US DIGITAL RESPONSE

Identity Proofing Vendor Comparison

Commercial solutions to automate identity proofing

December 4, 2020

Prepared by:
Unemployment Insurance Modernization Team
U.S. Digital Response

Table of Contents

Who We Are

U.S. Digital Response provides support for crisis response

Founded by former U.S. Deputy CTOs and seasoned tech industry veterans who led federal open data policies and digital government strategy, U.S. Digital Response (USDR) connects experienced, pro-bono technologists with local government and non-profit organizations responding to crisis, to quickly deliver critical services and infrastructure that support the needs of the public.

We are non-partisan, fast and free. We operate with humility and deep respect for our partners and believe that modern and resilient technology applied in the public interest can deliver people-centered services at the speed of need.

Our diverse volunteers work with your team to understand your needs, and get you the tools you need to deliver critical services to the people who need them — all within a few days to weeks. These volunteers have deep expertise, spanning engineering, data science, content strategy, design, logistics and supply chain, and disaster response.

We provide rapid staffing to governments of all sizes, from small cities to large states, in areas ranging from public health to economic recovery, and much in between.

If you are unsure of how to address a challenge, USDR can help to assess the problem first, before you invest in costly solutions.

Introduction

Most existing fraud detection in unemployment insurance (UI) systems has been aimed at identifying the claimants who are trying to claim more in benefits than they are owed, e.g., by misrepresenting their wages. Detection relied on cross-referencing the claimant-supplied information with data from their former employer(s) with government databases like departments of motor vehicles or the Social Security Administration. If any discrepancies are found, manual intervention is required.

These existing detection practices are insufficient in the face of the kind of fraud that has skyrocketed since the passage and implementation of the CARES Act in Spring 2020: identity theft.

Criminals are using stolen identities (Name, DOB, SSN, and sometimes Driver's License ID) and using that to apply for unemployment insurance before the "rightful claimant" (i.e., the real-world person attached to the applicant's identity) can. In this case, the identity attached to the claim is a real identity — but it is not the same as the identity of the person applying and, down the line, receiving the benefits (i.e., the applicant is a "fraudulent claimant").

Given the changing threat model of UI fraud, quickly delivering benefits to rightful claimants with less manual intervention requires updating systems to automatically do the following:

1. Scan the backlog for applications that clearly are or are not fraudulent; and
2. Confirm that a new applicant is presenting an identity that is unique, valid, and entitled to benefits, and is themself the rightful claimant.
3. Confirm that the person with an existing claim who changes personal information (e.g., bank account numbers) is the same person as the rightful claimant

USDR has researched companies that provide automated identity proofing services to help in these scenarios and taken the first pass at evaluating their solutions, government compatibility, and credibility. Below is a comparison of such vendors; this list is not comprehensive, but it includes the major players and some promising start-ups.

When it comes to identity proofing for workforce agencies, solutions may need to be integrated together to make a comprehensive plan. Other services may be needed for a specific use case. If you need help or advice evaluating or implementing any of these solutions, please contact USDR.

What is Identity Proofing?

Why You Need It

A well-integrated identity proofing solution can help reduce workload and increase claim handling rates by shifting repetitive tasks from employees to automated software or outsourcing manual work from employees to vetted vendors. This can happen when the identity proofing solution is automated in a few key ways:

- Identifying and correcting for errors, e.g., due to typographical errors in applications by either the claimant or employer
- Identifying one-off fraud by individual applicants, e.g., intentionally duplicate claims
- Identifying widespread fraud by criminal organizations, e.g., use of synthetic and/or stolen identities to claim benefits

Unemployment claims are susceptible to a few kinds of errors and fraud, some of which identity proofing can prevent or catch. Finding the right solution can be a balancing act, because you want to find fraudsters while maintaining an efficient and fair process for legitimate claims. If you tip too far one way, you may not be able to catch the fraudulent actors; if you tip too far the other way, you may incorrectly target legitimate claims, resulting in delays and hardship for claimants.

Unemployment insurance systems already have automated identity proofing solutions! They are used to cross-reference and verify the information given by an applicant and their former employer(s) with government databases like those from Departments of Motor Vehicles or the Social Security Administration.

However, more extensively automated identity proofing can help when someone's identity is not resolved by the existing system, and can also go a step beyond by finding synthetic identity fraud. For the former, these applications are queued for manual review and additional document collection. In the worst-case scenario, this requires an applicant to mail or fax a copy of the required documents; in the best-case scenario, an applicant can upload the documents to the benefits website. An identity proofing system that automatically handles errors and uncertainties will prevent applicants from winding up in your backlog.

In the long term, issues that could be resolved by identity proofing should make up a much smaller proportion of the backlog, but for now, unemployment insurance agencies could find

relief by working with an identity proofing vendor that can validate identity documentation without employee intervention.

Process of Identity Proofing

This section has been adapted from NIST Special Publication 800-63-3 and combined with additional research.

"Identity proofing" is the official term for what is colloquially referred to as identity verification; identity verification is technically just a step within a larger identity proofing process. Both are umbrella terms that encompass a range of techniques to collect and **resolve** data to a particular person, **validate** that the provided data is legitimate and accurate for that person, and/or **verify** that the data is truly the user. At all stages, identity proofing checks the consistency of the data as it relates to a unique person, with varying levels of certainty.

Identity proofing in its most technical sense is defined by NIST, which additionally provides an Identity Assurance Level framework and certification. The IAL requirements indicate a particular level of certainty about an identity's validity; the techniques typically associated with each stage of identity proofing are discussed in more detail below.

Identity Resolution

To start with, identity proofing requires that the "self-asserted," personally identifiable information (PII) provided by the user confirms that it belongs to a single, real person. It resolves this data by comparing it to public databases (e.g., checking the address provided by the user against a voter registration file).

A step-up in certainty would be to use **knowledge-based verification** (aka "KBV," aka "Knowledge-based authentication") to confirm the resolved identity by asking a question based on information others are unlikely to have (e.g., the system asks the user to provide the amount of their last utility bill). Depending on the specific KBV used, this technique can be a good opportunity to identify those using stolen identities.

Beyond that, more in-depth resolution techniques do not contribute toward an IAL2 designation, but they can be an important part of a solution for detecting fraud via the use of stolen or manufactured identities.

The more sophisticated forms of identity resolution are referred to as **synthetic identity detection**. With synthetic identity detection, machine learning (aka "artificial intelligence") is

used to combine the self-asserted data with other information you may have about a user (e.g., IP address, phone's IMEI) and compare it with additional databases (e.g., telco records, credit header files, utility bills). It is through synthetic identity detection that criminals using stolen identities are typically found.

Some synthetic identity detection systems go even further and perform "network level" detection, e.g.:

- How old is the domain name of the email address provided?
- How many applications have there been from this IP address?
- Have accounts on other sites been created with this combination of name + phone?

Note: a Social Security Number can be "resolved" to a person through synthetic identity detection, but it is not considered "validated" with any certainty until the Social Security Administration weighs in.

Identity Validation

Identity validation is the first stage in NIST's process of confirming that the claimant is the same person as the owner of the user account by evaluating "identity evidence." With enough pieces of evidence, you can say with some certainty that a person is who they say they are. To achieve IAL2 designation, a system needs to collect between 1–3 documents and validate them with the issuing source.

Document verification is a system where a user uploads a photograph of an official document (e.g., a driver's licence), and the validity of the document is verified through another system. If the document is verified through a system created by the vendor (e.g., that checks for accurate layout and font use, reasonable issuance dates, etc.), it is considered by NIST to be only "weak" evidence and thus does not contribute toward identity validation in the literal sense. That said, it can still be a useful feature of your system to have.

Only by checking with the department of motor vehicles that issued the driver's license can it achieve an evidence strength high enough for use in identity validation at IAL2 standards.

Note: while a tax form could be used in document verification, using that same form to determine program eligibility is not a part of identity proofing.

Identity Verification

Identity verification represents the highest degree of certainty that the user is who they say they are by establishing a physical connection between the applicant and the PII or evidence provided.

Common digital methods of true identity verification are:

- **Biometric verification** is, e.g., where a person takes a selfie that is compared to their photo on an official document.
- **Enrollment codes** or **two-factor auth (2FA)** is a way to verify that provided contact information is accurate by sending a code to a postal address, email address, and/or phone number (voice or SMS), and requiring that the enrollment code be provided to complete registration or login in the future.
- **Knowledge-based verification** can be a component of identity verification by referring to data only available in authoritative and private sources.

Recommended Process for UI Identity Proofing

IAL2 is the level of NIST certification that is generally appropriate for unemployment insurance agencies, but that designation may not be necessary for building a strong identity proofing system that addresses the needs of unemployment insurance agencies.

Synthetic identity detection's use of data points like IP address, email address, and phone number make it substantially more reliable than one might expect. Given the nature of the fraud that UI agencies face, it is often sufficient to have a robust "identity resolution" system that's premised on synthetic identity detection. Under these circumstances, identity validation or verification are only necessary when an identity cannot be resolved — only if synthetic identity detection yields uncertain results should somebody be routed through the expensive and time-consuming process of document verification. Vendors might refer to this kind of system as "step-up" or "escalating" verifications.

Whether you implement a step-up system, or a system where every claimant ends up with a fully proved identity, there are a number of benefits compared to the existing solutions that unemployment insurance agencies have:

- More bad actors are likely to be caught early on while letting legitimate claimants through the system
- The burden of document collection and inspection is removed from UI agencies' employees.

However, a step-up solution has additional benefits compared to solutions that fully prove all identities:

- Likely cost savings, as these validations and verifications can be expensive add-ons from some vendors (or baked into a higher base price from others)
- There would be a faster application process for the majority of users whose identities can be resolved with confidence using just synthetic identity detection. This reduction of individuals required to go through document verification also has the benefit of preserving the limited data plans that many people seeking unemployment have to manage.

User Experience of Identity Proofing

A strong identity proofing system can be achieved either through a single product offering, or multiple products and/or vendors. When you use multiple products (either from the same vendor or multiple vendors), you can decide not to have everyone go through all identity proofing steps, and/or leverage information from multiple products at the same time to make a determination. (It is important not to chain these in such a way that would permit fraudulent identities to slip through via the weakest service.)

There are two ways that identity proofing can be integrated into a UI system for applicants to provide the required information:

1. Use the vendor's API so that the applicant never leaves your application website. This option allows for greatest flexibility and can provide applicants with a more consistent experience.
2. From your application, direct applicants away from your website, through a process on a vendor's website, and then back to your website again. This option is likely less work for the UI agency to implement.

Identity proofing is ideally part of the initial applicant experience. This reduces the number of applicants that need additional manual review. However, identity proofing can also be used to manage a backlog. By creating a process that encourages applicants to return to the website to provide more information, backlogged claims can be handled with less manual intervention. (Indiana did this by sending applicants a letter that directs them to an online identity quiz.)

When thinking about the backlog, there are also options that don't require an applicant to provide any additional information. For such non-interactive identity proofing processes, the vendor will compare the applicant-provided data to authoritative data sources and return a confidence level, which indicates how certain they are that the applicant is the person who they

claim to be. (Wisconsin has done synthetic identity detection on applications in their backlog to speed up determinations.)

Commercial Uses of Identity Proofing

Outside of the context of unemployment insurance, the most lucrative use case for identity proofing is in financial services, where know your customer (KYC) and anti-money laundering (AML) laws require businesses to know the real identity of their customers. Many of the vendors in this space concentrate on the financial services sector, where identity proofing is only a piece of the KYC puzzle. (Such vendors' lack of interest in the government sector means that they are often not on schedule, but it is still plausible to sole-source their services.) However, even the identity proofing component of these services has many use cases:

- **Age verification**: Uses identity proofing to confirm whether a customer should have access to age-limited products
- **Personal safety**: Dating and similar personal services use identity proofing to track customers
- **Fraud detection**: Credit issuers want to be sure someone is who they say they are
- **Retailers**: Associating online identities with persistent people enables building persistent and accurate user profiles, supporting use cases such as targeted advertising

Vendor Considerations & Requirements

There are many players in the commercial identity proofing & fraud detection space that are good candidates for use by UI agencies. In addition to providing key overview data for each company, we have aggregated data that will help UI agencies in making a vendor decision. We have also listed out a number of other non-functional requirements that would be relevant to most implementations.

Key Considerations

In evaluating vendors, we came up with a list of key questions that influence the degree to which the vendor could help ease the identity proofing burden on UI systems:

1. **What is the pricing model, and what is the cost?** If it's by verification attempt rather than only successful verification, the overall difference in per applicant cost could be 5-20% depending on the vendor's success rate (which we don't really know). Additionally, if a company has known set-up costs, those are noted.
2. **What is the user experience (UX) like during identity proofing at account creation?** I.e., is it an API call that is run in the background without the user noticing and/or a UX provided by the vendor that the user is sent to? Some vendors have a single product that provides an experience that all applicants would have; other vendors have multiple products that can be chained together in the "step-up" method depending on individual results.
3. **How can it be used to process users in the backlog who have been flagged as potential fraud risks?** The most impactful functionality in this area is whether they have a "batch API" that can be used to help make a determination on many individuals at once, without needing those individuals to take further action. Some vendors need a special workflow set up to send people from the backlog to their site to gather, or re-gather, information.
4. **What methods does it use to verify identity**, per descriptions in the Process of Identity Proofing section?
5. **Where do they get the data against which they perform the identity proofing, including SSN?** Every data source has limitations, and so in general, more data is going to result in more people with positively proved identities while continuing to catch those trying to commit fraud. (On the other hand, more data sources is likely to be reflected in a higher price for that vendor.)

Supplemental Considerations

If you believe that a vendor is a good match for your needs based on the key considerations above, the following information about the company could help you finalize your decision. Please do not be discouraged by "unknown" answers for some of these questions — that we have been unable to get answers to these questions does not mean that they are unanswerable.

1. What notable (name-brand) customers do they have?
2. What special certifications/authorizations does it have?
3. Have other government entities used it?
4. Does this vendor have existing contracts through an available Federal Supply Schedule (FSS) through GSA or some other Governmentwide Acquisition Contract (GWAC)?

5. Is this vendor under a recognized socioeconomic program or status such as the 8(a) program or Service-Disabled Veteran-Owned Small Business (SDVSOB)?

Nonfunctional Requirements

While most state unemployment insurance agencies are trying to solve the same set of problems, the technologies and processes that they are working with vary greatly. Each organization will have to determine their own requirements in the following areas:

- Network API and style (e.g. REST/SOAP/GraphQL)
- Supported development languages
- Client libraries
- Security concerns
- Average and 99th percentile response times
- Scalability
- Error rate
- Support (API docs, consulting services, third-party support, etc.)
- Licensing, embedding, reuse
- Data storage and access policies (Do they store PII on their side? Do their employees have access to that data? If so, how are those employees vetted and/or held accountable?)
- Severability and replaceability (How is their contract structured? If they store data, is that data accessible in a bulk, machine-readable format?)
- Hosting model (SaaS or on-premise?)

Vendor Analysis

For each of the evaluated vendors, we have done our best to provide accurate information through a combination of research and conversations with company representatives. This section of the document summarizes some of the more important vendor differences to inform your decision making. For all the details, see Appendix 1: Evaluation of Key Considerations and Appendix 2: Evaluation of Supplemental Considerations.

If you are a representative of an identity proofing or fraud detection company and are not included in our list, or believe we have mischaracterized your product(s) or left out key information, please reach out to ui-team@usdigitalresponse.org so we can follow up for inclusion and/or clarification as appropriate.

Vendor Overview

Vendors Evaluated

Name, website, and last date updated in this document	Headquarters	Founded	User Base	Best for
Alloy https://alloy.co 12/3/2020	New York, NY	2015	Financial services, banking	KYC/AML compliance, fraud prevention
Cognito https://cognitohq.com 11/30/2020	Palo Alto, CA	2014	Financial services and marketplaces	KYC compliance; address and age verification
Ekata https://ekata.com 12/2/2020	Seattle, WA	2012	Online lending, retail banking, ecommerce and marketplaces	Identity records for dynamic PII
Experian https://www.experian.com 12/2/2020	Dublin, Ireland	1996	Government partners, financial services, online lending	KYC compliance, fraud prevention, identity records
ID.me https://id.me 12/2/2020	McLean, VA	2010	Government partners, retail, online healthcare	Identity records
IDology https://www.idology.com 11/17/2020	Tallahassee, FL	2003	Financial services, banking, retail	Identity and age verification
SentiLink http://sentilink.com 11/25/2020	San Francisco, CA	2017	Retail banking, credit card issuers, all types of lenders, and fintech	Synthetic fraud detection & analytics
Socure https://www.socure.com 11/30/2020	New York, NY	2012	Retail banking, credit card issuers, and remittance providers	Fraud scoring and analysis

Vendors Not Yet Evaluated

As we evaluate these and/or other vendors, their information will be added to this document's existing charts and commentary:

- Acuant
- Google Cloud Descriptive Data Analytics
- ID Analytics (subsidiary of Lexis Nexis)
- LexisNexis Risk Solutions: LexID Digital
- NASWA Integrity Data Hub
- TransUnion's IDVision with Iovation

A Federal Alternative: Login.gov

There is an identity proofing vendor that falls outside of the scope of this document, but that is likely to be of interest to readers: Login.gov, provided by the federal government. The single-sign-on service was launched by the General Service Administration in 2017, providing two-factor authentication, fraud detection, and Identity Assurance Level 2 (IAL2) under NIST-800-63A. It was initially available only to federal agencies, with a FedRAMP Moderate ATO, with customers including the Department of Defense, the Department of Homeland Security, the Department of Energy, and the Department of Transportation. At the end of 2020 they were granted permission by the White House Office of Management and Budget to accept state agencies as customers.

Login.gov is not a drop-in identity proofing vendor. They perform identity proofing, but only as a component of a user registration process within Login.gov. For employment agencies to use Login.gov for identity proofing, they need to replace their entire authentication flow with Login.gov, integrating it via OAuth 2.0 or SAML.

Summary of Vendor Offerings

- Alloy is the most configurable of the vendors; they have partnerships with many other vendors that provide a wide variety of identity verification methods that can be used in combination with each other. Their partners include most of the vendors evaluated in this report: Cognito, Ekata, IDology, SentiLink, and Socure. We do not have information on their pricing.
- Cognito's identity proofing focuses on basic PII: Name, phone, address, and SSN. Their unique offering is through using synthetic identity detection to confirm the validity of a Name / Phone number combo, and then using 2FA to confirm that the person is still in

possession of that phone number. (Additional KBV is an add-on for further detection of stolen identities.) With this reliance on 2FA, their product isn't as suitable for managing the applicant backlog without needing the applicants to take some action.

- Ekata specializes in confirming "dynamic PII" -- Name, phone, address, and email. By also looking at passively-collected information (e.g., IP address and phone metadata), they are able to detect stolen as well as synthetic identities. They do not have a batch way to process the applicant backlog without needing the applicants to re-enter this basic PII. They do have a dashboard where you can see the results of an individual's ID proofing process.
- Experian is one of the vendors that could provide all the identity proofing pieces; they have both a step-up offering and a full NIST IAL2 offering. It is one of two vendors that appear to have gotten contracts with state UI agencies since the passage of the CARES Act (5-6 states). Their synthetic identity detection product can be used on the applicant backlog without needing the applicants to take any action (document verification would of course need the applicants to provide that documentation). They were the one company that mentioned the use of "marketing data" as one of many data sources used in their synthetic identity detection.
- ID.me is another of the vendors that could provide all the identity proofing pieces; their primary offering is a full NIST IAL2 identity proofing solution. (They also offer pieces as individual products, but we do not have as much information on that.) It is the other vendor that has gotten contracts with state UI agencies since the passage of the CARES Act (AZ, CA, FL, GA, IN, MT, NV, PA, TX). Their document + biometric verification solution is the most sophisticated; if someone cannot be verified through a comparison of a selfie to the uploaded documents, they are routed to a "remote in-person" identity proofing video chat where those documents are presented in real time to an ID.me call center. To be used in applicant backlog management, it requires that everyone be sent to their site to re-enter their PII and provide documentation because it is an IAL2 certified solution.
- IDology is another of the vendors that could provide all the identity proofing pieces, though we don't have their pricing information. They appear well set-up to be used in a "step-up" identification process for either applicant creation or backlog management (i.e., their batch API can do synthetic identity detection without additional action from the applicant). Part of their unique offering is access to the Consortium Fraud Network that allows them to securely check the use of PII combinations in additional contexts.
- SentiLink focuses on synthetic identity detection, comparing the self-asserted PII to numerous data sources. The breadth of their data sources means that with sufficient PII collected, they should be able to detect stolen identities; however, they did not mention the use of passively-collected information, which can be very helpful in this regard.

They can be used at either application creation or to evaluate applicants in the backlog without the applicant needing to take action; they also have a dashboard where you can see the results of an individual's ID proofing process.

- Socure is another of the vendors that could provide all the identity proofing pieces. They explicitly recommend creating a "step-up" process and shared that the synthetic identity detection step can verify 90% of people, leaving only 10% to need the more expensive doc + bio verification step. They can be used for either applicant creation or backlog management (i.e., their batch API can do synthetic identity detection without additional action from the applicant)

Deep Dive: Pricing

Given the variety of products from these vendors and the way that the information was provided, it's hard to do a direct comparison -- but we can try by making a couple of assumptions and establishing some constants:

1. For the vendor with a set-up fee (Experian), the cost is amortized over 2 years and 10,000 claims per month.
2. For the vendors that provided approximate costs:
    a. Sentilink said $0.25 / verification: we will create a moderate cost range of $0.15 - $0.45 / verification.
    b. Socure said mid-to-high single digit cents / query: we will create this as a range of $0.04 - $0.09 / query.
3. Two vendors have access to eCBSV for checking SSN directly against the SSA database. Neither seemed to push for this option (nor provided information about the additional cost this add-on would incur), so we are excluding that cost from their estimations.
4. Not all queries will result in a verified identity; we will stipulate that a best-case scenario for all vendors other than ID.me is 95%, and that the worst-case scenario is 80%.
5. *Because ID.me has a virtual in-person proofing step that none of the other vendors have, we will stipulate that their best-case scenario for achieving a verified identity is 99%, and that their worst case is 85%.

Below are the results of calculating average cost per query (i.e., cost per new UI claim) for the 6 vendors whose pricing information we have

	Low average cost per query	**High average cost per query**

Cognito	$0.56	$0.94
Ekata	$0.10	$0.25
Experian	$0.11	$0.28
ID.me	$3.96	$3.40
SentiLink	$0.12	$0.43
Socure	$0.09	$0.29

Deep Dive: Platform "Bundling"

Alloy and Experian are different from the other vendors in that they explicitly and transparently leverage other companies' technology as identity proofing platforms. Both take information that others have already interpreted and use that as an input to their own risk interpretation.

Alloy has a platform that can combine multiple risk assessments about the same piece of data. For example, Alloy can interpret in parallel the fraud risk data sent by both SentiLink and Ekata about a particular Name + Address combination. Alloy has agreements with more than 65 partners in total that can be mixed and matched when setting up an identity proofing system. This immense flexibility (and overlap with the vendors evaluated in this paper) and the fact that no pricing information was made available make it hard to come to any conclusion about Alloy.

Experian's approach is slightly different. They build some of the infrastructure themselves, and they rely on other companies for specific pieces of the puzzle: Acuant provides their document verification; EmailAge by LexisNexis gives them a risk assessment specifically about the longevity of an email address and the domain to which it belongs. Experian bundles the vendors and features into 2 or 3 offerings, as distinct from Alloy's a la carte approach.

UI agencies themselves could also build their own platform by using different vendors at different steps of the process. (If you wanted multiple products to provide synthetic identity detection on PII, it would likely be more effective and less risky to achieve that through Alloy--with the caveat that their pricing is unknown.) For example:

1. Use your existing method to determine validity of SSN / Name / DOB combination
2. If that combination is valid, collect and use additional PII (address, mother's maiden name, email, phone, etc.) and evaluate it with one vendor's synthetic identity detection product.
3. If step 2 indicates a particular fraud risk, have that individual go through a document + biometric verification step.

Deep Dive: Handling Social Security Numbers

UI agencies already have in place methods to determine whether a provided SSN / Name / DOB combination is real (i.e., not synthetic). That functionality can remain in place alongside any new identity proofing mechanisms, as long as there is clear communication between pieces of the system.

There are 3 ways that vendors determine the validity of a provided Social Security Number (Ekata doesn't handle SSNs at all). Methods 2 and 3 below are more "official," but both Cognito and Socure believe their method to be effective.

1. Cognito and Socure have systems that search for prior use of a SSN / Name / DOB combination, e.g., through DMV records or credit files. A drawback of this approach (depending on the details of the vendor's implementation) is that it is possible for synthetically created identities to have credit files. Additionally, the vendors that rely heavily on credit bureau sources will systematically be less likely to prove the identities of those with less access to credit. Via both Cognito and Socure, Alloy has this functionality.
2. Experian, ID.me, and SentiLink have systems that check against the Social Security Administration Death Master File, which will not have any synthetic identities in it. All three vendors use additional methods to detect synthetic identities. However, it is updated at most weekly and is not a comprehensive record of all deaths in the country; a notable exception is that it excludes state death records. Via SentiLink, Alloy has this functionality.
3. In addition to leveraging the SSA Death Master File, SentiLink and Experian have access to the SSA's new eCBSV product, which allows them to effectively query the SSA directly and thus know with near-certainty that the SSN / Name / DOB match, and belong to a live human. Doing this check with SentiLink incurs an additional cost, and it's not clear how it interacts with Experian's pricing. Via SentiLink, Alloy may also have this access.

Deep Dive: Document Verification

Digitizing the document verification step for those whose identities are in question is a key part of detecting fraud *and* of reducing load in UI agency staff. As discussed in Recommended process for UI Identity Proofing, the system can require everyone to go through a document verification process, or only a subset of individuals (a "step-up" process).

The following vendors provide document verification:

- Alloy
- Experian
- ID.me
- IDology
- Socure

All of these vendors' documentation verification products combine it with a biometric verification step. The biometric verification is in the form of a selfie that gets checked for "liveness" (i.e., to check whether someone else's existing photo was uploaded) as well as compared against the provided photo ID.

ID.me's document + biometric verification is built into their primary product offering. They take doc + bio verification a step further than any of the other companies with a remote "in-person" identity proofing interview: a video call in which an applicant must present their documents live. This happens only for the set of people who cannot be verified at other steps in their process. (You can also get their document verification and/or doc + bio verification products individually, but we don't have information about the pricing.)

IDology, and Socure have their own stand-alone document verification products that could be used as the "step up" from a different vendor's synthetic identity detection. Alloy and Experian could likely provide just a document verification service, but it may not be the most efficient way to do so: Both use Acuant to provide document verification.

The following vendors do not have document verification:

- Cognito
- Ekata
- SentiLink

What's Next?

1. USDR can help you further evaluate vendors to find out which will best suit your state's specific needs. Reach out to ui-team@usdigitalresponse.org if you are interested.
2. Follow 18F's De-Risking Government Technology: State Field Guide when planning your identity proofing automation project.

3. See “Appendix B: Acceleration Plan for Identity Verification” in California’s Employment Development Department Strike Team Detailed Assessment and Recommendations to serve as a reference for how you can create a plan for your state.

If you have questions or need help solving unemployment insurance issues in your state, please contact the Unemployment Insurance Team at ui-team@usdigitalresponse.org.

Appendix 1: Evaluation of Key Considerations

For some of the vendors, the answer is “unknown,” and we continue working to try to find that information.

	Pricing	UX at account creation	Backlog management
Alloy	Unknown	Step-up process: - API for PII collection - UX for doc verification	- Has batch API to check PII - UX for doc verification
Cognito	$0.70 - $0.99 / verification	API for PII collection	Has batch API available but won’t be able to verify phone number
Ekata	$0.10 - $0.25 / query	API for PII collection	No batch API to check PII
Experian	$0.10 - $0.25 / query, plus $2,500 or $6,500 set-up fee based on implementation detail	Step-up process: - API for PII collection - UX for doc verification - UX for UI agents to input info provided via phone	- Has batch API to check PII - UX for doc verification
ID.me	$4.00 / verification; $2.00 for subsequent years’ renewal	- Complete UX for PII collection and doc verification	- UX for PII collection and doc verification
IDology	Unknown	Step-up process: - API for PII collection - UX for doc verification	- API for PII collection - UX for doc verification
SentiLink	~$0.25 / verification	API for PII collection	Has batch API to check PII
Socure	Mid-to-high single digit cents / PII query; add’l $1/query for doc verification	Step-up process: - API for PII collection - UX for doc verification	- API for PII collection - UX for doc verification

	Identity proofing methods (and product names, if applicable)	**Data sources**
Alloy	Highly configurable: KBV, 2FA, synthetic identity detection (including looking at device "fingerprinting" and IP address), document verification, biometric verification	Partnerships with 65+ data vendors including ones we have or will evaluate: Acuant, Iovation from TransUnion, Ekata, Socure, Cognito, Sentilink, and IDology
Cognito	- *Cognito Identity Verification Service:* 2FA, synthetic identity detection - *Blocksore product*: 2FA, synthetic identity detection, KBV	Credit bureaus and public data sources
Ekata	Synthetic Identity Detection	Public data sources -- does NOT check SSN
Experian	*Experian PreciseID:* Synthetic Identity detection, KBV, 2FA *Experian Identity Proofing:* Document verification, biometric verification	Credit file info; SSA Death Master File (also a partner in SSA's eCBSV program); marketing data; Motor vehicle info from auto dealerships and DMVs; public data sources
ID.me	Synthetic identity detection, document verification, biometric verification	Credit bureaus, SSA Death Master File, telco records, public data sources
IDology	*ExpectID:* Synthetic identity detection *ExpectID IQ:* KBV, synthetic identity detection *Document Scan Solution:* both document verification and biometric verification	Motor vehicle info, voting record, creditor information, utility bills Have "Consortium Fraud Network" for additional commercial sources
SentiLink	Synthetic identity detection	Credit bureaus, utility data, SSA Death Master File (also a partner in SSA's eCBSV program), selective service information
Socure	*KYC identity verification module & Sigma Fraud products:* synthetic identity detection *DocV product:* both document verification and biometric verification	Credit bureaus, utility data, telco, public data sources

Appendix 2: Evaluation of Supplemental Considerations

Note: as none of the evaluated vendors are under a recognized socioeconomic program or status, that information isn't duplicated in the chart below. For some of the vendors, the answer is "unknown," and we continue working to try to find that information.

	Notable commercial customers	**Notable government customers**	**Relevant certifications**	**Schedule information**
Alloy	Austin Capital Bank, Langley Federal Credit Union, Radius Bank	Unknown	Unknown	Unknown
Cognito	Brex, Nextdoor, Coinbase, BBVA	None	SOC2 Type 2 Certification	No
Ekata	Lyft, Alaska Airlines	None	SOC2 Type 2 Certification	No
Experian	NASWA Integrity Data Hub	Healthcare.gov, IRS, Michigan's MyLogin, 5-6 state UI agencies	NIST 800-63-3 IAL2 (for their full ID proofing product)	GSA (GS-35F-188AA) & NASPO
ID.me	LinkedIn, Lenovo	Vets.gov, 9 state UI agencies	NIST 800-63-3 IAL2/AAL2; in process of FedRamp authorization	Have a growing government business line, but do not promote availability on any found schedule
IDology	Unknown	Unknown	Unknown	Unknown
SentiLink	Several of the largest banks, credit card issuers, credit unions, and auto lenders	With at least one state's PPP	SOC2 Type 2 Certification, PCI Compliance, EI3PA Compl.	Unknown
Socure	Seven of the nine largest U.S. banks, six of the top 10 U.S. card issuers, Chime, SoFi	Unknown	-In processes for FedRamp authorization & NIST IAL2	Available on AWS Marketplace, so it may be simple to procure via an existing AWS contract