



ID.me



○

Eight best practices
government agencies
should require from
digital identity providers

Introduction

Identity underpins every transaction in society. Across the economy — and especially for government, healthcare, and finance — it is critical that organizations trust people are who they claim to be. Digital identity verification, however, is fundamentally broken.

The COVID-19 pandemic revealed the stark limitations of the identity layer of the internet. With in-person interactions curtailed, governments and companies scrambled to digitize their processes and services. McKinsey and Company estimated that the share of customer interactions on digital platforms jumped 41% to 65% through July 2020. It estimated that number to be even higher for public sector services, reaching 90% by April 2021.¹

As this historic digital migration unfolds, corners of the population are being left behind. Many people struggle to access government programs that require identity verification because data brokers and other legacy solution providers are unable to support people with common barriers: lack of credit history for young people or unbanked individuals, name changes due to marriage, international moves for immigrants and emigrants, and unease with technology.

Not having a digital identity impacts these groups of people as well as those who count on their governments for critical benefits and services, such as:

- ✓ aging veterans seeking healthcare benefits
- ✓ service economy workers who need unemployment assistance
- ✓ seniors who need to access Medicare
- ✓ distressed tenants in need of rental assistance

A dramatic increase in benefits fraud and identity theft further compounds these challenges. ID.me saw this firsthand during our work supporting unemployment claims for 27 states. Millions of Americans were unable to access unemployment benefits due to outdated systems and identity theft, while cybercriminals, foreign and domestic, stole billions in taxpayer dollars. Our data, supported by public data from the states and reported by Axios, ProPublica, and NBC News, show the fraud rate likely exceeds hundreds of billions.²




Introduction

This crisis is not ending anytime soon. The same fraudsters who got their start with unemployment have moved on to disaster response, small-business grants, and other forms of benefits. Delay in action by government agencies and commercial sector companies will cause continued emotional heartache for individuals who can't access the services they need and continued financial damage to programs across state, local, and federal governments. Commercial off-the-shelf solutions can reverse this trend faster than investing time and money building bespoke solutions.

Lastly, it is important to note that most government-branded solutions used at state and federal agencies are powered by commercial companies. Unless the government agency builds the underlying technology in-house, citizens' personal data is going to large private sector data brokers. Because the business model of these brokers is built on purchasing and selling data, they often find themselves walking a fine line between what's good for their business and what's in the consumer's best interests.^{3,4,5}



To respond to these increasing challenges and modernize digital identity, decision makers should look for eight best-in-class traits when choosing a digital identity provider. Digital identity providers who possess these traits can:

-  **maximize access**
-  **minimize fraud**
-  **pass cost savings onto government and other customers**



- **Maximizes access** by offering an omni-channel experience (self-serve, virtual in-person / video chat, and in-person) that achieves best-in-class pass rates

Maximizes access

Today, agencies employing legacy systems supported by data brokers have low pass rates and often make errors that lead to understandable frustration.⁶ Many groups of people struggle to get through these outdated and inadequate systems.

As one example, Americans over the age of 65 — a group that often participates in high-impact services such as Social Security, Medicare, and Veterans Administration benefits — suffer unfairly from data brokers' insufficient digital systems.

About 29% of Americans over the age of 65 do not own a smartphone⁷, 36% do not have broadband at home, and 25% do not use the internet at all.⁸

While credit bureaus and utilities tend to have records for individuals in this group, it is relatively more difficult for this group to access digital services. This makes it extremely difficult for legacy providers that offer only online self-service workflows to enable access for these groups of people.

Enabling access to everyone means providers must meet citizens and consumers "where they are." The only way to do this is via an omni-channel experience that includes self-service online workflows, virtual in-person proofing (video chat), and in-person verification (kiosks or brick-and-mortar locations).

Additionally, the pathways in an omni-channel offering reinforce each other by acting as "relief valves." In other words, when an individual has trouble verifying via self-serve, they can escalate to video chat or in-person, depending on their specific situation. This ensures that Americans with recent name or address changes or without access to smartphones and webcams can still verify their identity. These video call and in-person options can assist people even if they have an unreliable internet connection. It also eliminates the concerns that some have around new technologies, such as facial recognition.

ID.me's experience as the only provider of a NIST-compliant (<https://pages.nist.gov/800-63-3/>) omni-channel offering proves ready-to-deploy commercial-off-the-shelf (COTS) solutions that adopt this approach can achieve NIST-800-63-3 IAL2 pass rates that are more than twice that of limited-channel solutions.



29%

of Americans over the age of 65 do not own a smartphone⁷

36%

do not have broadband at home⁸

25%

do not use the internet at all⁸

2

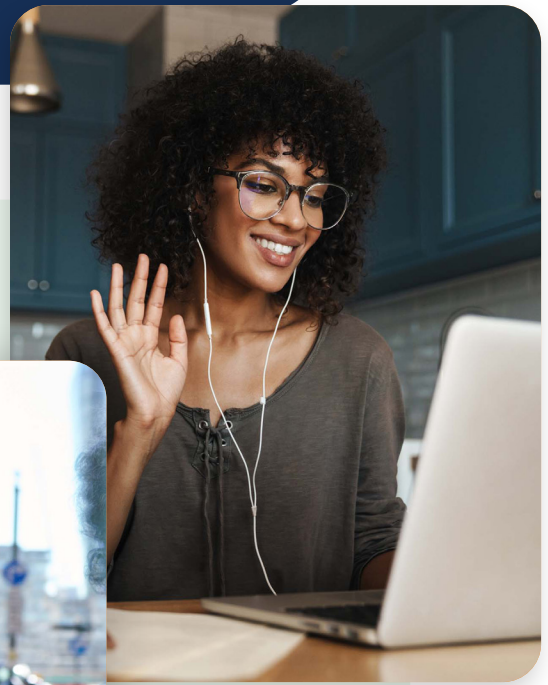
- **Makes verification pathways easy to use**
by offering multilingual options and broader Section 508-compliant accessibility

○ Makes verification pathways easy to use

Businesses and agencies should expect their credential service providers to enable access to all of their authentic potential customers. This means that credential products should offer features and services that enable broader access via multilingual options and broader Section 508 compliance. The user interface should be available across desktops, tablets, and mobile devices. Any in-person interactions must also be fully accessible for all users.

All products should be extensively tested and certified to be in conformance with ADA / Section 508 standards. Providers should be able to demonstrate that their products are in use by individuals with different abilities that include but are not limited to visual impairments, color blindness, or the inability to use mice/pointing devices.

In addition, to show our commitment to how languages increase access and equity, ID.me has made support resources available in 13 languages, our self-serve flow in five languages (nine by the end of 2022), and our video chat flow in spoken four. The provider's products should be internationalized and support identity verification and authentication in local languages. To expand accessibility, non-English options should be made available across channels (e.g., online as well as spoken languages on video chat).





- **Demonstrates commitment to consumer privacy and consent**

Demonstrates commitment

In its current form, digital identity is flawed. Credentials that consumers trust — such as those issued by their banks — aren't portable. Portable credentials like social media accounts raise serious questions about privacy and data control.

Americans want to know how companies use their personal data, so a credential service provider's position on privacy and consent is critical to winning trust. Sixty-two percent of Americans believe it is not possible to go through daily life without companies collecting data about them and 79% are concerned by how their data is being used by companies.⁹

The Obama/Biden National Strategy for Trusted Identities in Cyberspace (NSTIC) understood and anticipated citizens' needs. NSTIC addressed this challenge by including privacy enhancing identity solutions as a key pillar. To put these pillars into action, they began funding solutions that addressed concerns about the interplay between identity, privacy, and civil liberties.

That includes risks to privacy created by entities in different sectors linking individuals' transactions and the capacity for more tracking and profiling of individuals.¹⁰

NSTIC guidance and funding resulted in the development of products and commercial off-the-shelf (COTS) software that enhance privacy and promote citizen control of their data — solutions like ID.me. Supported by two grants from NIST, ID.me developed a product that offers NIST 800-63-3 IAL2/AAL2 credentials and does not share any user data without their explicit consent.

To be transparent with citizens, ID.me explicitly states what verified data will be shared with an entity and prompts the user for consent prior to transmitting that data. ID.me only shares what is necessary to complete a given transaction. These grants would not have been awarded to ID.me if NSTIC had not believed ID.me's product and values would enhance privacy for American citizens.

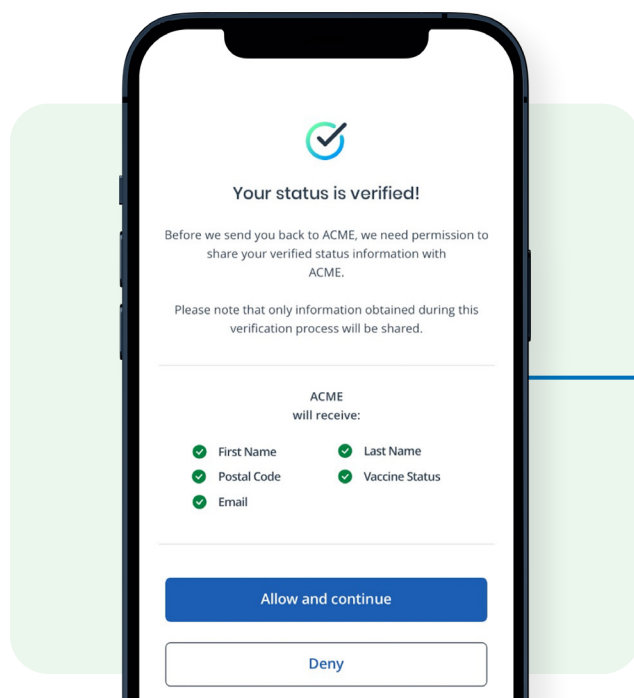


Figure 1: Asking permission before sending an individual's attributes to a generic organization

Demonstrates commitment

Credential service providers who are committed to privacy should be willing to speak openly about this commitment, similar to ID.me's Privacy Bill of Rights, which can be found [here](#). As a best-in-class credential service provider, ID.me must be an ethical steward of personal information and commit to supporting fundamental privacy rights:

- ✓ Individuals are solely in control of their data and must provide explicit consent for ID.me to share their information.
- ✓ Individuals can view all authorized apps and data elements in their "My Account" portal
- ✓ Individuals can revoke access to their data for any app or website at any time
- ✓ Individuals may destroy their ID.me credential and associated data at any time.



Not all credential service providers respect privacy and are open about their approach to it. Large data brokers used by government agencies today have paid fines in class-action settlements after taking data from trusted sources — such as DMVs — and then reselling it to other organizations that did not have a legally permissible use for that information.¹²

We believe a best-in-class CSP will encourage trust by being open and transparent about their stance on privacy. They will also be open and transparent about what data they are sharing and ask for consent prior to sharing it. This makes it easier for citizens to control their data and limit transmission to only what is needed to access required services and workflows.

4

- **Demonstrates a track record of fraud prevention** both “horizontally” between states and “vertically” between state and federal agencies – with a robust fraud prevention program and dedicated investigations teams

Demonstrates a track record of fraud prevention

Digital identity theft and online fraud continue to get worse. The Federal Trade Commission (FTC) reported that identity theft tied to government benefits increased by 2,920% year over year.¹³ Therefore, any credential service provider working with the government should be able to proactively identify, prevent, and report identity fraud. The provider must have a well-designed product, user behavior analysis, intelligence collection on attack vectors, and insights that can be utilized by businesses and government agencies.

ID.me's work with state unemployment agencies revealed preexisting identity verification systems based on data brokers and credit bureaus were unable to halt billions in fraud nor handle millions of new claims.¹⁴ Many identity theft cases stem from data breaches that occurred at large credit agencies and data brokers, most famously the 2017 Equifax breach that leaked 147 million identities to the dark web.¹⁵

Digital identity providers are the first line of defense against fraud and are critical to protecting taxpayer money. A recent ProPublica report found 84% of unemployment claims in Pennsylvania were fraudulent, with similar numbers reported across the country.¹⁶ Stopping fraud requires vertical integration across federal and state agencies, which is best enabled via public-private partnerships.

At a recent Federal Identity Forum and Expo, White House American Rescue Plan Coordinator Gene Sperling noted the government is unable to determine when a criminal uses the same stolen identity to commit fraud against multiple government agencies.¹⁷ Portable credentials that are used across federal, state, and commercial organizations — such as those offered by ID.me— can stop fraudsters who move across government agencies in ways that a federal-only solution cannot.

A federated identity provider with strong analytics capabilities can identify, investigate, and take action on stopping suspicious activity, including both first-party and third-party fraud. For example, a federated system could track an individual who has filed unemployment claims in multiple states or a Florida resident requesting unemployment benefits in California. Attack vectors can be identified across both federal benefit programs and federally funded, state-administered programs such as Department of Labor's Unemployment Insurance and Federal Emergency Management Agency's Individual Disaster Assistance.

Credential service providers should stand shoulder-to-shoulder with government agencies by assessing vulnerabilities, providing threat intelligence and warnings of attack vectors, and generating actionable insights on how fraudsters engage a specific agency. This support can enable agency leadership and law enforcement to take action to prevent fraud with minimal disruption of service to honest citizens. Any credential service provider working with the government must have a dedicated fraud and investigations team that can observe new attack vectors and dark web chatter to proactively identify and prevent attacks.



Identity theft tied
to government benefits
increased by
2,920%
year over year

Demonstrates a track record of fraud prevention

ID.me saw the consequences of inadequate security while protecting state unemployment benefits. ID.me repeatedly found dark web sources that successfully exploited knowledge-based verification and stolen identities using publicly available information.

Dark Web Chatter

April 06, 2021 | 10:44:00

Is someone who can help me with a method to find out DL numbers, or is a site like this I can card in?

April 06, 2021 | 11:29:00

Large data broker lookup, apply for a free trial with a fresh email ID from a new domain. They'll send an email asking to pick up their call and tell them about your business. If you can social engineer the staff and send them fake ID scans & docs, you'll be able to access their database.

February 08, 2021 | 01:05:05

-new logins for insurance agencies pulling DLs for any US driver. Not natgenagency. Lookups direct from large data broker \$500 account/lookups \$35

March 24, 2021 | 04:52:00

Method works for all 50 states, delivering data directly from large data broker
DL info: \$25 each (orders 40+ only)
Method and access: \$4k (selling in 2 hands)

The state of Arizona provides a strong example of a beneficial public-private partnership. The Arizona Department of Economic Security (DES) saw such high numbers of applications for Pandemic Unemployment Assistance (PUA) benefits that their systems became overwhelmed, creating an enormous backlog that precipitated a temporary halt to claims processing. A fraud analytics team found the vast majority of these claims were fraudulent due to identity theft.

Without a reliable method of verifying identity, Arizona risked sending billions of dollars to domestic and foreign cybercriminals. To counter the threat, Arizona partnered with ID.me to "gate" claims, requiring claimants verify their identity according to NIST 800-63-3 Identity Assurance Level 2 (IAL2) standards.

Over the next month, Arizona witnessed a 98.8% decrease in new claims attempted, a clear indication of fraud deterrence as identity thieves would rather abandon a state "gated" by ID.me than attempt to verify through the platform and leave a documented trail for investigators. Arizona achieved this without reducing access for legitimate claimants; in fact, many claimants who would have been blocked by legacy methods were able to efficiently gain access through the omni-channel solution. Arizona DES Director Michael Wisehart estimates that this approach saved the state at least \$75 billion in taxpayer dollars.¹⁸ A joint solution of NIST-compliant identity verification coupled with back-end fraud analytics is the most effective way to identify and prevent fraud. A best-in-class identity provider will be able to offer both in a single service.



- **Operates a risk-adaptive identity verification platform**
independently certified against the latest NIST and FedRAMP standards

Government agencies seeking to enable access to under-served demographics and prevent fraud should look for providers who can offer risk-adaptive identity proofing standards and a NIST-compliant platform. These options, as evidenced by Arizona's success halting pandemic unemployment insurance fraud, have proven effective in fraud prevention while increasing citizen access.¹⁹

The government should assess whether a provider meets these standards with the following criteria:

- ✓ **NIST compliance is assessed by the Kantara Initiative, Inc.**, an industry-recognized certifying body for Federal and Identity Credential Access Management Trust Framework Solution (FICAM TFS). Kantara accredits assessors and certifies credential service providers (CSPs).
- ✓ **Federal Risk and Authorization Management Program (FedRAMP), a General Services Administration (GSA) program** that ensures cloud software meets federal cybersecurity standards.

A credential service provider's identity proofing platform should be configurable to the identity assurance level required by each agency. For example, critical government benefits prone to fraud often require NIST IAL2/AAL2 with liveness and presentation attack detection, but other programs may require higher or lower levels of assurance based on an agency's unique risk assessment. If a credential service provider offers only one option, they are not equipped to handle identity proofing at scale with the network benefits of a shared service solution.



The National Institute of Standards and Technology (NIST), an agency of the United States Department of Commerce, publishes federal standards for identity proofing and authentication. See NIST Special Publication (SP) 800-63-2 and NIST SP 800-63-3.

Per Office of Management and Budget Memorandum 19-17, all federal agencies must deliver identity assurance and authentication services to the public in alignment with NIST SP 800-63 security and privacy requirements. Agencies are required to leverage existing credentials and identity federations that meet the agency's acceptable risk levels rather than standing up processes or capabilities to issue new credentials to users.



- **Shares the savings** from omni-channel offering network effects with the customer

An identity provider with citizen and consumer interests at heart will be willing to share savings directly with government agencies. There are two major sources of savings that a large, omni-channel digital identity network can enable for its customers:

1 Eliminate the need for labor-intensive activities (e.g. call centers). Federal agencies have already realized significant savings by offering omni-channel identity verification, as virtual-in-person offerings reduce reliance on expensive contact centers. A Government Accountability Office (GAO) report on the IRS from June 2018 asserts “in-person authentication at a Taxpayer Assistance Center is the most expensive way to authenticate taxpayers (about \$89 per interaction), followed by telephone (about \$54 per interaction).”²⁰ A video chat option, like what ID.me provides, verifies individuals for 80% lower cost than a call center. In-person proofing can now also be accomplished via NIST-approved commercial options for about 75-80% less than reported by GAO.

2 Federate digital identity credentials within a network. When a large portion of an agency’s user-base already possesses credentials issued by another agency or business, fewer new credentials need to be minted. For example, veterans who verify their identity to access the Department of Veterans Affairs through ID.me can then use their ID.me account to log in to another agency within ID.me’s network using just their username, password, and multifactor authentication. These veterans do not need to go through the initial identity proofing process at the second agency, streamlining customer experience and reducing costs.

This means agencies should be able to pay a small reuse cost instead of a larger initial-issuance cost. Government agencies should expect at least 15% of their user base to already have portable credentials, a number that increases where similar segments of the population interact (e.g., Department of Defense, Department of Veteran Affairs, Centers for Medicare and Medicaid Services, and State Departments of Health). The average member of ID.me’s network uses their credential to access the websites and services of three other distinct government agencies or businesses sites and services. These numbers will grow as a credential service provider’s network grows, meaning the savings will increase with larger networks.



Government agencies should expect their service providers to be able to generate these benefits and also be willing to pass them on to the sponsoring agency.



- **Supports rapid integration** via APIs and standard protocols — from vendor selection to “go-live” should be measured in days or weeks, not months



Available plug-and-play products eliminate the need for complex, in-house custom solutions. Digital identity providers should be on as many common open protocols as possible, including SAML 2.0, OAuth 2.0, and OIDC.

ID.me has found large-scale federal and state service offerings with millions of users can be onboarded and live within four to six weeks. Agencies don't have to navigate extended integration periods and bespoke software development to start increasing access and reducing fraud risk.

Additionally, government agencies and companies should expect their providers to scale across applications quickly through the use of APIs and white label brokerage capabilities.



- **Provides a 24/7/365**
customer support channel

An identity solution that offers both increased access and fraud prevention will need round-the-clock, 24/7/365 customer support. This ensures individuals have uninterrupted service, can conduct regular account updates, and can get help with any of the verification or authentication workflows. Robust customer support functions for a digital identity provider are key to increasing access and preventing fraud.

A philosophy of “No Identity Left Behind” should extend to all digital identity providers, which requires a commitment to customer support via video call, email, and live chat. Data brokers and credit bureaus struggle to offer responsive customer support – disputes and fixes for incorrect names or Social Security numbers take days and cost consumers hundreds of dollars.²¹ A strong customer service team can help reduce frustration, save time, and help all people to verify their identity and access government programs efficiently.

Customer support also helps with fraud prevention, such as reaching out proactively if an account shows signs of takeover, supporting the revivification of an individual if their account has been flagged for fraud signals, and documenting the tactics fraudsters are using. A best-in-class digital identity provider will offer support with these capabilities 24/7/365 and make it available via multiple channels, including but not limited to: email, chat bot, live chat with representative, and outbound phone.



ID.me has found that, depending on the government agency, **1 to 4% of members that access government services with a NIST credential will need some level of help in a given year.** Of these, about half are basic account maintenance and about half are related to fraud investigations. For the fraud investigations, many are precautionary measures taken to protect both individual accounts and the agency systems they are trying to access.

To further improve customer experience, providers can offer robust authentication capabilities that trigger account reverification as a way to prevent fraud, even when conducted by a legitimate individual with a valid verification. Signals from NIST 800-63-3 Authenticator Assurance Level 2 (AAL2), Identity Assurance Level 2 (IAL2), and Federation Assurance Level 2 (FAL2) should trigger notifications that individually or collectively may require account reverification. Providers should define and enforce rules to suspend and activate accounts individually or in bulk based on the circumstance.

Applying these best practices across use cases

The breadth of the pandemic unemployment insurance fraud has exposed vulnerabilities in many of the ways businesses, governments, and individuals interact online. However, it has also shown that requiring identity verification and enforcing the standards that exist today can achieve a win-win: eliminating fraud and increasing accessibility.

While these best practices were created during ID.me's work with state unemployment and access to federal benefits, there are many other uses across government including but not limited to:

- ✓ Access to Privacy Act records (e.g. OMB-21-04)
- ✓ Tax filing and claims
- ✓ Disaster relief assistance
- ✓ Insurance and compensation claims
- ✓ Pension access and guarantees
- ✓ Rental assistance programs
- ✓ Food assistance
- ✓ Fishing and hunting licenses
- ✓ Applications for healthcare benefits
- ✓ Access to healthcare data exchanges
- ✓ Pre-verifying for driver's license appointments



As pandemic-related unemployment winds down, fraud networks, inspired by their COVID successes, will be looking for their next opportunities. Action now will ensure that they don't succeed.

About ID.me

ID.me is fixing the digital identity layer for the internet by creating a trusted and portable digital ID. We believe that everyone should be able to participate in the digital economy safely, with minimal friction, and at the lowest cost possible. To fulfill this mission, we are committed to a philosophy of “No Identity Left Behind.” The approach involves two simple steps. First, we expand access to identity verification so communities that lack online access can verify through multiple channels. Second, make the verified login portable so people can seamlessly prove who they are at different websites with a single credential; the same way a Visa card streamlines payments.

In doing this, we are also making it harder for criminals to defraud government agencies.

The ID.me secure digital identity network has more than **66 million members with over 145,000 new subscribers joining daily**, as well as partnerships with **27 states, 10 federal agencies, and over 500 name-brand retailers**.

ID.me serves as a credential service provider and single sign-on login for state and federal agencies, including the Social Security Administration and the Department of Veterans Affairs. Companies in the healthcare and financial sectors use ID.me’s services to confirm that their users are who they say they are.



In addition to our verification offerings, we offer:

- ✔ **Group verification** (i.e., proof of affiliation with a group such as military or healthcare providers to gate access to everything from prescribing controlled substances online to discounts for nurses, first responders, and military).
- ✔ **Vaccine verification app** (i.e., a digital credential with the flexibility to support any organizational policy, including self-asserted status as well as uploaded documents).

Sources

- 1 Hajro, Neira, et al. What's next for Digital Consumers. McKinsey & Company, McKinsey & Company, 16 Aug. 2021, www.mckinsey.com/business-functions/mckinsey-digital/our-insights/whats-next-for-digital-consumers.
- 2 Salmon, Felix. A Deep Dive on the Astonishing Extent of Unemployment Fraud over the Course of the Pandemic. Axios 17 June 2021, www.axios.com/a-deep-dive-into-unemployment-fraud-027ba5a8-64b8-4fba-91e7-8ba84cd9edf0.html?deepdive=1.
- 3 Attorney General James Announces \$5.8 Million Multistate Settlement With LexisNexis." New York Attorney General Website, July 2, 2019, <https://ag.ny.gov/press-release/2019/attorney-general-james-announces-58-million-multi-state-settlement-lexisnexis>.
- 4 Cox, Joseph. "LexisNexis to Pay \$5 Million Class Action Settlement for Selling DMV Data." Vice, November 5, 2020, <https://www.vice.com/en/article/epddy4/lexisnexis-dmv-data-class-action-settlement>.
- 5 Spear and LexisNexis Risk Solutions team to expand and strengthen secure access to government agencies through the Login.gov Single Sign-On Solution. LexisNexis Risk Solutions. (n.d.). Retrieved October 12, 2021, from <https://risk.lexisnexis.com/about-us/press-room/press-release/20180912-single-sign-on>.
- 6 Holbrook, Alice. When LexisNexis Makes a Mistake, You Pay For It. Newsweek, 26 Sept. 2019, www.newsweek.com/2019/10/04/lexisnexis-mistake-data-insurance-costs-1460831.html.
- 7 Demographics of Mobile Device Ownership and Adoption in the United States. Pew Research Center: Internet, Science & Tech, Pew Research Center, 26 Apr. 2021, www.pewresearch.org/internet/fact-sheet/mobile/.
- 8 Internet/Broadband Fact Sheet. Pew Research Center. Available online as of April 7, 2021 at: <https://www.pewresearch.org/internet/fact-sheet/internet-broadband>.
- 9 Auxier, Brooke, et al. Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information. Pew Research Center: Internet, Science & Tech, Pew Research Center, 17 Aug. 2020, www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.
- 10 <https://www.nist.gov/blogs/cybersecurity-insights/breaking-news-new-privacy-pilot-federal-funding-opportunity>.
- 11 Some data related to NIST 800-63-63 credentials will be retained after account deletion solely for fraud prevention and government auditing purposes.
- 12 Cox, Joseph. LexisNexis to Pay \$5 Million Class Action Settlement for Selling DMV Data. Vice, November 5, 2020, <https://www.vice.com/en/article/epddy4/lexisnexis-dmv-data-class-action-settlement>.
- 13 Consumer Sentinel Network Annual Data Book. Federal Trade Commission. February 2021, https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf.
- 14 Person, and Paresh Dave. Factbox: States Using Id.me, RIVAL Identity Check Tools for Jobless Claims. Reuters, Thomson Reuters, 22 July 2021, www.reuters.com/business/states-using-idme-rival-identity-check-tools-jobless-claims-2021-07-22.
- 15 Bernard, Tara Siegel. Equifax Breach Affected 147 Million, but Most Sit Out Settlement. The New York Times, The New York Times, 23 Jan. 2020, www.nytimes.com/2020/01/22/business/equifax-breach-settlement.html.
- 16 Podkul, Cezary. How Unemployment Insurance Fraud Exploded during the Pandemic. ProPublica, www.propublica.org/article/how-unemployment-insurance-fraud-exploded-during-the-pandemic.
- 17 Waterman, S. (2021, September 1). White House recovery chief: Oversight key to beating ID fraud in government programs. SIGNAL Magazine. Retrieved October 2, 2021, from <https://www.afcea.org/content/white-house-recovery-chief-oversight-key-beating-id-fraud-government-programs>.
- 18 Arizona DES. Arizona Prevents More Than \$75 Billion in Unemployment Benefit Fraud. Arizona DES Report, September 30, 2021. <https://spark.adobe.com/page/A31Y9mEGah5Ea/>.
- 19 Arizona DES. Arizona Prevents More Than \$75 Billion in Unemployment Benefit Fraud. Arizona DES Report, September 30, 2021. <https://spark.adobe.com/page/A31Y9mEGah5Ea/>.
- 20 GAO-18-418, Identity Theft: IRS Needs to Strengthen Taxpayer Authentication Efforts. <https://www.gao.gov/pdf/product/692712>.
- 21 Holbrook, Alice. When LexisNexis Makes a Mistake, You Pay For It. Newsweek, 26 Sept. 2019, www.newsweek.com/2019/10/04/lexisnexis-mistake-data-insurance-costs-1460831.html.