House Committee on Ways and Means
Subcommittee on Social Security Hearing:
"Social Security Administration's Role in Combatting Identity Fraud"
May 24, 2023

Testimony of Katie Wechsler
Consumer First Coalition

Chairman Ferguson, Ranking Member Larson, and members of the Subcommittee: thank you for the opportunity to testify today on the Social Security Administration's (SSA) Role in Combatting Identity Fraud. My name is Katie Wechsler, and I am co-executive director of the Consumer First Coalition (Coalition). Formed in 2018, the Coalition is a group of financial services companies committed to combatting new forms of fraud, protecting identities, and upholding the privacy protections of consumers.

My testimony today is focused on the main priority of the Coalition — combatting synthetic identity fraud through the implementation of SSA's Electronic Consent Based SSN Verification (eCBSV) service. Congress authorized the creation of eCBSV in 2018 to address synthetic identity fraud.

What is Synthetic Identity Fraud?

Before I discuss SSA's eCBSV system, it's necessary to define synthetic identity fraud and understand why it is a considerable threat to consumers. As defined by the Federal Reserve as part of its FedPayments Improvement initiative,

> *Synthetic identity fraud is the use of a combination of personally identifiable information (PII) to fabricate a person or entity in order to commit a dishonest act for personal or financial gain.*[1]

Personally identifiable information that may be used to create a synthetic identity includes information that is unique to an individual (e.g., name, date of birth, Social Security number, and other government-issued identifiers). It may also include supplemental information that can help

[1] "Synthetic Identity Fraud Defined," The Federal Reserve FedPayments Improvement, https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/synthetic-identity-payments-fraud/synthetic-identity-fraud-defined/.

substantiate or enhance the validity of an identity, but cannot establish an identity by itself (e.g., a mailing or billing address, phone number, email address or digital footprint).

Common uses of synthetic identities include:

- Credit repair scams. This involves individuals' efforts to hide negative credit history or bad debt in order to appear creditworthy.
- Fraud for living. This is the use of false identity information to apply for employment or services (e.g., utilities, housing, bank accounts).
- Payment default schemes. These are schemes to use a false identity to obtain goods, cash, or services with no intent to repay over a period of time.[2]

Criminals create a synthetic identity by combining SSNs, names, and birthdates of multiple people, or by combining real information about a single person with fabricated information. A criminal will use this identity to apply for some type of credit, often a credit card. When financial institutions receive an application for new credit, they typically submit an inquiry to one or more of the credit bureaus. If an applicant has fabricated an identity, the credit bureaus will report that the identity does not have a credit history. As a result, the financial institution will reject the application.

This is, however, just the start of the synthetic fraud. Even though the credit is denied, the initial inquiry creates a credit file for the synthetic identity. The criminal will continue with similar attempts to obtain credit, and at some point, likely will be successful in obtaining a loan or credit card, albeit for a small amount. The criminal will use this new line of credit to establish a timely repayment history, often with the addition of "authorized user" tradelines. This repayment history can then be leveraged to obtain higher credit limits and additional accounts. It's a long game, but at the end, the criminal has successfully created a seemingly strong credit profile for a synthetic identity, which they use to obtain a large amount of credit, with zero intent to repay.

[2] FedPayments Improvement, "Synthetic Identity Fraud Defined."

Synthetic identity fraud is reported to be the fastest growing type of financial crime.[3] Synthetic fraud is estimated to cost several billion dollars in losses each year. Basic "Know Your Customer" checks often miss this type of fraud. One analysis found that credit card accounts associated with synthetic identities charge off 50 times more frequently than a typical consumer, for an average of $13,000.[4]

As one example, last year a Georgia man was sentenced to more than seven years in prison for a synthetic identities scheme that defrauded banks out of nearly $2 million.[5] In 2020, federal prosecutors charged two Florida residents with bank fraud conspiracy for allegedly using synthetic identities to commit crimes, including defrauding banks and stealing more than $3 million from COVID-19 relief programs.[6]

While the financial loss is often borne by financial institutions, the true victims are the actual owners of the stolen SSNs. Even worse, a frequent target of this fraud is children. One study found that in one year alone, one million children were victims of identity fraud.[7] Most parents are not checking their child's credit reports, and the child's SSN is rarely used. For fraudsters, this is ideal — an SSN that is not yet in the financial services and credit ecosystem. If a child is a victim of synthetic identity fraud, it could be many years before that fraud is uncovered. It may not be discovered until the child turns 18 and is applying for a student loan or their first credit card. At that point, they have a daunting and painstaking task ahead of them: undoing years of synthetic identity fraud and ensuring it is only their own name that is associated with their SSN.

---

[3] "The Need to Define Synthetic Identity Fraud," The Federal Reserve FedPayments Improvement, p. 3. https://fedpaymentsimprovement.org/wp-content/uploads/synthetic-identity-fraud-definition-overview.pdf

[4] Maxwell Blumenfeld, "Updated customer identification rules are long overdue," *American Banker*, April 22, 2022, https://insight.sentilink.com/hubfs/Bank%20Think%20Article%20American%20Banker%202022.pdf.

[5] "Georgia Man Sentenced to Over 7½ Years in Prison for Synthetic Identities Scheme That Defrauded Banks Out of Nearly $2 Million," United States Attorney's Office, Central District of California, https://www.justice.gov/usao-cdca/pr/georgia-man-sentenced-over-7-years-prison-synthetic-identities-scheme-defrauded-banks.

[6] "Two Men Who Allegedly Used Synthetic Identities, Existing Shell Companies, and Prior Fraud Experience to Exploit Covid-19 Relief Programs Charged in Miami Federal Court," United States Attorney's Office, Southern District of Florida, https://www.justice.gov/usao-sdfl/pr/two-men-who-allegedly-used-synthetic-identities-existing-shell-companies-and-prior-0.

[7] Al Pascual and Kyle Marchini, "2018 Child Identity Fraud Study," Javelin, https://javelinstrategy.com/research/2018-child-identity-fraud-study.

SSA holds the Solution to Stopping Synthetic Identity Fraud

Synthetic identity fraud is more prevalent in the U.S. than in other countries due in part to a strong reliance on SSNs as identifiers.[8] Thus, SSA is key to combatting this type of fraud. SSNs were originally created by SSA for a specific purpose: tracking earnings histories of individuals to determine Social Security benefits. "Over time, the use of SSNs has expanded substantially to become an almost de facto universal identifier in the United States."[9] When an SSN is compromised, it can easily be used by a fraudster to take over an identity or create a synthetic identity. SSA is the one true source of the information needed to determine whether an identity is real or fraudulent.

SSA recognized the problematic SSN-related identity fraud more than fifteen years ago. In 2008, the Agency created a written Consent Based Social Security Number Verification (CBSV) service.[10] This service, which remains in operation, enables paid subscribers to verify a name, date of birth, and SSN match against the SSA's records with written consent from the SSN holder. The CBSV service, however, is a paper-based process that requires a physical or "wet" signature from the SSN holder. This process takes time, and as more of the financial ecosystem went digital, it became impossible for most application channels to use the antiquated, paper-based system.

The Digital Solution: eCBSV

Responding to the need for a more efficient real-time solution, as part of a larger banking bill in 2018, Congress directed SSA to establish an electronic consent-based verification system.[11] The law required SSA to create a system that compares a name, date of birth, and SSN combination provided in an inquiry by a financial institution (as defined by Gramm-Leach-Bliley) or its service provider (together with financial institutions, so-called permitted entities) to confirm or not confirm the validity of the information provided. The system must be scalable and provide real-time machine-to-machine accurate responses. A financial institution may submit such a request to

[8] "Allure of a Synthetic to a Fraudster: Ease of Creation," The Federal Reserve FedPayments Improvement, https://fedpaymentsimprovement.org/wp-content/uploads/allure-of-a-synthetic-to-a-fraudster.pdf.
[9] FedPayments Improvement, "Allure of a Synthetic."
[10] In 2002, SSA had a pilot program, "Social Security Number Verification Pilot for Private Businesses," which was replaced in 2005 with the "Interim Verification Process." The CBSV program replaced that process in November 2008.
[11] Economic Growth, Regulatory Relief, and Consumer Protection Act, Pub. L. No. 115-174, § 215 (2018).

the system only if it has obtained a written, including electronic, consent from the individual who is the subject of the request. Additionally, the purpose of such a request must be for a credit transaction or for another permissible purpose as set forth in the Fair Credit Reporting Act.[12]

To use the system, a company must certify that it: (1) meets the statutory definition of a "permitted entity"; (2) is in compliance with the enabling statute; and (3) is in compliance with its privacy and data security requirements under the Gramm-Leach-Bliley Act, with respect to information the entity receives from SSA's system. The law gives SSA the authority to audit and monitor to ensure proper use by permitted entities of the system and deter fraud and misuses by permitted entities with respect to the system.

The Coalition worked closely with SSA as it developed eCBSV. We appreciate SSA's open and constructive dialogue as the agency worked to develop all aspects of the system, from the technical side of the API to the consent language and user agreement.

In 2020, SSA launched the pilot of eCBSV with 10 permitted entities. By 2021, SSA expanded enrollment to other permitted entities that initially expressed interest when the pilot was announced. In 2022, SSA opened enrollment again, permitting any entity that qualified to enroll as an eCBSV user, subject to agreeing to the user agreement. There are now 22 direct permitted entities, and several of those are service providers (e.g., credit bureaus), that are submitting verification requests on behalf of multiple financial institutions.

To be clear, SSA is not sharing its data with the users of the system. It provides a match/no match response or death indicator based on how the information provided by the permitted entity compares to SSA's data. This simple match/no match answer can stop synthetic identity fraud in its tracks. It also can help with financial inclusion. A match from eCBSV is a strong signal that the individual is who they purport to be, but are simply new to the credit system. Increasingly, eCBSV is being used to help validate thin-file consumers, which is promising for financial inclusion purposes.

[12] Fair Credit Reporting Act, 15 U.S.C. 1681b (2003).

We understand that roughly eight in 100 submissions come back as a "no match" response. Some analysis shows that of the eight that come back as a no match, three of those are fraudulent attempts and the other five are generally legitimate consumers and the mismatch was simply the result of a typo or a nickname being used.[13]

Costs of eCBSV

The law dictates that SSA's costs to build and operate the system shall be fully recovered from the users of the system. SSA establishes the amount to be paid by the users and shall periodically adjust those amounts to ensure that amounts collected are sufficient to fully offset the cost of the administration of the system.

Prior to the initial launch and as mandated by the law, SSA collected 50 percent of the start-up costs — $9.2 million.[14] The initial fee schedule ranged based on annual transaction volumes, with five tiers and annual fees ranging from $400 (for annual volume of up to 1,000) to $860,000 (for transaction volumes between 50,000,001 and up to 2 billion).[15] In November 2020, SSA stated that the total cost for developing the service is $45 million and SSA will recover the cost over a five-year period, assuming projected enrollments and transaction volumes materialize.[16]

In January 2022, SSA announced substantial changes to its eCBSV tier fee schedule. The revised tier fee schedule was based on 45 participating permitted entities in FY 2022 submitting an anticipated volume of 280 million transactions. The total cost for developing the service is $50 million through FY 2021, and SSA will recover the cost over a three-year period, assuming

[13] "The Electronic Consent Based SSN Verification Service," SentiLink, https://blog.sentilink.com/electronic-consent-based-ssn-verification-service.
[14] "Agency Information Collection Activities: Proposed Request," *Federal Register*, December 5, 2019, https://www.federalregister.gov/documents/2019/12/05/2019-26259/agency-information-collection-activities-proposed-request; "Agency Information Collection Activities: Proposed Request," *Federal Register*, March 10, 2020, https://www.federalregister.gov/documents/2020/03/10/2020-04807/agency-information-collection-activities-comment-request.
[15] *Federal Register,* December 5, 2019; *Federal Register*, March 10, 2020.
[16] "Agency Information Collection Activities: Proposed Request," *Federal Register*, November 30, 2020, https://www.federalregister.gov/documents/2020/11/30/2020-26292/agency-information-collection-activities-proposed-request.

projected enrollments and transaction volumes meet SSA's projections.[17] SSA moved from a five-tier schedule to a seven-tier schedule, with annual fees ranging from $400 (for annual volume of 1-1,000) to $7,500,000 (for annual volume over 50 million).

After that new fee schedule was announced, the Coalition expressed some concerns with SSA. We noted that the new fee schedule may inadvertently frustrate the purpose of eCBSV and interfere with SSA's goals to increase usage and participation. We also noted that the new tiers are structured in such a way that the marginal cost of a single additional transaction is significant, which will disincentivize greater use of eCBSV. We asked SSA to work closely with users on future adjustments to this schedule, particularly to incentivize greater use of eCBSV while also allowing SSA to recover its costs. We also asked for more information on the time period for recovering costs, and noted that a longer time frame may be needed to recover the costs.

Earlier this month, SSA announced another increase to the tier fee schedule. The new schedule is based on 20 participating permitted entities in FY 2023 submitting an anticipated volume of 65 million transactions. The total cost for developing and operating the service is $53 million through FY 2022. Of this amount, $38 million remains unrecovered/unreimbursed. The new subscription tier schedule is intended to recover these costs over a three-year period, assuming enrollments and transaction volumes meet these projections.[18] The new tier schedule is effective July 10, 2023. This new schedule has 10 tiers with annual fees ranging from $7,000 for annual transaction volume between 1-10,000 up to $8.25 million for annual transaction volume of 25,000,001 – 75 million.

These fee increases are significant. For example, in the first two years of the system, a user with an annual volume of 200,000 transactions paid an annual fee of $14,300. Last year that increased to $40,000, and beginning in July, for the same user, that annual fee will be $130,000. That is a nine-fold increase in fees for the same system. For a user with an annual volume of 20

[17] "Notice of Open Enrollment and Fee Increase for Our Electronic Consent Based Social Security Number Verification Service," *Federal Register*, January 14, 2022, https://www.federalregister.gov/documents/2022/01/14/2022-00638/notice-of-open-enrollment-and-fee-increase-for-our-electronic-consent-based-social-security-number.
[18] "Notice of Fee Increase for Our Electronic Consent Based Social Security Number Verification Service," *Federal Register*, May 9, 2023, https://www.federalregister.gov/documents/2023/05/09/2023-09753/notice-of-fee-increase-for-our-electronic-consent-based-social-security-number-verification-service.

million transactions, the initial annual fee was $276,500. In 2022, that increased to $1.5 million, and in July, that user's annual fee will be $6.25 million. That user will be expected to pay more than 22 times its original amount for the same service.

In developing this new tier schedule, SSA engaged in a constructive dialogue with the industry. In the new tier structure, SSA adopted two key suggestions from the industry: (1) the agency added more tiers between 1 million and 50 million transactions to incent greater use of eCBSV and (2) incenting permitted entities to submit higher volumes by discounting pricing as permitted entities use or commit to higher volumes. However, the new tier structure does not address two issues that must be resolved for the long-term success of the system: (1) the short timeframe SSA has set to recover the remaining costs of the initial system development and (2) the estimated annual operational costs. Accordingly, the industry sent a letter to SSA expressing concerns about further increasing the fee schedule. That letter is attached to my testimony.

Improving eCBSV

SSA's eCBSV is critical to preventing synthetic identity fraud. It is hard to envision a resource more suited for this task. While the ramp-up in usage of the system has taken some time, SSA is seeing steady transaction volume. That alone shows the need for this system.

The success of eCBSV is in the best interest of consumers, the financial services industry, and the government. If eCBSV is not efficient and effective, the only people who benefit are criminals. To ensure the long-term success of eCSBV, the Coalition offers the following:

First, as noted previously, the industry has serious concerns regarding the recently announced increase in the fee tier structure. To be clear, we fully understand and accept the industry's responsibility to reimburse SSA for the costs of eCBSV. That is not a point we dispute. What we do have concerns about is the short time frame in which SSA is trying to recover these costs. Total cost for developing and operating the service is $53 million through FY 2022. Of this amount, $38 million remains unreimbursed, and SSA has said it plans to recover that amount within three years. To do so, it has substantially increased the prices to use the system. If SSA continues on this path, we are very concerned that current and potential users will be deterred. We understand that SSA wants to attract new users and increase usage and participation, and we

believe these price increases will have the opposite effect. If that deterrence occurs, it will be impossible for SSA to recover the costs in the three-year timeframe. SSA has relayed to us that they are constrained due to the operations of appropriations law and the length of time they have to recover the initial build costs. We want to work with SSA and Congress on possible solutions, such as extending the recovery time period to 10 years.

Second, existing SSA policy makes it very difficult to determine the impact of the system on combatting fraud. A permitted entity receives only a binary match/no match response, with no indication of which data field caused the mismatch. The lack of insight restricts financial institutions from determining whether it was a potential entry error, such as a misspelled name or abbreviated first name, or an actual synthetic identity. We ask SSA to explore ways to share additional information about the reasons for mismatches, so that users can better understand the root cause of a mismatch. This may be in enhancements to or more transparency into SSA's "fuzzy logic." Such insights would significantly improve the usefulness of the system and allow calculations regarding its value in combatting fraud.

Finally, we believe it is worth exploring other ways eCBSV can be used. The system was established to assist financial institutions and their service providers with credit decisions. However, it may be possible for this system to be used by other entities with legitimate purposes, such as landlords for tenant screenings or employers for hiring purposes. SSA has used a substantial amount of resources to build this system, and it is worth exploring what other entities, both government and private, could use this system.

Thank you for holding this hearing today and for the opportunity to testify on synthetic identity fraud. SSA and eCBSV are critical to combat synthetic identity fraud. The Consumer First Coalition stands ready to work with SSA and Congress to extend the time frame to recover costs and enhance the effectiveness of the system. We want eCBSV to be an effective tool to thwarting synthetic identity fraud and protecting some of the most vulnerable consumers. If eCBSV fails, the only winners are the criminals.

March 1, 2023

Acting Commissioner Kilolo Kijakazi
Social Security Administration
6401 Security Boulevard
Baltimore, MD 21235

Re: eCBSV Tier Fee Schedule

Dear Acting Commissioner Kijakazi:

The undersigned associations have appreciated the opportunity to partner with the Social Security Administration ("SSA") to make the SSA's electronic Consent Based Social Security Number Verification ("eCBSV") Service as effective and efficient as possible. We, along with our members, have worked closely with SSA in developing and implementing the system mandated by Section 215 of the Economic Growth, Regulatory Relief, and Consumer Protection Act of 2018 (the "Banking Bill").

It is our understanding that SSA is considering changes to the eCBSV tier fee schedule, including significantly increasing the fees for many users. We urge you **not** to move forward with these changes to the tier fee schedule. We are very concerned that these potential increases will force some current users to withdraw from participation in the eCBSV program and deter potential new users from enrolling. At a time when SSA is hoping to attract new users and increase usage and participation, these changes would move the program in the opposite direction. If prices continue to increase, we have grave concerns on the viability of eCBSV in the long term.

We recognize that SSA must recover the costs associated with eCBSV, and we stand ready to work with SSA and other policymakers, including Congress and OMB, on the best approach to do so. However, we believe it is not feasible for SSA to fully recover the development costs by FY 2025. It is our understanding that as of August 2022, SSA has only recovered $12.4 million of the total development costs of roughly $50 million, resulting in $39 million in unreimbursed costs. We recognize that SSA may have constraints on the timing of recovering these costs, and we commit to working with policymakers to ease these constraints to the extent possible. Additionally, we ask SSA to reevaluate the annual operating costs of the system, as we are concerned that is not sustainable.

One underlying issue that seems to be contributing to the high number of unreimbursed costs is the original transaction and usage estimates used by SSA in building the system varied significantly from those estimates provided by industry and have continued to shift significantly year after year. In 2019, the industry relayed to SSA that a reasonable estimate based on industry surveys and Federal Reserve data would be to expect 300-400 million inquiries each year with an upper bound of 500 million, but noted that if permitted entities could reuse results (which they effectively can – by noting in their internal systems that data associated with an identity on file had matched data at SSA) that the volume would be much lower. SSA, however, moved forward with building a system that could support over 1 billion annual inquiries – or more than double the high-end of what industry suggested would be the likely volume if there was no way to reuse results.

In December 2019, SSA based its cost estimates for the eCBSV pilot phase on **10 participating entities** in FY 2020 submitting an anticipated volume of **307,000,000 transactions**; actual transactions in FY 2020 were much lower. Despite that lower number, in November 2020, SSA based cost estimates on **123 participating entities** in FY 2021 submitting an anticipated volume of **1,100,000,000 transactions**; again, actual numbers were much lower. In January 2022, SSA based its revised tier structure on **45 participating entities** in FY 2022 submitting an anticipated volume of **280,000,000 transactions**. At that time, SSA also stated that it anticipated recovering the development costs over a three-year period, assuming projected enrollments and transaction volumes meet SSA's projections.

We flag this history to note that SSA's projected transaction volume substantially diverged from the estimates that the industry provided in 2019, with the result being that the program incurred much greater costs in the eCBSV development than was necessary to address industry demand for the eCBSV system. As SSA moves to recover those dollars, it is important that the economics of the program also incent industry to use eCBSV. As noted earlier, we are concerned that another round of material price increases will instead force some current users to withdraw from participation in the eCBSV program and deter potential new users from enrolling – which will, in turn, make it much harder for SSA to recover the funds currently expended.

Additionally, existing SSA policy makes it very difficult to determine the impact of the program on combatting fraud. The average mismatch rate that SSA reports for submitted queries generally hovers around 8%. Unfortunately, a permitted entity only receives a binary match / no match response with no indication which data field caused the mismatch, whether it was name, date of birth, or wrong SSN. This lack of insight restricts financial institutions from determining whether it was a potential entry error such as a misspelled name, abbreviated first name e.g. Katy for Katherine, or an actual synthetic identity. We would ask SSA to reconsider this decision and explore ways that additional information could be shared about the reasons for mismatches to allow financial institutions to better understand the root cause of mismatch, which would significantly improve the usefulness of the system and allow calculations regarding its value in combatting fraud.

We want to continue to work with SSA to make eCBSV an effective tool in preventing synthetic identity fraud. We ask SSA to not move forward with the proposed increases to the tier fee schedule and work with the industry on developing a sustainable path forward.

We appreciate your attention to the issues we have raised. If you would like to discuss these issues, please contact Paul Benda, American Bankers Association, pbenda@aba.com, Jeremy Grant, Better Identity Coalition, jeremy.grant@venable.com, and Katie Wechsler, Consumer First Coalition, kwechsler@snwlawfirm.com.

Sincerely,

American Bankers Association Better Identity Coalition Consumer First Coalition