN Verifications to the Permitted Entity is the SSN holder's written, including electronic, consent as authorized by the Banking Bill.*

(2) The following language should be removed from Section II of the Draft User Agreement: "Exceeding the scope of the Written Consent as specified in the Written Consent, violates Federal law and subjects the Permitted Entity to civil and criminal liability." That language should be replaced with the following:

*Exceeding the scope of the Written Consent as specified in the Written Consent, violates the terms of this User Agreement and may result in a referral to the appropriate agency as described in the Banking Bill.*

(3) Paragraph VIII.D.B (p.17) should be deleted.

## E. Technical Specifications of the eCBSV System

We appreciate SSA's engagement with our members as the initial planning and design of eCBSV has taken place. We also appreciate that building a system such as eCBSV is an iterative process that takes time. However, it is imperative that firms making the investment of resources necessary to participate in eCBSV be provided an understanding of service level expectations to include a description of the services to be provided and their expected service levels, metrics by which the services are measured, the duties and responsibilities of SSA to provide a highly available system, remedies for Permitted Entities, and a protocol for adding and removing metrics.

*Recommendations*

(1) The term "commercially reasonable uptime and availability" in Paragraph III.B.5 (p.8) must be defined as at least an SLA level of 99.9% uptime and availability.

(2) Language should be added to Section V.A. of the Draft User Agreement stating that eCBSV architectures will ensure response time SLA, as measured by request initiation to message receipt, is appropriate to meet real-time objectives. This language should specifically state a target response time of <250ms with 99.9% of all transactions delivered in <400ms.

(3) Language should also be added to Section V.A. that clearly articulate maintenance windows and planned outages or period of degraded service.

(4) Paragraph III.A.3 conflates the intent of the Banking Bill with regard to the real-time versus batch response time expectation of eCBSV[10] and should be rewritten in part as follows:

*The Permitted Entity may submit requests for SSN Verifications either in one or more individual requests electronically for real-time machine to machine or similar functionality for accurate electronic responses within a reasonable period of time from submission (<250ms, with 99.9% of all transactions delivered in <400ms), or in batch format for accurate electronic responses within 24 hours….*

## F. Unilateral Amendments by SSA

[10] Specifically, paragraph (d)(3) states that the database shall "allow permitted entities to submit—
(A) 1 or more individual requests electronically for real-time machine-to-machine (or similar functionality) accurate responses; and
(B) multiple requests electronically, such as those provided in a batch format, for accurate electronic responses within a reasonable period of time from submission, not to exceed 24 hours.

Section X.2 (p.18) of the Draft User Agreement states that SSA reserves the unilateral right to implement "procedural changes, such as method of transmitting requests and results and limits on the number of SSN Verification requests."

The changes contemplated by this provision are potentially significant for Permitted Entities from compliance and operational perspectives. Such substantive changes could require substantial time to reconcile. Operational changes impacting the "method of transmitting requests," for example, would need to be integrated into development roadmaps and cycles that often span three to six months of advance work.

While SSA is well within its rights to make changes to any aspect of the eCBSV system or terms and conditions for participation, additional clarity and procedural details must be incorporated into this section in order to ensure Permitted Entities are able to maximize usage of eCBSV while minimizing disruption due to sudden, unexpected changes by SSA.

*Recommendations*

(1) Section X.2. should be expanded to clarify what types of limited changes Permitted Entities should expect. Permitted Entities should be given at least six months advance notice of substantive or operational changes, including changes that would impact the limits on the number of SSN Verification requests.

**G. Concerns Regarding Costs and Burdens**

As required under the PRA, the SSA's Federal Register notice details the cost burden on respondents, which includes the Permitted Entities, individuals who consent to the SSN Verification, and certified public accountant ("CPA") firms that will conduct compliance reviews. However, the quantitative conclusions reached regarding the cost burden estimates require additional explanation and detail. In particular:

- This cost burden includes only the 10 Permitted Entities that were selected in the initial rollout and estimates that there will be 307 million people whose SSNs SSA will verify. We ask that SSA provide more detail on how it reached the estimate of 307 million, and if that is representative of the 10 Permitted Entities that are part of the initial rollout, or if that estimate includes a broader group of eCBSV participants that will likely be part of the expanded rollout.

- Relatedly, it is unclear whether the published tier fee schedule reflects the estimates for 10 Permitted Entities or for the expanded rollout. This is critical as SSA states in the Federal Register notice it "…will recover the remaining development costs over three years using the following tier fee schedule." This timeframe will cover the expanded rollout. SSA has also stated that costs, including the remaining 50% of startup costs, will be recovered from "…all users during the first three years of

eCBSV."[11] We ask SSA to provide more information regarding this fee schedule and the assumptions used in it.

- Additionally, as this details the cost burden for only the 10 Permitted Entities involved in the initial rollout, we ask SSA to explain whether additional PRA notices and cost burdens will be provided to reflect the expanded rollout.

In conclusion, we thank you for the opportunity to raise these critical issues and look forward to working with you to address them. Resolving the issues we have identified in this letter in a quick and comprehensive manner is necessary for the successful rollout of eCBSV.

Sincerely,

American Bankers Association

Better Identity Coalition

Consumer Bankers Association

Consumer Data Industry Association

Consumer First Coalition

U.S. Chamber of Commerce

[11] *See* https://www.ssa.gov/dataexchange/eCBSV/fees.html.