The Electronic Consent Based SSN Verification Service

How eCBSV can help your financial institution fight fraud and approve more applications faster.

SentiLink

July 2022

Introduction

Technology continues to re-shape how consumers seek out and utilize financial services. As this innovation takes hold, it has presented one undeniable truth: For financial institutions making the move to digital, the risk of identity fraud increases.

To help address these new challenges and reduce risk, financial institutions have increasingly focused on data "sources of truth" to authoritatively answer whether a key piece of identity information is valid or not. Frequently, these sources are government entities: The Social Security Administration (SSA) for SSNs, the IRS for income and other tax transcript data, and state departments of motor vehicles for drivers license data are some examples.

In 2018, the SSA began development of a real-time, API-based system to allow the financial industry to verify a name, date of birth (DOB) and SSN combination. Now operational, it is known as the Electronic Consent Based SSN Verification service, or eCBSV. As the source of truth for which SSNs have been assigned to a given name and DOB, this system makes it possible for SentiLink partners to onboard more good customers more efficiently, while reducing fraud and risk.

SentiLink was selected out of 123 applicants to be part of SSA's initial pilot program with eCBSV. In fact, SentiLink was the first company in the history of the system to go live and initiate the first ever SSN verification request. No other company has more practical, technical and tactical experience working with SSA and partner financial institutions to successfully integrate this important service.

Increase incremental approvals of good customers.

As the authoritative source of SSN data, eCBSV can provide more insights on real people who may have less credit history, like young people, immigrants, or those new to credit.

Confirm suspected synthetic identities and reduce fraud.

eCBSV is the best treatment strategy for applicant identities that raise red flags as likely synthetic. As a step-up strategy, it allows confirmation that a suspected synthetic identity isn't a real person and makes it possible for someone inadvertently flagged to prove they're real.

Automate manual review and speed up origination.

Eliminate the need for ink signatures on paper-based SSA-89 forms. eCBSV allows the use of electronic signatures for capturing consumer consent, removing the need for paper SSA-89 forms.

eCBSV: Determining Eligibility and Ensuring Compliance

Today, eCBSV is fully operational and scaled to handle all anticipated volume, which was estimated by industry groups very early in SSA's planning process to be upwards of 350,000,000 verification requests per year.[1]

At its current pace, it will be a long time before the system reaches that level of volume, if it does at all. As of this writing, there are about two dozen entities directly enrolled with SSA, nearly 500 entities enrolled indirectly (i.e., through a service provider like SentiLink), but less than 100 actively using the system and sending requests.

Can You Use It? Two Key Issues to Determine Eligibility

As of April 2022, SSA has expanded the opportunity to enroll in eCBSV to all eligible entities. It is worth noting that the Banking Bill limits eligible participants to either "Financial Institutions" or a "service provider, subsidiary, affiliate, agent, subcontractor, or assignee of a financial institution." Collectively, companies that meet either of these definitions are considered "Permitted Entities."[2]

What is a "Financial Institution" in the Context of eCBSV?

At first glance, the term "Financial Institution" appears limiting and may discourage some — such as non-depository fintechs — from exploring eCBSV. However, in reality it is not as restrictive as many expect.

For those exploring eligibility for eCBSV, the important concept to note is that the definition of "Financial Institution" is not based on the type of institution and whether it is a regulated depository institution (i.e., a bank or credit union).

→ Instead, it is based on what activities the entity engages in, and whether those activities are, generally, financial in nature, incidental to such financial activity, or even complementary to a financial activity.

Through regulation, the Federal Reserve Board has interpreted this broadly.[3] As such, it follows that many non-depository financial institutions from across the financial services industry have enrolled as "Financial Institutions" for purposes of eCBSV.

[1] Some industry participants even provided SSA estimates of 1-2 billion annual verification requests. For a period of time, SSA relied on this in determining system requirements and projected development costs.
[2] See "eCBSV User Agreement," section 1.B., accessed at: https://www.ssa.gov/dataexchange/eCBSV/documents/eCBSV%20User%20Agreement%20FINAL.pdf
[3] See Appendix, Section 2.

Do You Have a "Permissible Purpose" to Use eCBSV?

Even if a company determines it meets the definition of "Financial Institution," to access eCBSV it must have a legally valid reason -- a "Permissible Purpose" as defined in the federal Fair Credit Reporting Act (FCRA). These purposes are most often associated with the specific scenarios under which it is legally permissible to obtain a consumer's credit report. The law that called for the creation of eCBSV, commonly known as "the Banking Bill," however, relies on those same reasons to regulate the circumstances in which eCBSV can be accessed.

Generally, these reasons are associated with activities initiated by a consumer related to the extension of credit but cover other interactions as well, including the broad category of a "legitimate business need" that is in connection with "a business transaction that is initiated by the consumer."[4] Recent court cases[5] have provided clarity on certain types of activities that meet this ambiguous legislative threshold.

The specific purpose for which a Financial Institution is requesting an eCBSV verification must be recorded for audit purposes for every verification request.

SSA allows that it can be explicitly stated in the consent language presented to a consumer, or that the consent language can simply refer to "this transaction," so long as an auditable log is maintained.

An FCRA compliance-focused assessment of relevant use cases for any company considering incorporating eCBSV is a critical step to address prior to enrolling. The static SSA-89 form[6], which as an electronically fillable PDF remains a valid means of obtaining consent for eCBSV, can serve as a useful guidepost for firms determining the best approach to addressing the "Permissible Purpose" question. For example, purposes listed on this form as reasons for authorizing consent include activities like applying for a mortgage, loan or credit card, as well as simply opening a bank account.

[4] 15 U.S.C. 1681b.
[5] See, for example: Domante v. Dish Networks, LLC. Accessed at https://casetext.com/case/domante-v-dish-networks-llc
[6] See: https://www.ssa.gov/forms/ssa-89.pdf
[7] See: SSA, eCBSV FAQ. https://www.ssa.gov/dataexchange/eCBSV/faqs.html?tl=18%2C19

Understanding Consumer Consent Requirements

As previously described, consumer consent is an essential prerequisite for use of eCBSV: A financial institution cannot request an eCBSV verification without explicitly asking the consumer and getting their approval to do so first. Consent can be captured in one of three ways:

- On a paper SSA-89 form with a "wet" consumer signature
- On an electronically fillable PDF version of that form
- Integrated electronically into a financial institution's existing business processes

For the third scenario, SSA prescribes very specific requirements for the format, appearance and retention (five years) of a consumer's consent. For example, SSA provides users the exact language that must be used and rules dictating how it must be formatted and makes clear that their language and any "I consent" or similar checkbox cannot simply be merged into existing terms and conditions: Intent to sign must be clear and explicit that the consumer is providing consent for eCBSV.

Generally, there are two viable approaches to surfacing the SSA consent language to applicants: Organizations can either include the SSA consent language and associated "I Consent" as an addition to their onboarding application form, or as a separate screen altogether, depending on how they would like to manage applicants' interaction.

The introduction of any friction into a digital onboarding process creates a degree of abandonment risk and is a factor worth considering. That said, SentiLink's partners have not reported any significant impact of the SSA's consent requirements on abandonment rates.

Example of Required Consent Language:

Authorization for the Social Security Administration to Disclose Your Social Security Number Verification

☐ I authorize the Social Security Administration (SSA) to verify and disclose to [Name of Financial Institution] through SentiLink Verification Services Corp., their service provider, for the purpose of this transaction whether the name, Social Security Number (SSN) and date of birth I have submitted matches information in SSA records. My consent is for a one-time validation within the next [number of days].

I agree. By [clicking/checking here], you are signing the consent for SSA to disclose your SSN Verification to [name of Financial Institution] and SentiLink Verification Services Corp. You agree that your electronic signature has the same legal meaning, validity, and effect as your handwritten signature.

Primary Use Cases

eCBSV and Synthetic Identities

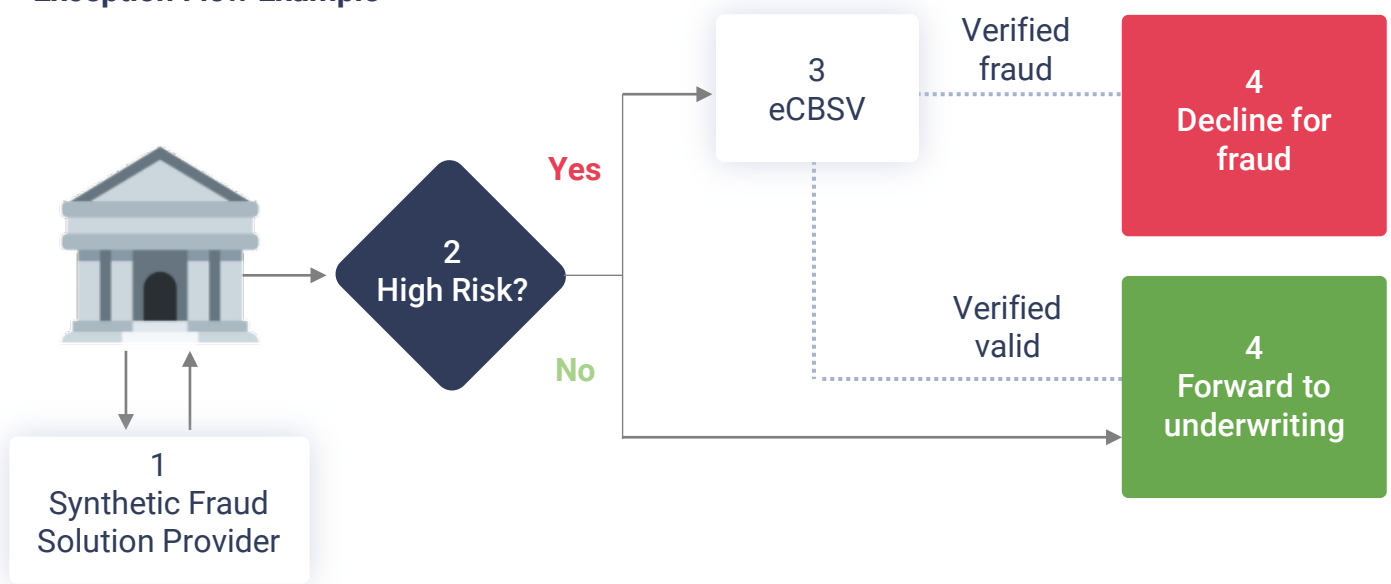
Reducing synthetic identity fraud was a primary motivation when Congress enacted the Banking Bill.[8] Today, it remains the fastest growing type of financial crime in the U.S., often goes undetected and costs the financial industry several billion dollars each year in losses.

Technically, there are two types of synthetic fraud: One where someone manipulates their identity, and another where an identity is totally fabricated. In its simplest form, a synthetic identity is one where the name, date of birth and SSN don't correspond to any real person. That synthetic identity can then be used to apply for credit, just as any other person would.

To help address both and reduce losses, incorporating eCBSV is a critical step. A key consideration is where in the application funnel eCBSV should be placed. One option is to utilize eCBSV at the top of the funnel for all applications as a first pass.

A second option is a lower funnel placement, utilizing eCBSV as an exception flow. Institutions with fraud detection services at account opening are using eCBSV to quickly and accurately confirm whether applications flagged as high risk are either fraudulent or actually clear.

Exception Flow Example



[8] See: https://www.scott.senate.gov/media-center/press-releases/scott-leads-bipartisan-effort-to-curb_childrens-identity-theft

Match Rates and Funnel Placement

What strategy an institution opts to use will impact its observed match rates from eCBSV. At the start of 2021, SentiLink observed an eCBSV positive match rate at 95%. By the end of the year, we observed a match rate of 93.3%. According to SSA, as of May 2022, the overall system match rate is 92.8% and dropping slightly each month.

As our partners' experience with the system has matured, in many cases so has their utilization strategies. As described above, some continue to send most, if not all, applicants through eCBSV at the top of the application funnel. Realistically, these partners are likely experiencing similar trends we have observed over time or in line with SSA's reported data. When a financial institution changes from sending all applications through eCBSV to only sending select high-risk ones, their mismatch rates
will logically increase.

Achieve Greater Efficiency and Speed

If an institution already requires SSA-89 forms as part of the onboarding or application process (e.g., mortgages, licensing requirements), eCBSV allows for faster completion, submission, and processing by nature of migrating the process online.

eCBSV can also be added to existing KYC processes as another verification layer. It should not, however, be the only KYC check an organization performs on its customers. Our experience with eCBSV indicates the majority of mismatches (2/3rds, in fact) are not due to fraud, but are instead the result of input typos, unreported name changes, use of a nickname, and other inconsistencies that, though harmless, could lead to low double-digit mismatch rates for certain products.

Mortgage Highlight: An Expanding Use Case

No segment of the financial industry has more experience working with SSA — through its legacy paper-based CBSV system —than the mortgage industry. Historically, the "wet signature" requirement on an SSA-89 form to access CBSV was of no real consequence to a customer experience already rooted in large volumes of paperwork and long time horizons. More recently, as the transition to digital has touched homebuyers, mortgage providers have placed increased importance on the value of finding ways to speed up the application process and reduce costs.

Seconds vs. Days: Using eCBSV to Speed Up the Application Process

Integrating eCBSV's consent requirements into a digital mortgage application process is achievable in one of two ways: Either by serving the applicant with an electronically fillable PDF of the SSA-89 form or by presenting the SSA-approved electronic disclosure (shown previously).[9] When processing SSA-89 forms digitally, mortgage lenders using SentiLink as an eCBSV service provider are averaging response times of less than 300 milliseconds. This includes the roundtrip time from when they submit an identity to SentiLink for verification until they get an answer from the SSA. Manually processing paper-based SSA-89 forms can take days, including the time to get an ink signature from customers and get a response from the SSA. Additionally, if the paper-based validation fails, an institution may be compelled to try again, further delaying the underwriting and credit evaluation process.

[9] Note that Fannie Mae and Freddie Mac have differing requirements for verifying SSNs.

Approve More Thin Files

eCBSV can be used to quickly and easily obtain more signal on a subset of applications that existing KYC processes have flagged as risky, in lieu of asking for additional history or information to verify an identity. This can decrease onboarding or signup friction while providing similar rigor.

Consumer Lending and Incremental Approvals

For financial institutions focused on lending to populations new to credit (e.g., students, new to the U.S.), eCBSV has proven to create significant lift. Consider the experience of a mid-sized financial institution using eCBSV. In the past 12 months, 14% of the applications designated a “match” by eCBSV didn’t have a credit report. Without eCBSV these consumers may have immediately been turned down for credit given an inability to verify their identity. At a minimum, they would have been required to go through additional steps to verify their identity such as providing a government issued ID, taking a selfie or being interviewed by phone. With eCBSV, that step-up, manual verification path is eliminated, creating an opportunity for the bank to efficiently approve 14% more applications while also providing a lower friction onboarding experience for these consumers.

SentiLink Case Studies

A partner financial institution was presented with an identity on an application that appeared extremely new. On closer inspection, the individual was shown to have a lengthy history with an ITIN, but it was theorized may have been applying with a newly issued random SSN, which could not be verified by traditional means. Here, a bottom-of-funnel request to eCBSV provided the conclusive evidence that this was a legitimate applicant, and the partner was able to establish an account with the consumer.

A partner escalated a case to our risk operations team involving a thin-file applicant with a randomly issued SSN. However, with only scant "signs of life" found online indicating the applicant might be an international student, it was not possible to make a determination if the SSN was legit, stolen, or completely fabricated. Again, eCBSV provided a "Yes" match, resulting in a lower friction onboarding process for the applicant and peace of mind for the partner.

Even at this relatively early stage of experience with eCBSV, it's clear the system is benefitting the underserved/unbanked, helping financial institutions reach more eligible borrowers.

Understanding eCBSV's Limitations

While eCBSV is unquestionably an important treatment strategy to help combat synthetic identity fraud, it is by no means a panacea and should be considered as one valuable asset in a Chief Risk Officer's toolkit.

As mentioned at the outset of this paper, SSA is the "source of truth" for SSNs. But even sources of truth like a federal agency are not infallible and are prone to similar data quality issues and technical limitations as can impact any other database.[10] Additionally, while the SSA is the source of truth for which SSNs they have issued, there is nothing preventing them from issuing SSNs to identities that don't exist due to fraudulently filed SS-5 forms.

Targeted Products/Segments

The products offered and segments targeted will influence your eCBSV experience. FIs with more exposure to immigrant demographics may experience a lower match rate due to complications with naming conventions and date formats. Including this factor in your eCBSV implementation plan will help you appropriately plan and staff for eCBSV.

Fuzzy Logic

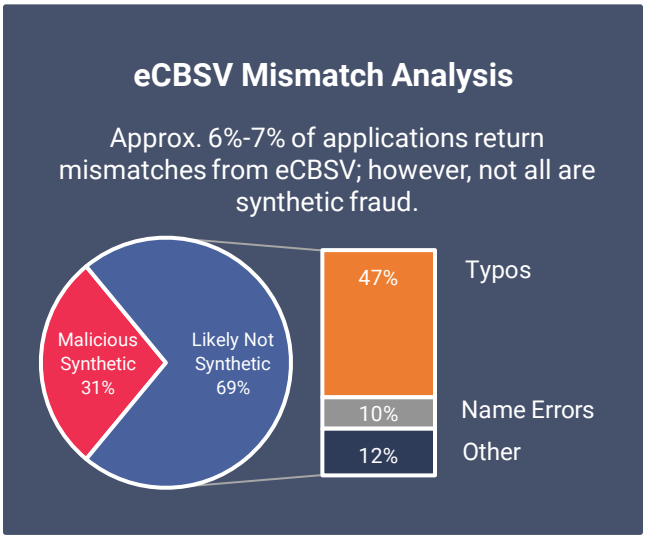
Fuzzy logic applied in information retrieval systems is not a new concept and is a readily available technology that can greatly enhance the value of a database. However, by all accounts, the use of fuzzy matching logic in eCBSV is limited. SSA has been very guarded in terms of sharing insights into what fuzzy logic it employs, but what we do know can be summarized as follows:

- SSA does incorporate fuzzy matching in the event an eCBSV submission includes the maiden name of a spouse. That is, if a maiden name is provided on an application even though a married name change has taken place, eCBSV should provide a "Yes" response.

- Similarly, if a person has had their SSN reissued or has legitimately corrected some other aspect of their name or DOB with SSA, eCBSV will return a "Yes" match for the old and new/corrected information. For example, if a person who has had their SSN reissued provides their name, DOB and original SSN on a financial application, eCBSV will return a "Yes" for that combination.

[10] See Appendix, Section 3.

- As discussed previously, we've observed a match rate of approximately 93.3%. Of the 6.7% that were returned as a "No" match/mismatch, **we identified 31% as malicious fraud attempts (compared to 25% at the start of 2021).** That means 69% of mismatches aren't fraud due to things like "fat-finger" typos, and that it's possible 4.6% of consumer applications could be rejected due to a typo in their name, DOB or SSN. Again, given the near binary limits of SSA's matching logic, this nuance is important to keep in mind for financial institutions looking to approve more applicants.



System Performance

Latency has always been a concern for eCBSV participants. SSA continues to experience the occasional unplanned disruption or outage, and SSA technical support remains a source of frustration. That said, at the end of 2021, eCBSV was averaging a response time of 280ms (compared to 345ms earlier in the year). This comes even as volume is beginning to increase, a sign that the infrastructure SSA built to support eCBSV at scale is likely up to the task.

Amount of Data Validation Prior to eCBSV

Data validation prior to eCBSV will naturally improve match rates. Is the date of birth and SSN valid? Is the SSN a 9-digit number, and is it truly an SSN or is it an ITIN (which starts with the number 9)? Simple data validation checks prior to eCBSV can significantly increase match rates and improve overall approval rates and conversion.

Conclusion

Financial institutions across the industry are increasingly shifting to digital-first or digital-only applications for products and services. While this change makes it possible to reach new markets and consumers outside of any physical footprint, it increases the chances for fraud to occur at onboarding, particularly identity-related fraud such as identity theft and synthetic identity fraud.

Integrating eCBSV offers many potential benefits for financial institutions. Insights gained from tapping into the "source of truth" for name/DOB/SSN combinations will reduce fraud, increase approvals of legitimate consumers, and can speed up digital underwriting processes. SentiLink works with partners to ensure an implementation strategy meets their technical requirements and risk considerations and adheres to all the detailed compliance requirements set forth by the SSA.

Appendix

SECTION 1: Origin Story: How "e" Met "CBSV"

Over the last decade, synthetic identity fraud has become a significant and costly challenge for financial service providers. This type of identity fraud involves the use of a fictitious combination of name, date of birth and SSN to apply for financial products with the intent of defrauding financial institutions, government entities or individuals.[11]

Unlike with a case of identity theft, where the name/DOB/SSN combination is likely to belong to an actual person, a synthetic identity can be created using a combination of real and fake credentials, including SSNs.

The U.S. Congress recognized the important role the SSA, as a source of truth, could play in helping combat synthetic identity fraud. After all, the SSA is responsible for the assigning of SSNs (a process called enumeration), issuing Social Security cards, as well as any later replacements of cards or re-issuance of SSNs in certain cases. Thus, in 2018 a law was passed directing the SSA to develop a system through which financial services companies can, after obtaining written or electronic consent from a consumer, transmit to SSA via an API a name, DOB and SSN and request that SSA verify whether the given combination matches with what they have on file. The system is called the Electronic Consent Based SSN Verification service, or eCBSV.

A Brief History

The eCBSV is an important evolution of a long-lived, antiquated system. Since 2002, the SSA has played a role in assisting companies that provide identity verification services — and the financial industry more broadly — with iterations of a fee-for-service system permitting verification of an SSN against the Agency's records. The system has been known by several names: The "SSN Verification Pilot for Private Businesses," the "Interim Verification Process" and, starting in 2008, the "Consent Based SSN Verification" service (CBSV).[12]

Each of these iterations shared a common heritage rooted in paper: Specifically, the CBSV and its predecessors all required that companies would first obtain a physical "wet signature" consent by a consumer prior to requesting a verification. Over time, and due to the paper-based nature of this system, the CBSV was utilized almost exclusively by the mortgage industry. The system averaged about 3,000,000 verification requests per year.

In 2016, new types of identity fraud — including synthetic identity fraud — were growing in significance. Some in the financial industry — credit card issuers in particular — recognized the potential benefit of replacing the "wet signature" requirement with an equivalent and legally valid electronic signature, which would make the CBSV available in applications where paper is not involved.

[11] https://blog.sentilink.com/sentilink-white-paper-defining-synthetic-fraud
[12] See: "Social Security Administration, Office of the Inspector General, Consent Based SSN Verification Program Audit Report," July 2009.

While SSA was unwilling to do this on its own, Congress was quick to recognize the benefits of such a change and enacted in May of 2018 the bipartisan "Protecting Children From Identity Theft Act" as part of a broader measure commonly referred to as "the Banking Bill." This legislation gave SSA the mandate to create a system to allow the financial industry to verify in real-time the name, DOB and SSN of a consumer, with the consumer's electronic consent.

SECTION 2: Defining "Financial Institution“

Section 215 of the Economic Growth, Regulatory Relief, and Consumer Protection Act (“the Banking Bill”) directs SSA to modify or develop a database for accepting and comparing fraud protection data provided electronically by a “Permitted Entity.” [13] The database compares fraud protection data submitted against such information maintained by SSA in order to confirm (or not confirm) the validity of the information submitted and provides a response in real-time machine-to-machine format. The information submitted by a Permitted Entity must be pursuant to a written, including electronic, consent by the individual consumer, and must be in connection with a credit transaction or any circumstance described in section 604 of the Fair Credit Reporting Act.[14]

A “Permitted Entity” is a “Financial Institution” or a service provider, subsidiary, affiliate, agent, subcontractor, or assignee of a Financial Institution. The term “Financial Institution”[15] is tied to two laws — the Gramm Leach Bliley Act (“GLBA”) and the Bank Holding Company Act (“BHCA”). Specifically, in the Banking bill, “Financial Institution” has the meaning given the term in section 509 of the GLBA.[16] GLBA defines a Financial Institution as “any institution the business of which is engaging in financial activities as described in section 143(k) of title 12” (also known as Section 4(k) of the BHCA (“Section 4(k)”).[17]

Section 4(k) establishes that certain activities are financial in nature, including lending or transferring money, insuring against loss, providing financial advisory services, and engaging in any activity that the Federal Reserve Board (“Board”) has determined, by order or regulation that is in effect on November 12, 1999, to be so closely related to banking as to be a proper incident thereto, subject to the same terms and conditions in such order or regulation, unless modified by the Board.[18] Section 4(k) also authorizes the Board to make a determination of whether an activity is financial in nature or incidental to a financial activity.[19] The Board’s regulations implementing Section 4(k) list activities that are financial in nature or incidental to a financial activity.[20] This list includes those activities that the Board determined by an order that was in effect on November 12, 1999, to be so closely related to banking as to be a proper incident thereto (and therefore financial in nature).

[13] 42 U.S.C. § 405b.
[14] 15 U.S.C. § 1681b.
[15] 42 U.S.C. § 405b(b)(4).
[16] 42 U.S.C. § 405b(b)(2).
[17] 15 U.S.C. § 6809(3)(A).
[18] 12 U.S.C. § 1843(k)(4).
[19] 12 U.S.C. § 1843(k)(2).
[20] 12 C.F.R. § 225.86.

SECTION 3: Understanding the Numident

The data underlying eCBSV derives from a system called the Numident. This is the database system of record for SSA enumeration data, containing the unique, life-long SSN assigned to an individual based on applications for Social Security cards, as well as the reported change history the consumer's identity goes through during the life of their SSN, such as a name change resulting from marriage or divorce.

The Inspector General of SSA is tasked with reporting on the accuracy of the Numident. Based on our analysis of the most recent data, SentiLink determined that the organic error rate of the Numident is anywhere between 0.05–2.13%. This broad range is dictated by the relatively wide range of error rates between the three possible methods of enumeration: Visiting an SSA field office, enumeration at birth, and enumeration at entry. For eCBSV participants, we expect this to result in 1 out of every 200 eCBSV requests that will generate a false mismatch stemming from a Numident error. That is, a real applicant will be told that their record cannot be found in the Numident because of a Numident specific error, leading to potential consumer frustration and lower customer conversion.