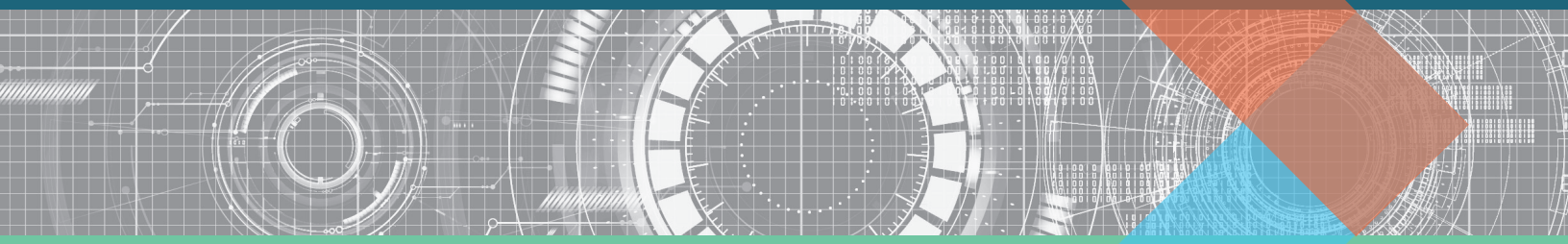
BETTER IDENTITY COALITION



# Better Identity in America:

## A Blueprint for State Policymakers

## ABOUT THE BETTER IDENTITY COALITION

The Better Identity Coalition is an organization focused on developing and advancing consensus-driven, cross-sector policy solutions that promote the development and adoption of better solutions for identity verification and authentication.

The Coalition was launched in 2018 as an initiative of the Center for Cybersecurity Policy & Law, a non-profit dedicated to promoting education and collaboration with policymakers on policies related to cybersecurity. Members of the Better Identity Coalition are recognized leaders from different sectors of the economy, encompassing firms in financial services, health care, technology, telecommunications, fintech, payments, and security. Our 27 members include AT&T, CVS, Discover, Early Warning, Equifax, Experian, Facetec, Fidelity, ID.me, IDEMIA, JPMorgan Chase & Co., LexisNexis, MassMutual, Mastercard, Microsoft, Norton LifeLock, Notarize, Okta, OneSpan, Onfido, PNC Bank, Ping Identity, TransUnion, Uniken, US Bank, Wells Fargo, and Yubico.

As the government contemplates new policies to improve the quality of digital identity in the United States, the Better Identity Coalition is bringing together leading companies to help develop innovative ideas that improve security, privacy, and convenience for all Americans.

More on the Coalition can be found at https://www.betteridentity.org/ or by contacting info@betteridentity.org.

# TABLE OF CONTENTS

## EXECUTIVE SUMMARY

**Today, the variety of services available online is greater than ever before, offering consumers the power to engage in all sorts of transactions from a device in the palm of their hand. But conversely, the ability of businesses and governments to offer high-value transactions and services online is being tested more than ever, due in large part to the challenges of proving identity online**.

The inadequacies of the nation's digital identity infrastructure have enabled cybercriminals to steal billions of dollars and created major barriers for Americans trying to obtain critical benefits and services. These issues were only exacerbated during the COVID pandemic – and even as the impacts of the pandemic wane, the challenges posed by increased criminal attacks on identity systems remain.

The lack of a widely adopted easy, secure, reliable way for entities to verify identities or attributes of people they are dealing with online creates friction in commerce, leads to increased fraud and theft, degrades privacy, and hinders the availability of many services online. While the market has responded with an array of products that aim to address the identity challenge for specific use cases, the tools available today are uneven in terms of accuracy and reliability, don't work well for everyone, and are increasingly coming under attack.

More than $56 billion was stolen as a result of identity fraud in 2020 - an increase of 333% over 2017 numbers.[1] State governments were heavily targeted in attacks to steal pandemic relief dollars, but the private sector was hammered as well; the Identity Theft Resource Center reported that data breaches grew 23% from 2020 to 2021, with breaches impacting more than 293 million people.[2]

As the number of impacted Americans grows, consumers need better identity solutions that empower them to decide what information they share, when they share it, and in what context.

The members of the Better Identity Coalition came together in 2018 to create a set of consensus, cross-sector, technology-agnostic policy recommendations for improving identity in America. The "Policy Blueprint"[3] we published in 2018 outlined a detailed action plan for the Federal government to take to improve identity in America. This paper is intended to serve as a companion piece to that Blueprint – focused on the vital role that states play.

Here there is good news: State governments are perfectly positioned to lead the way in solving these problems! Our recommendations do not purport to solve every challenge in the identity space. Rather, we have focused on a handful of common-sense initiatives that are practical for states to implement and will be meaningful in their impact; the State Policy Blueprint we put forth in this document is squarely focused on making identity systems work better.

**Our Blueprint for State Policymakers contains six key initiatives:**

1) **Place the Department of Motor Vehicles (DMV) at the center of state digital identity solutions.** Adversaries have caught up with the systems America has used for remote identity proofing and verification. The DMV – as the one government entity where nearly every adult goes through a robust, in-person identity verification process – is ideally positioned to address this problem. States should modernize legacy identity systems and embrace new privacy-protecting mobile Driver's License (mDL) solutions that empower residents to protect themselves from identity theft in the digital world.

2) **Establish attribute validation services at vital records bureaus to support next-generation, consumer-centric remote identity proofing and verification systems.** Next to DMVs, vital records bureaus are the most important agencies in the state identity ecosystem. In their role of issuing birth certificates, marriage certificates, and death certificates, vital records bureaus are on the front line of identity, and often have foundational information that can be used to validate identities.

3) **Embrace identity innovation for better services.** States need to embrace new technologies to enable a broader array of services for constituents. Specifically, states should pass Remote Online Notarization (RON) laws that would enable a secure, standard approach to virtual notarization services. Additionally, states can complement mDL and other government-based attribute validation services with commercial identity tools that are certified as meeting rigorous NIST standards.

4) **Make sure identity works for everybody.** While state DMVs are the logical starting point for most residents, they don't work for everybody. Roughly ten percent of adults do not have a driver's license or state ID, and in many cases, people lack critical identity documents like birth certificates and Social Security cards needed to get one. This disproportionately impacts the most marginalized communities, including people of color, the elderly, the poor, as well as survivors of domestic violence and those reentering society after time in prison. As states invest in new digital identity tools, they should also invest in services to ensure that their most vulnerable residents are not left behind.

5) **Promote and prioritize the use of strong authentication.** Passwords continue to provide the attack vector in the majority of breaches and cyber incidents, and some legacy tools used for multi-factor authentication (MFA) are coming under attack as well. State governments should adopt strong phishing-resistant authentication as well as the use of electronic signatures, and update legacy policies that create barriers to the adoption of strong authentication solutions.

6) **Do no harm.** Some states have passed security and privacy legislation that has inadvertently precluded use of some identity security technologies, or mandated non-standard approaches to identity verification or authentication that put government, business, and residents at risk. In many cases, these have been driven by sincere efforts to protect residents but have ended up creating risks that are far greater than the things legislators intended to guard against. States should leverage digital identity standards published by the National Institute of Standards and Technology (NIST) rather than create requirements for new, one-off approaches. Additionally, states should consult with security and identity experts when crafting new policies to ensure they do not inadvertently create new mandates that make things worse.

Note that there are no "moonshot" items in this Blueprint. This is by design: history has shown that lofty identity initiatives which aim to solve every problem struggle to get traction, given their complexity and difficulty. Instead, we have focused on a set of proposals that are both significant in impact and achievable – should state governments choose to act on them – in the next two to three years.

## I. INTRODUCTION

**The ability to offer high-value transactions and services online is being tested more than ever, due in large part to the challenges of proving identity online. The lack of a widely adopted easy, secure, reliable way for both government and private entities to verify identities of people they are dealing with online creates friction in commerce, leads to increased fraud and theft, degrades privacy, and hinders the availability of many services.**

The pandemic made it clear: that there is no longer a question of **if** states have to act to improve digital identity – only **how** they should do it. Consensus on a policy framework to enable better identity solutions has been difficult to establish, given the complexity of the issues at hand, as well as the extensive – but inadequate – legacy infrastructure in place.

While concerns about security and fraud have elevated identity, the issues at play also touch on privacy and consumer empowerment, as well as development of better trust models that can enable government and commercial organizations to offer new types of high-value online services to a wider swath of Americans. When done right, identity can be "the great enabler" – helping to drive innovation and new, better ways of delivering services, while improving privacy, security, and user experiences.

When done right, identity can be "the great enabler" – helping to drive innovation and new, better ways of delivering services, while improving privacy, security, and user experiences.

In 2018, the members of the Better Identity Coalition came together to create consensus, cross-sector policy recommendations for improving identity in America. Our 2018 publication "Better Identity in America: A Blueprint for Policymakers" outlined key recommendations for the Federal government that would make identity systems work better. Since its publication, the Blueprint has won wide bipartisan support, and led to the introduction of bipartisan legislation in the U.S. Congress that would implement many of its recommendations.[4]

### This new paper specifically focuses on the role that State governments can play in improving digital identity for their residents.

Our recommendations – presented in this paper – do not purport to solve every challenge in the identity space. Rather, we have focused on a handful of common-sense initiatives that are practical to implement and will be meaningful in their impact; the Policy Blueprint we put forth in this document is squarely focused on making identity systems work better.

### History of identity in the United States (or "Where we are and how we got there")

Americans are not legally required to obtain a driver's license, Social Security number (SSN), or any other identity credential. To be clear, for all purposes nearly every American needs to get a credential, since some sort of government-issued identity document is required to open a bank account, get a job, pay taxes, receive government benefits, drive a car, board a plane or purchase alcohol. However, if someone does not need to do any of those things, there is no law that requires them to get an ID.

While the U.S. has long rejected efforts to create a national identity, lack of such an ID does not mean that the U.S. does not have a government-backed identity system. Instead, a patchwork system has emerged of identifiers and credentials issued by a variety of different Federal, state, and local entities, including DMVs, vital records bureaus, the Social Security Administration, and the State Department. This patchwork has worked relatively well for in-person transactions where it was important to verify someone's identity; service providers could simply ask to see someone's credentials. However, the model has fallen apart online.

Nothing quite captured the extent of this challenge in the digital age like Pete Steiner's famous 1993 New Yorker cartoon; in 2022, it still perfectly describes our challenges with addressing identity online.


*"On the Internet, nobody knows you're a dog."*

While in some cases anonymity or pseudonymity online (being a "dog") is appropriate or desirable, there are many cases where individuals, agencies, and businesses want or need to be able to definitively prove identity online. In these cases, our legacy systems have struggled; Americans remain dependent on paper and plastic-based identity credentials, none of which were designed to be easily used or validated online.

Instead, we have relied on systems where knowledge of identity data – someone's name, birthdate, Social Security number, address, or credit data – has been presumed to mean that the individual holding that data must be that person. Unfortunately, years of massive data breaches have resulted in all of this data being readily available online. As attackers have caught up with these legacy systems, their use looks like attempts to ignore the elephant in the room: that government alone confers identity authoritatively, and that government is thus in a strong position to address the challenges we have today and make identity better.

Not by issuing a national ID – but by enabling consumers to ask government to stand behind the paper and plastic credentials it already issues in the physical world.

### The COVID-19 pandemic exacerbated existing problems in our digital infrastructure

The arrival of the pandemic meant that state DMVs, unemployment agencies, licensing agencies, and state Medicaid programs could no longer welcome residents into government offices to conduct in-person transactions – and not all transactions could easily be transitioned online.

The rapid creation and rollout of the Pandemic Unemployment Assistance (PUA) program and other pandemic relief programs required states to establish online application processes for millions of Americans; in many states, these processes allowed organized criminals to exploit weak identity verification systems based on knowledge factor to steal billions of dollars. The Federal Trade Commission (FTC) reported an astounding 2920% increase in identity theft reports tied to government benefits.[5] During a U.S. Senate Committee hearing on Pandemic Response and Accountability, the U.S. Department of Labor estimated fraud tied to pandemic response could be as high as $163 billion.[6]

While the final fraud numbers are not yet known, the message is clear: **massive amounts of money were stolen from the government by organized crime, and non-existent or inadequate identity systems provided the attack vector that enabled it to happen.**

Governments were not the only victims here. Outside of fraud, there are stories of thousands of Americans who were unable to get the unemployment benefits they needed and rightfully deserved because they were unable to prove who they were online. In some cases, those same people have been getting 1099-G tax forms detailing the taxes they owe on Unemployment Insurance benefits that a criminal claimed before them – adding insult to injury.

In the private sector, identity theft and fraud skyrocketed as well, as the same organized criminals who were exploiting weak identity proofing systems in government exploited similarly weak systems used by industry.

**Bottom line: adversaries have caught up with America's first-generation approaches to digital identity, in a way that inhibits access, fuels fraud, and erodes trust. Identity solutions need to evolve and improve.**

### Industry filled the gap – but attackers have caught up

Industry has responded over the years by providing solutions in compliance with the Digital Identity Guidelines that NIST sets to fill the "identity gap" in the U.S. Initially, industry digital identity proofing solutions relied largely on Knowledge-Based Verification (KBV), which relied on a subject's ability to answer questions that were presumably secret – and thus answerable only by the individual being asked the question – in order to verify that someone was who they claimed to be and not a proverbial "dog on the Internet."[7]

While these solutions were helpful for several years, they also became targets of attack for adversaries. Their goal has been simple: steal identity data in order to aggregate and analyze it – and then turn it against systems that used knowledge of personal data as a means of protection. For this reason, NIST has advised agencies not to rely solely on KBV for remote identity proofing; many states found when they used KBV in the early days of the pandemic, attackers were able to answer the questions the system teed up using information stolen in previous breaches.[8]

Better Identity Coalition members also have seen stepped-up attacks on these knowledge-based systems and learned that merely answering the questions correctly cannot guarantee authenticity; one financial institution commented that if someone correctly answers a knowledge-based quiz too quickly or accurately, it is a signal that they might be dealing with an attack from a "bot" rather than a real human being. Criminals have caught up with America's first-generation approaches to digital identity, in a way that inhibits commerce, fuels fraud, and erodes trust.

Industry continues to innovate, and today newer solutions that use artificial intelligence, biometrics, and machine learning to augment some of the legacy knowledge-based tools. While these new solutions can offer better performance – and, indeed, in the near term, they represent the best tools available for government and industry – America is currently dependent on solutions that try to guess what only the government truly knows. In this next phase of improving digital identity, government needs to play a more direct role.

## Identity by the Numbers: The Cost of Outdated Solutions

- **$56 billion** stolen as a result of identity fraud in 2020 – up 333% since 2017
- **293 million** people impacted by data breaches in 2021 – a year in which reported breaches grew 23%
- **$20 billion** lost to synthetic identity fraud in 2020
- **61%** of 2020 breaches exploited identity as an attack vector – using weak or stolen passwords to access systems and steal data
- **2920%** – the increase in identity theft reports to the FTC tied to government benefits
- The pandemic saw a spike in government document and benefits fraud from almost 6,000 reported cases in Q1 in 2020 to a spike of 273,000 a year later in Q1 2021.
- **39 million** victims of identity fraud scams in 2020
- **1.25 million** children fell victim to identity theft and fraud in 2021, costing the average affected family more than $1,100
- **$8.64** million is the average cost of a breach recovery
- **$35.2 billion** spent by financial institutions to comply with Anti Money Laundering (AML, Know Your Customer (KYC), and other identity-related compliance requirements.
- **49%** of Americans under 40 are more concerned about fraud now than pre-COVID-19

## II. BETTER IDENTITY IN AMERICA: A VISION OF THE FUTURE

While digital identity in America is fraught with problems, they are not unsolvable. On the contrary, many of the most glaring problems in digital identity are ones that can be addressed through active partnerships between the public and private sectors.

Before defining a plan of action, however, it is important to first lay out a high-level vision of what "Better" means. Collectively, we believe that Better Identity in America means that the following outcomes have been achieved:

**a. Better Security – Less Fraud and Identity Theft** – embracing the recommendation of the Commission on Enhancing National Cybersecurity to eliminate identity as a major attack vector.[9]

**b. Better Convenience** – enabling consumers to open new accounts with ease, without having to go through duplicative, burdensome enrollment processes where they have to duplicate the experience they went through at the DMV.

**c. Better Confidence for Consumers, Service Providers, and Government Agencies** – that identities asserted online are reliable and trustworthy, and that they work well for everyone.

**d. Better Privacy** – shifting the predominant model for identity verification from one based on firms aggregating personal data without opt-in consent to one where consumers proactively request that their government-held data be shared for the sole purpose of verifying identity.

## III. BETTER IDENTITY: HOW STATES CAN GET THERE

At the core of our recommendations is the belief that the private sector will not be able to solve America's identity challenges on its own. We are at a juncture where state governments will need to step up and play a bigger role to help address critical vulnerabilities in the new "digital identity fabric."

**Our Blueprint for State Policymakers contains six key initiatives:**

1. **Place the DMV at the center of state digital identity solutions**
2. **Establish attribute validation services at vital records bureaus to support next-generation, consumer-centric remote identity proofing and verification systems**
3. **Embrace identity innovation for better services**
4. **Make sure identity works for everybody**
5. **Promote and prioritize the use of strong authentication**
6. **Do no harm**

## 1. Place the DMV at the center of state digital identity solutions

It's a rite of passage. A 16-year-old goes to their state driver license issuer, hands over a birth certificate, Social Security card, and other documents, takes a written test and driving test and then receives that ubiquitous piece of plastic that they use for so many purposes other than driving. Roughly once a decade that same individual will revisit that office to renew that license and get an updated picture. This is one of the few instances where a resident goes somewhere in person, hands over documentation that is validated and verified, and is then given an identification document.

This in-person identity proofing for a document that most U.S. residents (89%) have sets it apart from every other credential in the U.S.[8] And for in-person transactions such as buying a beer, opening a bank account, or applying for a government service, the driver's license enables people to prove who they are. But there is no way for people to "reuse" that identity online. Instead, almost every time consumers apply for a new account online, they are asked to go through a new process to prove who they are again.

**Here is where states are ideally positioned to help: by deploying new mobile Driver's License (mDL) apps and other digital identity services that create a digital counterpart to the plastic cards they issue today.**

Issuing mDLs will enable states to close the "identity gap" between physical and digital ID and empower their residents with a new tool that gives them greater security, better protects their privacy, and is easy to use. With mDLs, states can give every resident a tool that enables a state to "vouch" for them when they are trying to prove who they are online – by validating the information from their driver license.

Congress has already recognized the promise of mDLs; the *REAL ID Modernization Act*, passed in 2020, makes clear that a driver's license can be a physical or a digital credential – and ensures that any mDL issued in accordance with Federal standards will be accepted by the Federal government for REAL ID purposes.[11]

If states had an mDL program in place at the start of the COVID-19 pandemic, officials could have leveraged the millions of state-backed identity proofing processes residents had already gone through at its DMV offices to validate the identities of most applicants for unemployment benefits.

The security and privacy benefits of mDLs are significant. Today when someone hands over their driver's license, all of the information can be seen, captured, and stored. However, mDLs, in comparison, allows a consumer to select only information that is relevant to the transaction. For example, someone trying to buy alcohol can prove they are over 21 without sharing their birthday or address. The retailer selling alcohol also can know with certainty that the information is accurate.

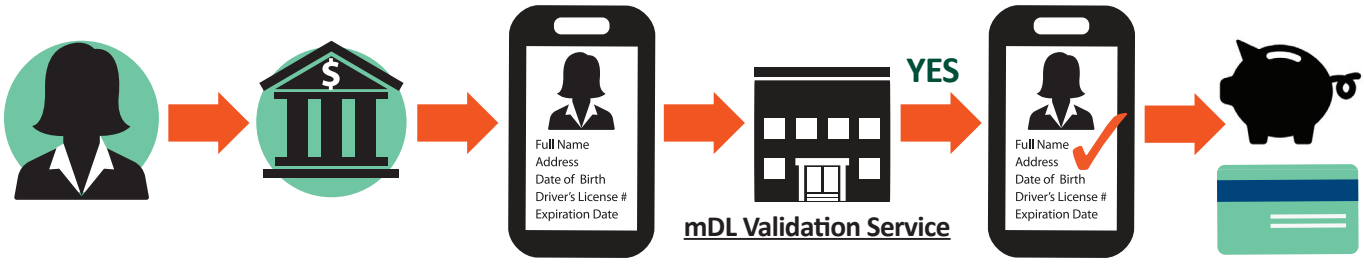
### Prioritize remote identity mDL use cases over in-person

Much of the international standards work around mDLs has revolved around enabling in-person use cases – such as letting someone use their phone instead of their driver's license when going through an airport security checkpoint or entering a bar. These are "nice to have" use cases but viewed against the backdrop of an explosion of massive identity fraud in online applications, they should be a second-tier priority.

By prioritizing mDL solutions that address the inability of organizations to easily and securely identity proof consumers online, states can address the most critical shortcoming in America's digital identity infrastructure and stop billions of dollars in identity-related cybercrime and fraud each year.

This is not to diminish the importance of mDL standards, like ISO 18013-5, which currently focus on in-person use cases – the TSA and others have said they will not accept mDLs that do not adhere to this standard, and thus states should embrace it in any mDL offering. However, states need to focus first on ways that mDL initiatives can address online identity fraud and identity proofing challenges.

**Here is how this idea could work for Stacey – a consumer opening a bank account online:**




**Stacey goes to bank website to open a new account**

**Bank website requests identification information**

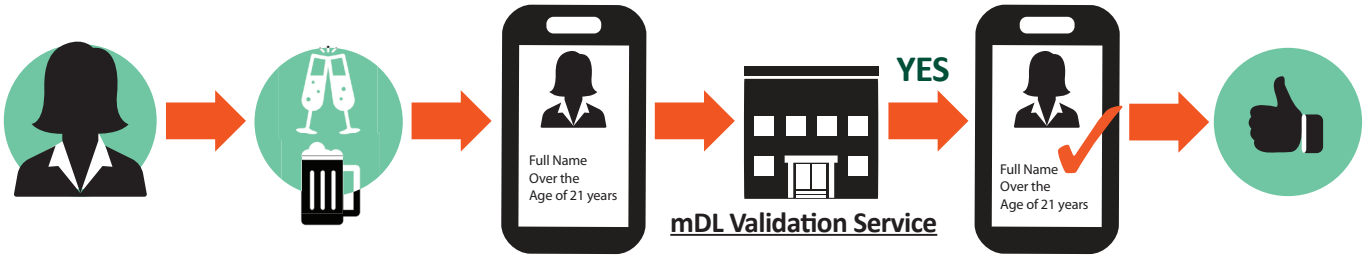
**Stacey asserts only the necessary attributes from her mDL, in this example, omitting height and weight**

**Information is validated by authorized organization**

**Confirmation is sent back to the bank**

**Accounts are opened**

**Here is how this idea could work when Stacey purchases age-restricted products online:**




**Stacey goes to website to purchase alcohol**

**Website requests identification information**

**Stacey asserts the necessary attributes from her mDL, in this case photo, name, and that she is of legal age - Photo is necessary to confirm the person receiving the order is who placed it**

**mDL digital signature is validated by the issuing authority**

**Confirmation is sent back to the website**

**Purchase completed**

A number of states such as Arizona, Maryland, Florida, Connecticut, Iowa, Kentucky, Oklahoma, Colorado, and Utah have already started to move forward with mDLs, but rollout and adoption has been slow.

**Complement mDLs with new attribute validation services.**

While mDL deployment will take time, in the near term, states can make a material difference in improving remote identity proofing solutions by launching identity attribute validation services that enable consumers to ask the DMV to validate whether identity data submitted matches what an agency has on file when they are trying to prove their identity.

Attribute validation services represent an easy lift for DMVs, in large part because the DMV does not have to share any personal information through the service. Instead, a DMV need only provide a "Yes/No" answer as to whether identity data provided to another agency or business to open a new account matches what the DMV has on record. This is another meaningful way, in addition to mDLs, that states can enable DMVs to vouch for residents when they are trying to prove who they are online.

For the attribute verification services states do not need to create these new systems themselves: today the American Association of Motor Vehicle Administrators (AAMVA) administers the Driver's License Data Verification (DLDV) system, which provides a single tool that public agencies and third parties can use to confirm DMV data. A core challenge with DLDV is full participation by all states. Without this there's a notable gap in the utility of DLDV, since service providers need a system that covers the entire country, rather than just certain states.

Without full participation of all jurisdictions many organizations will still need to have various fallback services in order to serve all U.S. residents. This will result in a varied user experience depending on where one lives and potentially varying security requirements.

Governors and state legislatures of states that are not fully participating in DLDV – New York, California, Louisiana, Alabama, Alaska, and South Carolina – should take action to join their counterparts. This would enable DLDV to be used widely and effectively across the public and private sector to deliver more accurate identity proofing and guard against identity fraud.

With this, states should also look to establish new identity validation services that allow a consumer to electronically request that the state which issued their driver's license validate (with a Yes/No answer) whether a "selfie" image that the consumer takes matches the driver's license image on file in the state DMV. This validation service would effectively let a third party determine whether a remote user in possession of a driver's license is who they claim to be – rather than someone who might have stolen a license.

Such a service could help enable higher-assurance identity proofing and also help to alleviate concerns about accuracy and bias issues in some current products that match selfies to a lower-quality photo obtained by having a consumer take a picture of their driver's license. That said, it will be important to architect these new systems to ensure that they only use matching algorithms that have been proven in third-party testing to be both accurate and equitable, and that also ensures selfies are not retained by the state.

### ACTION ITEMS

***Governors and state legislatures should jumpstart the deployment of mDLs in their states by:***

1) Directing their DMV directors to create a plan for launching mDLs.
2) Considering restructuring the DMV to separate the identity division from the motor vehicle division – enabling a tighter focus on the challenges of digital identity and implementing mDLs.
3) Exploring whether new legislation is needed to authorize the use of mDLs – and if so, passing it.
4) Prioritizing online use cases of mDLs over in-person applications – to ensure that the most urgent needs for digital identity are addressed first.
5) Implementing driver license attribute validation services that enable state residents to verify their identity with the state DMV – ideally by fully participating in the American Association of Motor Vehicle Administrator's Driver's License Data Verification (DLDV) service.
6) Educating consumers and businesses in their state about mDLs and how they can be used.

## 2. Establish attribute validation services at vital records bureaus to support next-generation, consumer-centric remote identity proofing and verification systems

Next to DMVs, vital records bureaus in states, cities, and counties are the most important agencies in the state identity ecosystem. In their role of issuing birth certificates, marriage certificates, and death certificates, vital records bureaus are on the front line of identity, and often have critical information that can be used to validate foundational identity information.

Unfortunately, many of these bureaus are stuck in the paper world and there is no way for their data to be used to support identity proofing events online. So long as these systems are limited to paper, they will not be able to support next-generation remote identity proofing and verification systems.

State vital records bureaus should join DMVs in launching new digital services for attribute validation - enabling consumers to ask an agency to validate whether identity data submitted matches what an agency has on file when

they are trying to prove their identity. The National Association for Public Health Statistics and Information Systems (NAPHSIS) introduced the Electronic Verification of Vital Events (EVVE) service that enables federal and state agencies to verify birth and death certificate information. However, access to the service is largely limited to government agencies, with little to no ability for non-governmental entities to use it.

By launching similar programs that tie to state vital records bureaus, states can create additional "levers" for ensuring that more people are able to prove who they are online.

### ACTION ITEMS

***Governors and state legislatures should jumpstart the deployment of consent-based identity attribute validation services in their states by:***

1) Directing vital records bureaus to create a plan for launching attribute validation services.
2) Exploring whether new legislation is needed to authorize the use of attribute validation services – and if so, passing it.
3) Educating consumers and businesses in their state about attribute validation services and how they can be used.

## 3. Embrace identity innovation for better services

mDLs and attribute verification services are critical to enabling access to services but there are other steps states can take to also drive identity innovation.

**First, states can complement mDL and other solutions with commercial identity tools that are certified as meeting rigorous NIST standards.**

While mDLs should be a top priority, there is no question that it will take time to roll them out in the states. In addition, some people may not want to get an mDL – or will not have a smartphone or other tools needed to use one. And as noted earlier, about 10% of adult Americans do not have a driver's license today. Alternative solutions will be needed.

Here, states can complement DMV-centric solutions with commercial identity solutions that have been certified as meeting digital identity guidelines published by the National Institute for Standards and Technology (NIST). Specifically, solutions that meet "Identity Assurance Level 2" (IAL2) as defined by NIST are able to deliver an alternative to government-crafted solutions, while still delivering on security and privacy.

**Second, states should embrace innovation when it comes to notarization by passing new Remote Online Notarization laws that enable a secure, standardized approach to virtual notarization.**

In the United States, notarization - an official authentication certification process provided by a notary public - has provided trust in documents and transactions for centuries. Today, notarization remains a critical process in verifying the identity of a signer, providing assurance that a signature is genuine, and an acknowledgment that a signer understands a document's contents.

Traditionally an in-person process, notarization was transformed in 2012, when the Commonwealth of Virginia became the first in the nation to bring notarization into the online world using the process of Remote Online

Notarization (RON). RON is a modern form of notarization that enables a user to have a document notarized entirely online using audio-video technology, identity proofing tools, and electronic documents and storage.

While COVID-19 increased the demand for remote transactions generally, the demand for RON skyrocketed in 2020 and 2021, helping to propel the industry and laws surrounding online notarization forward. Available today to signers in all 50 states through interstate recognition, RON has been permanently authorized to be performed by notaries in 41 states as of the publication of this report. As we continue to transition into a fully online world, making RON available to the notaries across all 50 states will empower notaries across the country to utilize this important digital service and help modernize our nation's digital infrastructure from coast to coast.

The common components of RON include identity proofing, and the use of audio-visual technologies. Identity proofing is typically done via KBV and credential analysis and then identity is verified during the audio-visual session during the transaction. Additionally, the audio and video of every signing session are recorded and retained so that if a question were to arise about a transaction, the recording could be reviewed.

## ACTION ITEMS

***Governors and state legislatures should:***

1) Pass remote online notarization (RON) laws to expand convenient and secure remote transactions and avoid passing remote ink notarization (RIN) laws due to the reliance on outdated practices and failure to provide adequate safeguards.
2) Ensure that RON laws embrace a common standard and framework, such as NIST's Digital Identity Guidelines, to deliver a policy framework for RON that is technology-neutral and avoids prescriptive technology requirements, enabling upgrades over time.
3) Complement mDL and other government attribute-exchange services with commercial identity tools that are certified as meeting rigorous NIST standards.

## Improving Identity While Preserving Privacy

Better Identity in America must deliver Better Privacy - shifting the predominant model for identity verification to one that is consent based rather than one based on firms aggregating personal data without consent.

Against that backdrop - it is important to note that the history of government identity systems, privacy and personal data has not always been a happy one. In 1994, Congress passed the Driver's Privacy Protection Act (DPPA) after issues arose with some state DMVs failing to properly protect personal information - leading, among other things, to a murder after a stalker obtained his victim's home address from a state DMV. The DPPA places strict limitations on who can access DMV data, and under what circumstances. This enables DMVs to share data if the subject consents - meaning that the use case described above with mDLs would be permitted.

That said, new identity proofing solutions like mDLs backed by state DMVs must be architected to protect privacy, not risk it. Beyond potential harm to individuals, protecting privacy is essential to gaining the trust of consumers to use these new solutions. The mDL standard (ISO 18013-5) accounts for privacy and should be followed closely. Accordingly, following the mDL standard will help states ensure they are crafted with a "privacy by design" approach. That means:

"New identity proofing solutions like mDLs backed by state DMVs must be architected to protect privacy, not risk it."

- Privacy implications are considered up front at the start of the design cycle -- and protections are embedded into the solution architecture.
- Identity data is shared only when consumers request it.
- Identity data that is shared is only used for the purpose specified.
- Consumers can release information at a granular level enabling selective disclosure.
- Relying parties may only request attributes that are necessary to process the transaction.
- Relying parties only receive match/no-match, Y/N responses – such as age verification services that share that someone is over 21 but does not share their birthday.
- Identity providers deploy measures to prevent mDL holders from being tracked across relying parties

A privacy-preserving architecture is critical for achieving mDL adoption. Accordingly, we believe the model should support full consumer control of the information they share with a relying party whether it be a governmental or commercial entity. In any mDL implementation, state DMVs should not be sharing or transmitting data. Rather, their role should be limited to issuing digitally signed credentials that individuals can use to share their data, as well as in some cases, "vouching" for individuals by validating whether data submitted matches what is in the DMV database (i.e., providing a match/no match response).

## 4. Make sure identity works for everybody

As states invest in new digital identity systems, it is important to make sure that these new systems are accessible to all their residents – and that some populations are not excluded or left behind.

So many basic necessities – getting a job, a bank account or housing – are inaccessible to those who lack "foundational" identity documents. One downside of the increased security requirements of the REAL ID Act has been that many Americans cannot easily get a driver's license, because they cannot produce or access the multiple documents, such as birth certificates or Social Security cards, needed to prove who they are. . This disproportionately impacts the most marginalized communities, including people of color, the elderly, the poor, as well as survivors of domestic violence and those reentering society after time in prison.[12]

In many states, the only option for someone "stuck" in a situation where they do not have foundational identity documents is to turn to charities and other non-profits for assistance. These groups do some inspiring work – the I.D. Ministry operated by Foundry United Methodist Church in Washington D.C. is one example – but it should not fall entirely to charities and churches to address gaps in government identity systems that exclude some Americans.

Here, states can help – by shifting policies in DMVs and vital records bureaus so that someone who lacks all the required documents is not just told "Come back when you have them" but also asked "Do you need assistance in getting them?" Americans should not have to seek out help from a church or a charity to get a service that is inherently governmental; states should look to lead the way in ensuring that their residents can get assistance if they somehow get stuck in the system.

The benefits of helping people here go beyond the "do good" aspects; economists forecast that U.S. GDP could grow an extra 4% by 2030 with investments in robust digital identity infrastructure.[13] But those benefits will only fully accrue if everyone can access "Digital First" identity infrastructure that they can use in banking, health care, retail, and government services to protect the security and privacy of their information and enables them to access more high value, trusted services online.

### ACTION ITEMS

***Governors and state legislatures should:***

1) Direct the DMV, vital records bureaus, or other agencies to create services that help those residents on the margins of society if they struggle to get foundational identity documents. This may be done directly through a government agency, or by partnering with third parties that provide this assistance.
2) When designing new physical or digital identity systems, consider ways to ensure that they are accessible to all, no matter someone's age, income, or ability.

## 5. Promote and prioritize the use of strong authentication

There is no such thing as a "secure" password in 2022, and even some widely used multi-factor authentication (MFA) tools such as those that use one-time passcodes (OTPs), or push notifications are now easily compromised through automated phishing attacks.[14] Any authentication tool that is based on "shared secrets" can be easily defeated by adversaries. 2020 saw a 450% increase in username and password breaches with 1.48 billion breached records.[16] Additionally, 61% of breaches in 2020 were conducted using compromised credentials.[16]

States should move both their enterprise and citizen-facing services to stronger forms of authentication, based on multiple factors to prevent these common attacks.

The good news here is that industry and government have recognized the problems with old authenticators and multi-stakeholder efforts like the Fast Identity Online (FIDO) Alliance and the World Wide Web Consortium (W3C) have developed standards for next-generation authentication that are embedded in most devices, operating systems, and browsers, and enhance security, privacy, and user experience. The Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) has called FIDO "the gold standard of multi-factor authentication" and the White House has required the use of phishing-resistant MFA in both enterprise and citizen-facing services, calling out the FIDO and W3C standards.[17]

In addition, we've seen the emergence of technology that can deliver continuous risk-based authentication – analyzing data from dozens of data points to create a "risk score" that determines how much and what access to provide.[18] State governments should continue work already underway in promoting this strong authentication technology that is already used in financial services, health care, government, and consumer applications.

A risk-based approach is critical to ensuring that digital applications deliver the right level of strong authentication. Both government and industry should look to leverage risk- based guidance such as NIST's Digital Identity Guidelines (SP 800-63-3), which lays out a comprehensive approach to assessing risk and selecting appropriate authentication controls to address those risks. Many commercial authentication products are built to align with NIST guidelines, enabling states to avoid creating custom solutions here.

An important consideration for policymakers when crafting new legislation or regulation on privacy and security is to make sure that new rules are not written so broadly that they might preclude use of promising technologies for risk-based identity proofing and authentication. For example, while Europe's General Data Protection Regulation (GDPR) limits the collection of data in many circumstances, it also highlights that in protecting security and preventing fraud, there are cases where an entity may have a "legitimate interest" in processing personal data – including cases where such data can be used to deliver secure authentication.[19]

Likewise, the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA)[20] create exceptions for requirements to delete personal information about a consumer if that information: "is necessary for the business or service provider to maintain the consumer's personal information in order to ... detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity."

However, if states were to pass laws that applied a different standard to data use for secure authentication and preventing fraud, it could have a chilling effect on the market. Companies would then have to grapple with a variety of laws across 50 states with each having different definitions, standards, and requirements for security and fraud prevention. Such a patchwork approach would inhibit the deployment of new, innovative authentication technologies and place consumers at risk.

## ACTION ITEMS

***Governors and state legislatures should:***

1) Ensure agencies enable phishing-resistant MFA for individuals accessing services online, as well as consider the use of risk-based analytics authentication tools used by financial services, health care, and other private sector organizations.

2) Ensure their states avoid creating restrictions on use of data that might preclude use of technologies for risk- based authentication that can assure security and prevent fraud.

## 6. Do no harm

As detailed in this Blueprint, when done right, identity can be "the great enabler" – helping to drive innovation and new, better ways of delivering services, while improving privacy, security, and user experiences.

However, there are also plenty of ways that digital identity systems can be implemented poorly, in ways that create new security challenges, erode privacy and civil liberties, make things harder for people online, or exacerbate existing inequities.

The recommendations in this Policy Blueprint are carefully crafted to drive the former outcomes – and help states avoid the latter. That said, this Blueprint does not address every challenge in digital identity, and states will need to be thoughtful in their approaches to different issues.

There are three aspects of "do no harm."

1) **First, make sure that any new digital identity system is architected to be secure, protect the privacy of those who are using it, and is easily used by the vast majority of individuals.**

   As this paper has discussed, it is important that states be thoughtful and intentional as they design any new identity system to maximize the benefits while avoiding unintentional consequences.

2) **States should follow NIST standards wherever practical to ensure they set a high bar for security, privacy, and interoperability.**

   When it comes to digital identity, the Federal government has invested more than 15 years and millions of dollars in creating standards and guidance. NIST's Digital Identity Guidelines outline a risk-based approach for both government agencies and private sector entities to select appropriate security controls for identity and authentication; the guidance is widely recognized across the globe and even cited by other governments, who defer to NIST standards rather than craft their own.

   NIST standards are also crafted in concert with security and privacy community stakeholders, ensuring that they reflect critical input from a wide array of experts.

   A number of states have made well-intentioned attempts to try to create their own standards, products, or requirements for how public and private entities in their state should handle identity proofing or authentication. For the most part, these efforts have fallen short, and in some cases, had the impact of mandating weak or outdated solutions.

   For example, a number of states have mandated identity verification approaches that require the use of KBV, despite NIST and many security experts pointing out how attackers have caught up with it. California is the most notable here; as we detail in a sidebar, their new regulations tied to the state's recently-passed privacy laws call for KBV to be used to validate the identities of people seeking access to their data – despite security studies showing this will put some people at risk.

   Likewise, some states continue to cling to outdated requirements for things like password complexity that may make their systems – and their citizens – more vulnerable.

One advantage of using NIST guidance is that it is updated every few years to reflect both evolutions in attack vectors, as well as innovations in industry that guard against them. Thus, by referencing NIST Digital Identity Guidelines in state laws and regulations – rather than legislating or regulating their own approach – a state can be assured that their security requirements automatically evolve over time, without a need for the state to update laws or regulations.

**3) Finally, legislators and policy makers should not ban any identity technology outright, but instead focus on crafting policies to govern the use of technology responsibly.**

Across the U.S. there are numerous proposals to ban the use of facial recognition biometrics. There is a reason this has been happening: in some cases, governments have misused facial recognition systems, leading to horror stories where people have been wrongly arrested. Moreover, NIST has documented that some second-tier biometric algorithms have difficulty identifying women and people of color.

What is getting lost in many of these discussions is that all face recognition applications don't present the same risks; nor is every algorithm "biased;" in fact, NIST has stated that "those algorithms that are the most equitable also rank among the most accurate."[21]

Moreover, while we are very concerned about surveillance applications using face recognition, there are some applications of face biometrics that have been proven to be helpful to people of color. For example, a 19-year-old African American woman with no credit history would have a good chance of failing to pass a remote identity verification solution that relied on KBV questions tied to a credit report. However, if she had a driver's license and a smartphone, she could take a picture of that license and then a selfie, and the remote verification system could then match the selfie to the photo on the license – allowing her to quickly open an account and obtain the services she needs.

Such a use case is dependent on the use of a "best in class" algorithm that meets NIST's requirement for being "most equitable and most accurate." And it is also dependent on the solutions being designed to mitigate risks by architecting solutions up front to set a high bar for equity, privacy, and security.

We have seen a number of instances where the press or policymakers have inappropriately conflated issues tied to one application of face recognition with another – for example, suggesting that problems associated with surveillance applications mean that face recognition should not be used on someone's smartphone. It will be important for policymakers to ensure that any polices around the use of biometrics technology are appropriately targeted to specific applications and the specific risks or harms associated with those applications, rather than apply blanket bans on the use of technology in any circumstances.

As part of a focus on "do no harm," we note that there should always be backup options for those who cannot or choose to use a system that incorporates face biometrics as part of applying for a government service. Identity solutions need to meet people where they are comfortable; while biometrics can be a valuable option for many people, they should not be the only option; multiple paths to prove identity should be made available.

## ACTION ITEMS

***Governors and state legislatures should:***

1) Look first to NIST and ISO identity standards and guidelines – and only seek to craft their own if they have clearly determined that those existing standards and guidelines cannot address a state's requirements.

2) Consult with security and identity experts when crafting new policies to ensure they do not inadvertently create new mandates that make things worse.

3) Avoid blanket "bans" on use of identity technologies like face recognition; instead, target polices limiting the use of biometrics technology to specific applications and the specific risks or harms associated with those applications.

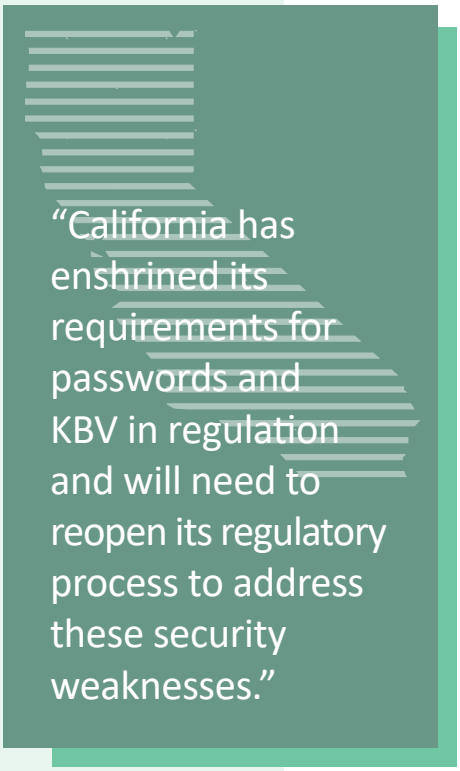
## Poorly crafted identity policies can put consumers and businesses at risk.

One example of where a state has made a well-intentioned – but poorly crafted – attempt to create its own digital identity requirements is in California, where new regulations around the California Consumer Privacy Act (CCPA) may inadvertently put residents and business at risk.

CCPA enables residents the right to access, correct or delete their data, which is an important tool to enable consumers to have control over their data. To do so, residents would undergo identity proofing and then create an account with the organization to request the information.

A core challenge with enabling someone to request their data: if the company or organization receiving that request is not using adequate controls to verify the identity of the requestor, then criminals are almost certain to use this as an attack point to steal that data.

This is a well-known attack vector that has already been a problem in Europe in the wake of GDPR: A 2019 Blackhat presentation entitled GDPArrrrr: Using Privacy Laws to Steal Identities, detailed how an adversary could exploit GDPR's new "Right of Access" to gain unauthorized access to a consumer's data. In the paper, the two co-authors teamed up, with one of them posing as the other in making requests to 150 companies. In total, 40% of the companies shared personal data with the impersonator without any strong identity verification.[22]




The CCPA and CPRA regulations, unfortunately, may open up California residents and businesses to similar attacks:

> *For accounts where a business has a password protected account with a consumer, the regulations say businesses need only verify the password before sharing all of their data – despite ample documentation that passwords are frequently compromised and that passwords alone do not provide sufficient security to protect someone's personal data.*

> *For accounts where a consumer either does not have a password-protected account – or claims they have forgotten their password – the regulations say businesses should match "at least three pieces of personal information" – essentially a very weak version of KBV that is unlikely to stop most cybercriminals.*

By relying on NIST's Digital Identity Guidelines instead of looking to create its own approach to identity verification and authentication, California could have better protected its residents and businesses from identity-centric attacks. Moreover, pointing to NIST guidelines would ensure that California would stay ahead of new identity-centric attacks, given that these guidelines are updated regularly. As things stand, California has enshrined its requirements for passwords and KBV in regulation and will need to reopen its regulatory process to address these security weaknesses.

## IV. NEXT STEPS: A CALL TO ACTION

### States face a clear choice:

States can sit back and fail to modernize identity policies and watch identity-related cybercrime and fraud get worse as legacy solutions continue to fail – steps that will likely create additional barriers to the availability of services online and erode trust.

Or states can take a proactive approach and take action to get ahead of the identity conundrum – a step that will allow the U.S. to address security challenges and enable the growth of new digital products.

This Blueprint for State Policymakers lays out a clear set of policy initiatives for states that are both significant in impact and achievable in the next two to three years.

State governors and legislators should each move to advance the initiatives outlined in this Blueprint, with an eye toward turning identity into the great enabler and driving trusted digital service delivery, to enhance security, privacy, equity, convenience, and innovation.

## STATE ACTION PLAN: A PATH TO BETTER IDENTITY

**1. Place the Department of Motor Vehicles (DMV) at the center of state digital identity solutions.** Adversaries have caught up with the systems America has used for remote identity proofing and verification. The DMV – as the one government entity where nearly every adult goes through a robust, in-person identity verification process – is ideally positioned to address this problem. States should modernize legacy identity systems around a privacy-protecting, consumer-centric model that empowers residents to ask a state that issued a credential to stand behind it in the digital world – by validating the information from the credential. States should:

### ACTION ITEMS

**1)** Launch new mDL apps that create a digital counterpart to the traditional physical credential – letting people "reuse" the process they went through at the DMV when they need to prove who they are online.

**2)** Create new digital services at the DMV to validate identity attributes – allowing consumers to ask the DMV to provide a "yes/no" answer to third parties as to whether identity data submitted matches what an agency has on file when they are trying to prove their identity. The easiest way to do this is for states to fully participate in AAMVA's DLDV.

**2. Establish attribute validation services at vital record bureaus to support next-generation remote identity proofing and verification systems.** Along with DMVs, state vital records bureaus should also launch new digital services for attribute validation services - enabling consumers to ask an agency to validate whether identity data submitted matches what an agency has on file when they are trying to prove their identity.

### ACTION ITEMS

**1)** Directing vital records bureaus to create a plan for launching attribute validation services.

**2)** Exploring whether new legislation is needed to authorize the use of attribute validation services – and if so, passing it.

**3)** Educating consumers and businesses in their state about attribute validation services and how they can be used.

**3. Embrace identity innovation to improve access to services.** States need to embrace new technologies to enable a broader array of services for constituents.

### ACTION ITEMS

**1)** Specifically, states should pass Remote Online Notarization laws that would enable a secure, standard approach to virtual notarization services.

**2)** States can complement mDL and other government solutions with commercial identity tools that are certified as meeting rigorous NIST standards.

**4. Make sure identity works for everybody.** While state DMVs are the logical starting point for most residents, they don't work for everybody. One out of ten adults in does not have a driver's license or state ID, and in many cases, people lack critical identity documents like birth certificates and Social Security cards needed to get one. This particularly impacts the elderly, the poor, as well as survivors of domestic violence and those reentering society after time in prison. As states invest in new digital identity tools, it is critical that their most vulnerable residents are not left behind.

**ACTION ITEMS**

1) Direct the DMV, vital records bureaus, or other agencies to create services that help those residents on the margins of society if they struggle to get foundational identity documents. This may be done directly through a government agency, or by partnering with third parties that provide this assistance.
2) When designing new physical or digital identity systems, consider ways to ensure that they are accessible to all, no matter someone's age, income, or ability.

**5. Promote and prioritize the use of strong authentication.** Passwords continue to provide the attack vector in the majority of breaches and cyber incidents, and some legacy tools used for multi-factor authentication (MFA) are coming under attack as well. State governments should promote strong phishing-resistant authentication as well as the use of electronic signatures, and update legacy policies that create barriers to their adoption.

**ACTION ITEMS**

1) States should enable phishing-resistant MFA for individuals accessing services online, as well as consider the use of risk-based analytics authentication tools used by financial services, health care, and other private sector organizations.
2) States should avoid creating restrictions on use of data that might preclude use of technologies for risk-based authentication that can assure security and prevent fraud.

**6. Do no harm.** Some states have passed security and privacy legislation that has inadvertently precluded use of some identity security technologies, or mandated non-standard approaches to identity verification or authentication that put government, business, and residents at risk. In many cases, these have been driven by sincere efforts to protect residents but have ended up creating risks that are far greater than the things legislators intended to guard against. States should:

**ACTION ITEMS**

1) Leverage digital identity standards published by NIST, which typically align with the ISO rather than create requirements for new, one-off approaches.
2) Consult with security and identity experts when crafting new policies to ensure they do not inadvertently create new mandates that make things worse.

## ENDNOTES

[1]https://www.ftc.gov/news-events/news/press-releases/2022/02/new-data-shows-ftc-received-28-million-fraud-reports-consumers-2021-0

[2]https://www.idtheftcenter.org/publication/identity-theft-the-aftermath-study/

[3]https://www.betteridentity.org/s/Better_Identity_CoalitionBlueprint-July2018.pdf

[4]https://foster.house.gov/media/press-releases/foster-katko-langevin-loudermilk-introduce-bipartisan-digital-identity

[5]https://www.acfeinsights.com/acfe-insights/overview-federal-trade-commission-2020-consumer-reports#:~:text=Credit%20card%20fraud%20had%20consistently,%25%2C%20as%20compared%20to%202019.

[6]https://www.hsgac.senate.gov/imo/media/doc/Testimony-Turner-2022-03-17-REVISED.pdf

[7]https://pages.nist.gov/800-63-3/sp800-63a.html

[8]https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf

[9]https://www.nist.gov/cybercommission

[10]https://hedgescompany.com/blog/2018/10/number-of-licensed-drivers-usa/#:~:text=on%20this%20page.-,What%20percentage%20of%20American%20adults%20have%20a%20driver's%20license,than%2026%20million%20licensed%20drivers.

[11]https://www.dhs.gov/real-id/news/2020/12/28/dhs-modernizes-critical-identification-requirements-after-congress-passes

[12]The challenges many people face in getting basic ID credentials – and the consequences of what happens when they do not – was detailed at https://www.washingtonpost.com/lifestyle/magazine/what-happens-to-people-who-cant-prove-who-they-are/2017/06/14/fc0aaca2-4215-11e7-adba-394ee67a7582_story.html

[13]https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth

[14]https://www.vice.com/en/article/y3vz5k/booming-underground-market-bots-2fa-otp-paypal-amazon-bank-apple-venmo

[15]2021 ForgeRock Consumer Identity Breach Report

[16]Verizon Data Breach Investigation Report

[17]https://www.cisa.gov/mfa

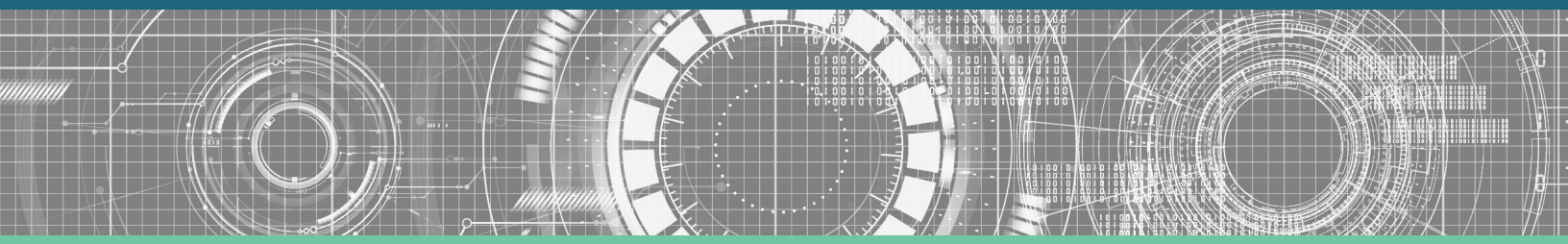
[18]https://zerotrust.cyber.gov/federal-zero-trust-strategy/#identity

[19]See GDPR Recitals 47 and 49 at https://eur-lex.europa.eu/legal-content/EN/TxT/PDF/?uri=CELEx:32016R0679&from=EN

[20]See https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

[21]See https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

[22]https://i.blackhat.com/USA-19/Thursday/us-19-Pavur-GDPArrrrr-Using-Privacy-Laws-To-Steal-Identities-wp.pdf



https://www.betteridentity.org