April 22, 2021

Via Electronic Mail Submission

Social Security Administration, OLCA
ATTN: Eric Lowman
Acting Reports Clearance Officer
Office of Office of Legislative Development and Operations
3100 West High Rise
6401 Security Blvd.
Baltimore, MD 21235

Office of Management and Budget
ATTN: Desk Officer for SSA

RE: Agency Information Collection Activities, Comment Request, Docket No. SSA-2021-0012

Dear Mr. Lowman:

The undersigned associations appreciate the opportunity to comment on the Social Security Administration's ("SSA") proposed amendments to the User Agreement and Technical Specifications and Systems Security documents for participants in the SSA's electronic Consent Based Social Security Number ("SSN") Verification ("eCBSV") Service, as well as the document titled "Addendum to the Supporting Statement for Electronic Consent Based Social Security Number Verification, 20 CFR 401.100 OMB No. 0960-0817 ("the Addendum"), 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]

We strongly oppose approval of the amendments to the eCBSV User Agreement contained in this proposed collection request. As currently drafted, the proposed amendments would (1) disenfranchise many American citizens traveling or living outside of the jurisdiction of the United States, including deployed servicemembers; (2) inappropriately and unnecessarily expand SSA's regulatory authority; and (3) impose excessive burdens on users of the system. Collectively, these proposals represent a significant regression in the progress SSA has made to date with eCBSV and undermine the intent of the eCBSV as a tool to prevent fraud. Further,

[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.

SSA has not provided a clear articulation of its basis for these amendments, and very little explanation or justification. As such, SSA cannot demonstrate that the 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]

Critically, it is important to highlight the impact these proposed changes are likely to have on fraud in the United States. Today, a portion of identity fraud affecting Americans originates outside the United States. The proposed changes would make it impossible to protect against that. Were these changes to take effect, we would expect to see a dramatic spike in synthetic identity fraud attempts against Americans originating outside our borders as fraudsters realize that an IP address traced by a bank to just outside the U.S. border with Mexico or Canada means the eCBSV will not be available to screen those applications for fraud.

In this letter, we provide analysis and recommendations for the four issues we have identified that, if addressed, will ensure the ongoing development of the eCBSV is not compromised and that the proposed changes meet the requirements of the PRA.

1) Restrictions on the "transferring" and "processing" of SSN Verifications or Written Consents will harm Americans abroad, including servicemembers, and perpetuate fraud from outside the jurisdiction of the United States.

In exchanges with SSA prior to publication of this collection request, we understood the genesis of the proposed changes to be a concern within SSA over the storage of SSA's data, and in particular, *where* it would be physically stored by Permitted Entities. This idea is corroborated in the Addendum to this proposed collection request when SSA states as justification "We are including this language to make it clear that the Permitted Entities must ensure the security and confidentiality of SSN Verifications and Written Consent ***which they store***." (Emphasis added). We do not disagree with amendments to the User Agreement intended to help ensure the security and confidentiality of SSA-owned data, so long as those amendments adhere to SSA's statutory authority under the Banking Bill and other federal agency guidelines.

However, the proposed changes to the User Agreement and technical documentation go beyond restricting how SSA data is stored to include restrictions on the "transferring" and "processing" of SSN Verifications and Written Consents. In attempting to regulate how Permitted Entities process and transfer information from eCBSV, SSA is putting restrictions not just on the location of the data at rest, but also is imposing restrictions based on the physical location of where the consumer is applying for the financial product.

If adopted, SSA's proposed language would prevent a Permitted Entity from accepting Written Consent from an American consumer not physically located within the jurisdiction of the United States. If the Permitted Entity were to do so, that may be considered "transferring"

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

Written Consent outside of the U.S. jurisdiction in violation of the proposed language. The result of the proposed language is that a Permitted Entity will be unable to obtain a Written Consent and subsequent SSN Verification for an American located outside the jurisdiction of the United States. As mentioned previously, these changes will also incentivize criminals to shift their operations outside of the U.S. or to simply load a credit application via a VPN in order to be seen as an application from another country, exacerbating the fraud eCBSV is intended to help prevent.

The range of consumers that would be harmed by this change is expansive – from members of the diplomatic corps and the thousands of servicemembers and their families deployed overseas to vacationers and expatriates. This sort of dramatic limitation of eCBSV clearly frustrates the purpose of the Banking Bill by exposing these individuals to potential fraud that the eCBSV is specifically meant to reduce, and this does not provide any "utility" to the public.

In addition, restrictions on the "processing" of SSN Verifications and Written Consents will place significant resource burdens and costs on many Permitted Entities with operations around the globe. For example, a U.S.-based financial institution that offers credit cards to American consumers may utilize a data center outside the jurisdiction of the United States to process and underwrite applications. In addition, some Permitted Entities maintain call centers with employees overseas who field calls – including those related to credit applications – from American consumers. Under the proposed information collection, Permitted Entities with these and similar operations would be prohibited from "transferring" and "processing" data related to eCBSV to any of these facilities, significantly disrupting business operations.

Regardless of where a Permitted Entity's operations are located around the globe or whether certain services and processes are outsourced to cloud or managed service providers, rules and regulations promulgated pursuant to the Gramm-Leach-Bliley Act ("GLBA") make clear that the ultimate responsibility for the security of the data remains with the Financial Institution. Specific to a cloud or managed service provider, a financial institution will "flow down" to its service providers the obligation to adhere to applicable law and relevant contractual limitations relating to the data to be handled by the service providers (*e.g.*, eCBSV User Agreement). As we have described in previous PRA filings, federal financial regulators have oversight authority over both a financial institution and any entity that the financial institution engages as its third-party service provider. In fact, in the context of regulatory oversight and examination, financial regulators view the activities of a bank's third-party service providers as if reviewing the activities of the bank itself.

Recommendation

- Remove all references to "processing" and "transferring" in the proposed new sections of both the User Agreement and Technical Specifications documents.

2) Any changes should be limited in scope to "SSN Verifications" only, not "Written Consents."

Throughout our engagement with SSA over the past several years, it has been well understood that the SSN Verification as it is defined in the User Agreement is, in fact, SSA's data. This is logical and appropriate because SSA is the source of the underlying data to which the SSN Verification relates. However, in this proposed information collection, SSA has, for the first time, introduced the notion that Written Consent is its property as well. We object to this idea and assert that Written Consent is the property of the Permitted Entity, not SSA, and therefore the storage or access of such data cannot be restricted by SSA as they have proposed.

The Written Consent is part of a credit application, which is the property of the Permitted Entity. It is the Permitted Entity's responsibility to maintain the application, including the Written Consent, in a safe and secure manner, in accordance with GLBA and other applicable law. It is helpful to couch this in the context of a real-world hypothetical: A consumer wishing to apply for a credit product visits the website of a Financial Institution participating in eCBSV and begins the application process. At a certain point in that electronic application flow, the consumer is presented with disclosures and notifications which require affirmative consent, such as an acknowledgment that the Financial Institution, as part of the application process, will obtain a credit report on the consumer. This would also include the OMB-approved eCBSV consent language (Exhibit C in the User Agreement). Does SSA own this portion of the electronic application that was designed, developed, tested by and originated from the Permitted Entity? Moreover, does the fact that a Permitted Entity is providing to a consumer government-approved words on a computer screen or other electronic device convey ownership of all or part of that digital interaction to the U.S. government?

We do not believe the legal authorities cited by SSA – the Privacy Act, 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 – support any of these claims or SSA's assertion of its right to maintain ownership and control of Written Consents. In fact, no reading of the key SSA rule – 20 C.F.R. 401.100 – could reasonably conclude that ownership of "written consents" resides with SSA. To be sure, this regulation makes clear that obtaining written consent is a requirement for disclosure of an official record or information by the Commissioner (as does the Banking Bill); but that is an entirely unrelated standard from the concept of data ownership. To the extent that SSA is concerned with the privacy and security of Written Consents, that matter has already been addressed by the Banking Bill and User Agreement, which both identify GLBA as the controlling body of rules and regulations – the later requiring a certification of compliance with GLBA – and therefore the federal banking agencies as the regulatory authorities with jurisdiction.

Further, in the context of eCBSV, it is the Permitted Entity which is receiving Written Consent from the consumer, as evidenced by the fact that SSA requires Permitted Entities to maintain Supporting Documentation (which may include all completed and signed Written Consents, SSN Verifications, and audit logs or audit trails if required) to demonstrate in the course of an audit that Written Consent was obtained *by the Permitted Entity* for each SSN

Verification request made. The authority to conduct audits, however, does not convey ownership rights of Written Consents to SSA.

Recommendation

- The scope of the proposed changes in both the User Agreement and Technical Specifications should be limited in applicability solely to SSN Verifications. References to Written Consent in the proposed new sections should be deleted.

3) Proposed new regulatory and "verification" requirements are a duplicative and unnecessary encroachment into bank regulation by SSA, and conflicts with FISMA and FedRAMP guidance.

The first iteration of the User Agreement – issued December 5, 2019 – contained numerous regulatory directives and cybersecurity requirements that would have effectively positioned SSA as a new federal bank regulator and examiner. In our letter of January 17, 2020, we strenuously objected to this overreach by SSA into the jurisdiction of federal banking regulators. Through that PRA process, the User Agreement was substantially modified to avoid these pitfalls. We believe this was recognition by SSA and OMB of the sole jurisdiction maintained by the federal banking agencies to write and enforce rules that govern the cybersecurity and privacy practices of financial institutions and their service providers.

The proposed language in this information collection is in direct conflict with the end result of the User Agreement. As described in the Addendum, Change #2 and Change #3 both contain language imposing regulatory obligations related to privacy and data protection on already-regulated financial institutions. Specifically, both Changes state that Permitted Entities "must adopt" certain policies and procedures related to data protection.

Disappointingly, we find it necessary to revisit points we raised 15 months ago in a previous PRA process about an issue we felt confident was resolved, but apparently is not.

The changes proposed in this information collection to the eCBSV User Agreement would grant SSA regulatory 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.

Any requirements related to PII and the handling of sensitive information by Permitted Entities is outside the scope of the Banking Bill and 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. Importantly, these standards apply to the key data elements

involved in an eCBSV interaction: Fraud Protection Data, Written Consents, and SSN Verifications.

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…."

Additionally, SSA's proposed restrictions limiting certain activities to the jurisdiction of the United States is at odds with both the risk-based approach to information security called for by FISMA as well as the government's own guidance to cloud service providers in FedRAMP. Fundamentally, SSA is incorrectly applying an unduly high risk standard to eCBSV data. As background, FISMA calls for agencies to take a risk-based approach to securing data, stating that "[t]he head of each agency shall be responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction…of information…and information systems."[5]

Applying this test to data exchanged through the eCBSV: Permitted Entities submit "Fraud Protection Data" to SSA and receive an "SSN Verification" in response. The "SSN Verification," which we recognize is SSA's data, is a "Yes/No" response. However, as the Banking Bill and the eCBSV User Agreement agree, "Written Consents" are processed and maintained by Permitted Entities and never "cross the line" into a computer system of the federal government, and are therefore outside the scope of FISMA and FedRAMP. Thus, and in line with the points we made in item #2 above, the only appropriate focus of this information collection should be on SSN Verifications.

Despite this, SSA has seemingly proposed to apply a "FedRAMP High" classification to this data. This restriction, which is normally applicable to the Federal government's own cloud systems, is reserved for those few government systems "…where loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. FedRAMP introduced their High Baseline to account for the government's most sensitive, unclassified data in cloud computing environments, including data that involves the protection of life and financial ruin."[6]

The single piece of government data that originates in a government system and is transferred to a Permitted Entity is the SSN Verification. This data element contains no personal information. No reasonable person could conclude that the unauthorized access, use, disclosure, disruption, modification, or destruction of a "Yes" or "No" would amount to a material risk for SSA or the individual whose Fraud Protection Data was verified through eCBSV. Further, no

[5] 44 U.S.C. 3554.

[6] As defined at https://www.fedramp.gov/understanding-baselines-and-impact-levels/.

reasonable person could conclude that the fate of an SSN Verification could impact the government's ability to protect "life and financial ruin."

On a separate but related point, as described in the Addendum, Change #2 and Change #3 both contain the following language: "The Permitted Entity must verify the effectiveness of policies and procedures to ensure the security and confidentiality of SSN Verification or Written Consent and retain appropriate evidence."

This new "verification" requirement is not supported by any justification, has never been an element of any prior iteration of the User Agreement, and is not supported by precedent in the bank regulatory space. Due to a lack of sufficient justification or explanation, it is unclear what problem SSA is attempting to solve with its introduction at this point in time.

Federal regulations relating to the security and confidentiality of PII and other sensitive data maintained by financial institutions and their service providers frequently require the establishment of processes and procedures to meet these high regulatory standards. Federal financial regulators also require ongoing assessments of the efficacy of these rules to ensure they are keeping pace with changing cybersecurity risks. To cite one example, the Interagency Guidelines Establishing Information Security Standards,[7] issued by the federal banking agencies, states that each institution shall "…assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks." Additionally, the Federal financial regulators require institutions to test and evaluate their information security systems through self-assessments, tests, and audits with appropriate coverage, depth and independence. The regulators expect the institutions to use these tools to gain confidence that its information security programs are operating as expected and reaching the intended goals.[8]

"Verifying" the effectiveness of these policies and procedures, as SSA has proposed, is not a requirement that aligns with existing federal regulation. Financial regulators understand that managing risk is a dynamic, evolutionary process and have crafted regulations to accommodate that important reality. SSA's proposed requirement that these policies and procedures be "verified" is not only inconsistent with federal regulations and its own User Agreement, but is an inappropriate, ill-advised approach that imposes unnecessary and duplicative burdens on users of eCBSV.

Recommendation

- The proposed new section III.A.22 of the User Agreement should be re-written as follows in order to resolve all of the regulatory overreach issues we have described throughout this letter and align the User Agreement with existing GLBA regulatory requirements:

  > Consistent with its Permitted Entity Certification and existing obligations under the GLBA, the Permitted Entity shall maintain policies and procedures that 1) ensure the security and confidentiality of the SSN Verifications and 2) ensure SSN

[7] *See "*Interagency Guidelines Establishing Information Security Standards," implementing section 501(b) of GLBA issued by the federal banking agencies (Security Guidelines).
[8] FFIEC IT Examination Handbook: Information Security, pp 52, 54 (Sept. 2016).

Verifications that are maintained in a Managed Service Provider or Cloud Service Provider are encrypted at rest and in transit, and 3) assess the sufficiency of these policies and procedures on an ongoing basis. The Permitted Entity must not provide the Managed Service Provider or Cloud Service Provider the key to unencrypt the SSN Verification maintained in their environment. The Permitted Entity must also ensure that the SSN Verifications are stored within the jurisdiction of the United States (i.e., within the continental United States, Hawaii, Alaska, Puerto Rico, Guam, and the U.S. Virgin Islands).

- The proposed new section V.A.5 of the Technical Specifications and System Security section, as described in Change #3 of the Addendum, should be re-written as follows to align the User Agreement with existing GLBA regulatory requirements:

  Consistent with its Permitted Entity Certification and existing obligations under the GLBA, the Permitted Entity shall maintain policies and procedures to ensure that SSN Verifications are encrypted at rest and in transit. The Permitted Entity must also ensure that SSN Verifications are stored within the jurisdiction of the United States (i.e., within the continental United States, Hawaii, Alaska, Puerto Rico, Guam, and the U.S. Virgin Islands).

4) The definition of "cloud service provider" is overly broad and conflicts with the User Agreement.

The proposed definition[9] of "cloud service provider" is a general definition that is overly broad for purposes of eCBSV. In fact, due to the fact that the definition is extremely broad, it is likely to result in conflicts within the User Agreement and excessive or impossible technical burdens for some Permitted Entities.

For example: Under the proposed changes to the User Agreement, a "cloud service provider" is a "third-party" (which is a "service provider") that offers "cloud-based platform, infrastructure, application or storage services" to Permitted Entities and are restricted from certain activities, such as obtaining encryption keys. However, some Permitted Entities that are also service providers to financial institutions do operate "cloud-based platforms" and provide cloud-based platform and/or application services. Therefore, under the proposed changes, these entities would be both Permitted Entities *and* Cloud Service Providers and would be unfairly limited in their ability to access the data.

This conflict would make it impossible for some Permitted Entities to provide services to Financial Institution clients for purposes of eCBSV. We do not believe this was SSA's intent. Also, as we have described previously, it is important to note that Permitted Entities, Financial Institutions, cloud service providers and managed service providers in the financial services

[9] This appears to be the general-purpose definition developed by Microsoft. See: https://azure.microsoft.com/en-us/overview/what-is-a-cloud-provider/

sector are regulated and overseen to ensure compliance with comprehensive data security requirements.

Recommendation

We request SSA resolve this by taking the following two actions:

1) Modify the definition of "cloud service provider" to limit it to the specific areas of concern for SSA in the context of eCBSV as follows: *A third-party company offering cloud-based infrastructure or storage services.*
2) Add clarifying language to both the definitions of "cloud service provider" and "managed service provider" to indicate that, for purposes of the User Agreement, these definitions do not include "cloud service providers" or "managed service providers" who are Permitted Entities.

In conclusion, we reiterate our strong objection to this proposed information collection. In its current form, it represents a step backward for the development of the eCBSV and implementation of the Banking Bill. We appreciate the opportunity to provide these comments and look forward to working with you and your colleagues to resolve these issues in a way that keeps eCBSV on track for success.

Sincerely,

American Bankers Association

Better Identity Coalition

Consumer Bankers Association

Consumer First Coalition

Consumer Data Industry Association

U.S. Chamber of Commerce