US DIGITAL RESPONSE

# Race and Inequity in Identity Proofing Methods

## Recommendations to Reduce Inequitable Impacts of Identity Proofing Systems

Updated: February 2, 2021

**Alyssa Levitz**
Unemployment Insurance Modernization
U.S. Digital Response

# Who We Are

U.S. Digital Response serves the immediate needs of the public by activating highly-skilled talent, leveraging new technology, and partnering directly with governments and nonprofits.

Our 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.

Our diverse cohort of volunteers has 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.

If you have questions or needs regarding unemployment insurance, please contact the team at ui@usdigitalresponse.org or fill out our form.

# Identity proofing introduction

PDF Download of Report 2020-12-11 USDR Identity Proofing.pdf - 501KB

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.

# Race and inequity in identity proofing methods

## Introduction

The vast fraud committed through the use of stolen and synthetic identities in UI programs has spotlighted the need for updated identity fraud detection mechanisms. The Dec. 2020 Continued Assistance Act mandated states make such a change for Pandemic Unemployment Assistance in particular. As States are implementing new technologies and systems, they need to consider the ways in which they are impacting racial inequities in UI benefits. States can do this by:

1. Finding and mitigating the ways in which their identity fraud detection flags will disproportionately affect POC
2. Increasing accountability for ensuring rightful claimants make it through the system

# Background

In UI systems, there is a balance between finding fraud and getting benefits out in a timely manner. Right now, a lot of fraud is slipping through and benefits are severely delayed. As we work to shift this balance, we need to ensure that we reduce – not broaden – racial inequities in UI.

During the Great Recession, young white men received UI benefits almost twice as often (13.6%) as young black men (7.1%). While there are many factors at play, one piece that can't be ignored is the fact that POC are more likely to be flagged for identity fraud (though there is no evidence they are more likely to commit identity fraud).

Now is the right time to be looking at this issue, as the Continued Assistance Act of December 2020 created a new requirement for States to have digitized identity verification processes for Pandemic Unemployment Assistance. Many States had already begun doing, or actually completed this, by the time the legislation passed; however, even those States should look at their identity fraud detection processes (including the contracts they have with vendors) and surrounding user experience.

At the same time, States should also make sure that being flagged for potential identity theft does not on its own kick off other processes like trying to find benefits fraud so that the racially disparate outcomes are not compounded.

# Recommendation 1: Find and mitigate inequitable impact of identity fraud detection flags

There are several common mechanisms by which people get caught up in fraud detection systems in a way that disproportionately targets POC. Below are some common problem areas and how to resolve them.

## Recommendation 1.1: Systems should not use IP Address Geolocation as a binary signal for fraud but instead as part of risk score

IP addresses are used to geolocate web traffic. For UI agencies, traffic coming from, e.g., out of state can be suspicious. However, there are several limitations to this approach that ultimately amount to the fact that IP addresses are not particularly trustworthy as a binary fraud detection mechanism; they should be used as part of a risk score.

- IP Address databases might simply be out of date
- Black and Latinx adults are 25% less likely than White adults to own a laptop or desktop computer. Without a desktop computer to file (a situation that also disproportionately happens to those who are housing insecure), you might be using devices from friends or relatives or a library (if open), or using your cell phone – all of which means your location may change from week to week, and your apparent location may change even more.

## Recommendation 1.2: Audit and fix system's English bias in name-matching

Many UI systems were built with just English names in mind, which does not reflect the linguistic and cultural diversity of the United States. Systems need to be able to handle:

- Short first and family names without error
- Long first and family names without truncation
- Non-Roman characters (spaces, hyphens, apostrophes, accents) without error

In addition to being able to accurately store names with the above characteristics, the identity fraud detection process needs to have some flexibility in how it interprets and cross-references names across pieces of the application. It needs to account for mistakes that the system made with someone's name (e.g., truncated after 10 characters in part A but truncated after 15 characters in part B) as well as for cultural considerations (e.g., someone might have "Graciela" on their birth certificate but "Grace" on their driver's license, or sometimes put a second surname in a middle name field instead of the last name field).

## Recommendation 1.3: Update threshold for number of claims filed from same address

One common flag for UI fraud is many people filing from the same address. However, "[f]amilies of color and families with foreign-born members are more likely to live in multigenerational households," meaning they are more likely to be flagged on suspicion of fraud. Further, the addresses of homeless shelters and other social service agencies can be used in the absence of permanent housing. This should be taken into account when determining a threshold for flagging claims.

Additionally, UI agencies should:

- Ensure they are looking at all parts of the address (e.g., including apartment or floor number) when comparing addresses for multiple claims filed. Otherwise, those who live in multi-family housing units will disproportionately be targeted.
- Proactively "clear" addresses known to be used by those who are housing insecure and thus could have many claims filed

## Recommendation 1.4: Ensure there is a clear alternative to digital document verification

Many States' identity verification solutions require claimants to provide photo IDs corroborating their identity. This is important for a robust determination that someone is who they say they are (per NIST IAL2 standards), but it does raise some concerns.

Document verification processes can cause a number of issues from the name mismatch described above – or a complete break in the process because someone doesn't have the

right (or any) documentation. People who are poor, formerly incarcerated, or Black are less likely than their richer, White counterparts to have a valid ID.

In any document verification step, there must be a clear way for a claimant to get in touch with a representative of the agency to find an alternative method for proving they are who they say they are. Otherwise, people without IDs are categorically going to be denied benefits in a racially skewed outcome.

# Recommendation 2: Increase accountability for ensuring rightful claimants make it through the system

An unknown number of legitimate claimants are being prevented from receiving the benefits for which they are eligible. This marks a failure of the UI system that has not received as much attention as it deserves.

There is currently no way to tell the difference between someone who gave up because they were a criminal and knew they couldn't pass the step, and someone who gave up because they didn't understand or have the required documentation to move on.

But we can--and should--tell a different story: one that gives as much weight to how easy these systems are for the rightful claimants to pass through as it does to how good they are at catching criminal actors.

## Recommendation 2.1: Do not count incomplete applications as fraud

It is currently in the interest of both identity proofing vendors and the UI agencies that contract them to conflate unstarted and incomplete applications with fraud. The vendors' performance looks more impressive if they don't counter the perception that everyone who doesn't get positively identified is fraudulent. UI agencies, under intense scrutiny from the public and US DOL, are able to look more effective.

But, again: The fact that someone was stopped from receiving benefits does not mean that they were rightly stopped. Agencies and vendors should be careful with their language and not imply that unstarted or incomplete applications are fraud.

The agencies should work with the vendor(s) that provide their identity verification solutions to ensure that the unstarted and incomplete applications are tracked and reported separately from those whose incomplete or completed applications had a positive indicator of fraud detected. That data from the vendor should be made available on a user-by-user basis to the UI agency so they can connect it to their own claimant data and break it down by race.

Distinguishing this “false” rejection rate from the overall rejection rate of these systems is a key step toward improving benefits participation rate.

## Recommendation 2.2: Usability test the complete experience

While the document+biometric verification products will have gone through usability testing within the vendor's company, UI agencies should usability test the end-to-end experience themselves or in partnership with the vendor.

Whether the identity proofing is included in the initial application, triggered by a change on the account, or requested as part of a backlog-clearing process, it exists in a context beyond what the vendor could've usability tested independently: e.g., surrounding website interface, digital notification or physical letter asking them to complete the identity proofing process. Here are some key questions to ask about the experience:

- How is someone notified that they need to go through additional identity verification?
  - Does it make clear what people should do if they don’t have a photo ID or have difficulty going through the vendor’s process?
  - What methods are used, and are those effective for the population in question? (Have you considered using SMS?)
  - Has the notification content been usability tested in all languages? (Do people understand what is being asked of them, and the importance of them following through?)
- Is the claimant reminded to start the process if they don’t ever begin? (They should be.)
- How long does someone have to complete the identity proofing process? Does the data support this time period? (California increased the period from 10 to 30 days.)
- What languages is the vendor’s user experience available in?
- If someone starts but does not finish the application:
  - Is there a clear way from the vendor’s user experience for someone to get direct agency help if they are unable to provide what the process requires?
  - Is the claimant reminded to complete the process if they begin but do not finish? (They should be.)

By conducting their own usability testing, UI agencies have the opportunity to make sure that the experience has been tested by a representative sample of people based on the demographics of the population seeking UI benefits. If anything is found to be unclear, the

agencies should work either on their own or with the vendor to ensure that the experience or communication is improved.

## Recommendation 2.3: Ask your doc+bio verification vendor for performance measures by skin type classifications

In a 2018 study co-authored by researchers at the MIT Media Lab and Microsoft Research, lighter-skinned men were more than 40x less likely to be misclassified than darker-skinned women in common face recognition software. A response by IBM to that paper said that they made significant improvements to their system, but lighter-skinned men were *still* 13x less likely to be misclassified than darker-skinned women.

The NIST Face Recognition Vendor Test found that when image quality is low and you're trying to match a photo to one of many possibilities (1:N), "false negatives are generally higher in people born in Africa and the Caribbean, the effect being stronger in older individuals."

If these patterns are at all present in the 1:1 matching use case between a selfie (which isn't necessarily going to be high quality or well-lit) and an ID photo, it would contribute to racial disparities in benefits participation rates.

Ultimately, more information is needed on how false rejection rate differs by skin type. onfido,* a company with a document+biometrific verification product, has been transparent about how its false *acceptance* rate differs by continent, but there doesn't appear to be data on false rejection rate by skin type from *any* of the major players in the space.

UI agencies should ask the vendor they are using for document+biometric verification for these performance metrics, and if there is any discrepancy between performance for different skin types, they should ask how the vendor is planning to improve. Jumio,* another company that provides this product, published "5 Practical Ways to Reduce AI Bias in Online Identity Verification," which is a succinct and useful list to reference.

* **Note:** USDR is neither affiliated with nor endorses any vendors. Additionally, at the time of this publication, neither onfido nor Jumio has been evaluated as part of USDR's ID Proofing Vendor Comparison, but that shouldn't be seen as an indicator of their suitability for UI agencies' needs.

# References and thanks

All sources are linked inline. I particularly want to call out the phenomenal and in-depth research in New America's Public Interest Technology New Practice Lab's Unpacking Inequities in Unemployment Insurance report, September 2020, in particular Section 3: A Focus on Fraud Over Accessibility: The Punitive Design of UI.

Thanks also to Robin Carnahan, Sara Hudson, Waldo Jaquith, Julia Simon-Mishel, and Sam Zeitlin for the knowledge they shared with me in conversations.

# 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.

# 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.

# Process of identity proofing

**Note:** This section has been adapted from NIST Special Publication 800-63-3 and combined with additional research. IAL2 is the level of NIST certification that is generally appropriate for unemployment insurance agencies.

“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:

- Identity resolution: comparing personally identifiable information (PII) provided by the user to public databases.
- Identity validation: confirming that the claimant is the same person as the owner of the user account.
- Identify verification: establishing a physical connection between the applicant and the PII or evidence provided.

# 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.

# User experience of identity proofing

## UX flow

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 (risk score), 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.)

Regardless of the way you integrate with a vendor, you should make sure that there are clear ways for someone to get direct agency help if they are unable to provide what the process requires. Doing so is an important piece of reducing the racial inequity gap of UI benefits in two key ways:

1. People who are poor, formerly incarcerated, or Black are less likely than their richer, White counterparts to have a valid ID. In any document verification step, there must be a clear way for a claimant to get in touch with a representative of the agency to find an alternative method for proving they are who they say they are. Otherwise, people without IDs are categorically going to be denied benefits in a racially skewed outcome.
2. No UX is perfect, and those with lower digital literacy may need additional support or other lower-tech mechanisms to complete their application and prove they are who they say they are. We note this here because Black and Latinx adults are 2-3 times less likely than their White counterparts to be digitally literate.

---

## UX metrics

There is currently no way to tell the difference between someone who gave up because they were a fraudster and knew they couldn't pass the step, and someone who gave up because they didn't understand or have the required documentation to move on. An unknown number of legitimate claimants are being prevented from receiving the benefits for which they are eligible. This marks a failure of the UI system that has not received as much attention as it deserves.

Success ought to look like ensuring every legitimate claimant is able to access the benefits for which they are eligible; we should not assume that everyone who doesn't complete the application was trying to commit fraud. For more on this idea, read this OpEd or see Race and inequity in identify proofing methods.

# Identity proofing vendor comparison

## 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.)

→ Appendix I: Vendor evaluation of key considerations
/identity-proofing-vendor-comparison/appendix-i-vendor-evaluation-of-key-considerations

## 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)?

→ Appendix II: Vendor Evaluation of Supplemental Considerations
/identity-proofing-vendor-comparison/appendix-ii-vendor-evaluation-of-supplemental-considerations

## 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


→ **Appendix I: Vendor evaluation of key considerations**

/identity-proofing-vendor-comparison/appendix-i-vendor-evaluation-of-key-considerations

→ **Appendix II: Vendor Evaluation of Supplemental Considerations**

/identity-proofing-vendor-comparison/appendix-ii-vendor-evaluation-of-supplemental-considerations

# 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 the appendices:

*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**<br>https://alloy.co<br>12/3/2020 | New York, NY | 2015 | Financial services, banking | KYC/AML compliance, fraud prevention |
| **Cognito**<br>https://cognitohq.com<br>11/30/2020 | Palo Alto, CA | 2014 | Financial services and marketplaces | KYC compliance; address and age verification |
| **Ekata**<br>https://ekata.com<br>12/2/2020 | Seattle, WA | 2012 | Online lending, retail banking, ecommerce and marketplaces | Identity records for dynamic PII |

| | | | | |
|---|---|---|---|---|
| **Experian**<br>https://www.experian.com<br>12/2/2020 | Dublin, Ireland | 1996 | Government partners, financial services, online lending | KYC compliance, fraud prevention, identity records |
| **ID.me**<br>https://id.me<br>12/2/2020 | McLean, VA | 2010 | Government partners, retail, online healthcare | Identity records |
| **IDology**<br>https://www.idology.com<br>11/17/2020 | Tallahassee, FL | 2003 | Financial services, banking, retail | Identity and age verification |
| **SentiLink**<br>http://sentilink.com<br>11/25/2020 | San Francisco, CA | 2017 | Retail banking, credit card issuers, all types of lenders, and fintech | Synthetic fraud detection & analytics |
| **Socure**<br>https://www.socure.com<br>12/11/2020 | 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:
    1. Sentilink said $0.25 / verification: we will create a moderate cost range of $0.15 - $0.45 / verification.
    2. Socure said mid-to-high single digit cents / query: we will create this as a range of $0.04 - $0.09 / query.
3. 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%.
4. *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 2 ways that vendors determine the validity of a provided Social Security Number (Ekata doesn't handle SSNs at all). The second method is 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.

Note: Two vendors, SentiLink and Experian, have access to the SSA's new eCBSV product, which *for their financial customers only* 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. Unfortunately, the SSA does not currently allow for other uses of this API, despite how useful and effective it would be for the UI identity theft detection scenario.

# 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 I: Vendor evaluation of key considerations

For more information on each of the considerations, please see Key Considerations.

For some of the vendors, the answer is “unknown,” and we continue working to try to find that information. For ease of reading on a variety of screen sizes, the evaluation is split into two charts:

## Part 1

| | Pricing | UX at account creation | Backlog management |
|---|---|---|---|
| Alloy | Unknown | Step-up process:<br>- API for PII collection<br>- UX for doc verification | - Has batch API to check PII<br>- 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:<br>- API for PII collection<br>- UX for doc verification<br>- UX for UI agents to input info provided via phone | - Has batch API to check PII<br>- 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:<br>- API for PII collection<br>- UX for doc verification | - API for PII collection<br>- 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:<br>- API for PII collection<br>- UX for doc verification | - API for PII collection<br>- UX for doc verification |

# Part 2

| | 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<br>- 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<br>Experian Identity Proofing: Document verification, biometric verification | Credit file info; SSA Death Master File; 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<br>ExpectID IQ: KBV, synthetic identity detection<br>Document Scan Solution: both document verification and biometric verification | Motor vehicle info, voting record, creditor information, utility bills<br><br>Have “Consortium Fraud Network” for additional commercial sources |
| SentiLink | Synthetic identity detection | Credit bureaus, utility data, SSA Death Master File, selective service information |

| | | |
|---|---|---|
| Socure | KYC identity verification module & Sigma Fraud products: synthetic identity detection<br>DocV product: both document verification and biometric verification | Credit bureaus, utility data, telco, public data sources |

# Appendix II: Vendor Evaluation of Supplemental Considerations

For more information on each item, please see 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<br>-SOC2 Type 2 Certification<br>- ISO 27001/ 27017/27018 | Available on AWS Marketplace, so it may be simple to procure via an existing AWS contract |

If you have questions or needs regarding unemployment insurance, please contact the team at ui@usdigitalresponse.org or fill out our form.

US DIGITAL RESPONSE