Department of Administrative Services

Innovate Ohio Platform

Teaching Old Dogs a New Trick for Digital Identity Verification

How the State of Ohio implemented machine learning and behavioral biometrics to catch fraudsters *before* they commit crime

Contact

Katrina Flory

State Chief Information Officer
Department of Administrative Services,
State of Ohio

katrina.flory@das.ohio.gov

Project Dates

06/16/2023 - 01/26/2024

State

Ohio

Agency

Administrative Services

Category

Cybersecurity

"We aren't just adding an online option to an in-person process. We're rethinking digital service delivery to make sure it's inclusive, accessible, and secure for all Ohioans."

- **Katrina Flory**, *State of Ohio Chief Information Officer*

Executive Summary

Cybersecurity tops the list of "2024 Priorities" for State CIOs – and not for the first time. This burgeoning era of artificial intelligence (AI) brings with it new threats – *and new tools*. Both private and public sectors are investing heavily in behavioral biometrics, predictive analytics, and machine learning to beat cybercriminals at their own game. To stay ahead of the curve, we need to leverage cutting-edge technology. State government is called to provide the public with world-class cybersecurity in a way that is equitable, adaptive, automated, and fiscally responsible.

A three-phase project recently implemented by the Ohio Department of Administrative Services' (DAS) InnovateOhio Platform (IOP) could offer other states a potential model in their pursuit of peak security operation and cyber resiliency. Over a six-month period, IOP and vendor-partners from Deloitte and Socure integrated inclusive technology, a strong variety of data, including biometric data, and machine learning to verify a user's digital identity quickly and accurately, detect emerging fraud patterns, and halt fraudulent account creation and takeovers. The goal of this cybersecurity project, ultimately, is to drive statewide adoption of a trusted, verified digital identity to expand access to digital state services and programs.

The Complicated History of 'Dogs on the Internet'

In the early 1990s, internet service providers like America Online (AOL), brought the internet into our homes and commercial web browsers, like Netscape Navigator, made it easier than ever to access. Digital identity verification wasn't on the radar back then. Online interactions were centered around email, chat rooms, and resource sharing. Many online interactions were anonymous, or in today's parlance, unverified, because there wasn't much need for it yet. This was a double-edged sword, as it turned out, because on the internet, you could be almost anyone. Or vice versa.

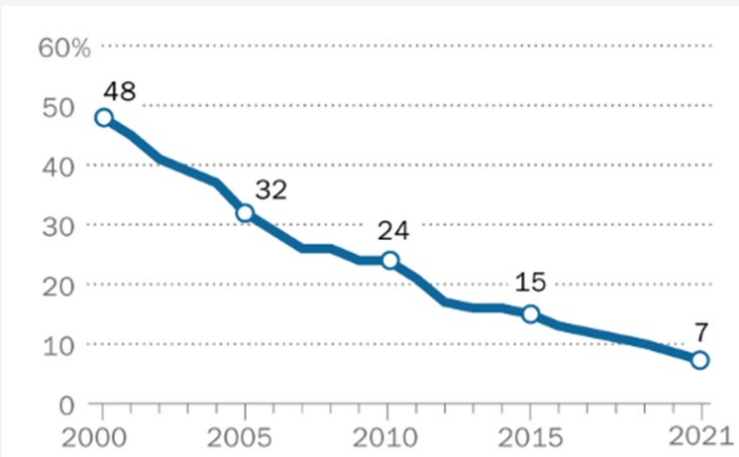
New Millennium, New Internet

By the mid-aughts "Google" is a verb, "like" is a noun, and Peter Steiner's cartoon is now a popular meme. The rise of tech giants and e-commerce led to a proliferation of personal and financial data on the internet. Yet, many accounts had only basic cybersecurity protection – a username and password – which most of us used and reused across our personal and professional accounts. Cybercriminals took advantage, stealing and selling unfathomable quantities of data.

The *Washington Post* reconnected with Steiner just after the 20th anniversary of his now-iconic "Internet Dogs" cartoon. They asked him about the unexpected relevancy and longevity of his joke, turned idiom, turned cybersecurity wisdom to protect ourselves from identity theft and fraud. "It's as true as it ever was," he said. "The internet is so ubiquitous, so ever-present in our lives that now – unlike a dog here or a dog there – it's become … a huge, baying pack of hounds that won't shut up." [1] By 2020, estimates indicated more than 15 billion stolen account credentials had been leaked on the dark web – the result of 100,000 separate data breaches. [2]

Offline Population has Declined Substantially Since 2000

% of U.S. adults who say they do not use the internet



Above: "7% of Americans don't use the internet. Who are they?" April 2021. Pew Research Center. pewresearch.org/short-reads

1. "NOBODY KNOWS YOU'RE A DOG: As Iconic Internet Cartoon Turns 20 Creator Peter Steiner Knows The Joke Rings As Relevant As Ever" by Michael Cavna. July 2013.washingtonpost.com/blogs/comic-riffs/post/nobody-knows-youre-a-dog-as-iconic-internet-cartoon-turns-20-creator-peter-steiner-knows-the-joke-rings-as-relevant-as-ever/2013/07/31
2. "New Dark Web Audit Reveals 15 Billion Stolen Logins From 100,000 Breaches" by Davey Winder. Forbes. July 2020. forbes.com/sites/daveywinder/2020/07/08/new-dark-web-audit-reveals-15-billion-stolen-logins-from-100000-breaches-passwords-hackers-cybercrime

Still, staggering amounts of our personal data live online. And you can't say we've gotten much better at prioritizing cyber hygiene. A 2024 survey ahead of National Password Awareness Month found that 84 percent of people reuse their passwords across online accounts. [3] Unfortunately, research by Verizon (itself a recent victim of a major data breach) confirms weak or stolen **passwords were the point of entry for 80 percent of 2023 data breaches** related to hacking.[4] Even with mainstream adoption of multifactor authentication (MFA), the data in accounts isn't necessarily safe. With so much leaked and stolen PII available for purchase, common forms of knowledge-based MFA are not as effective as they once were.

Simply put, **there are too many dogs on the internet** who can answer tricky questions about a person's loan records, personal history, and educational background. Better digital identity verification and access controls continue to be a top security priority across the board. It was critical for the State of Ohio to reimagine how it conceptualizes and verifies digital identity for its most valuable resource: Ohioans.

Idea

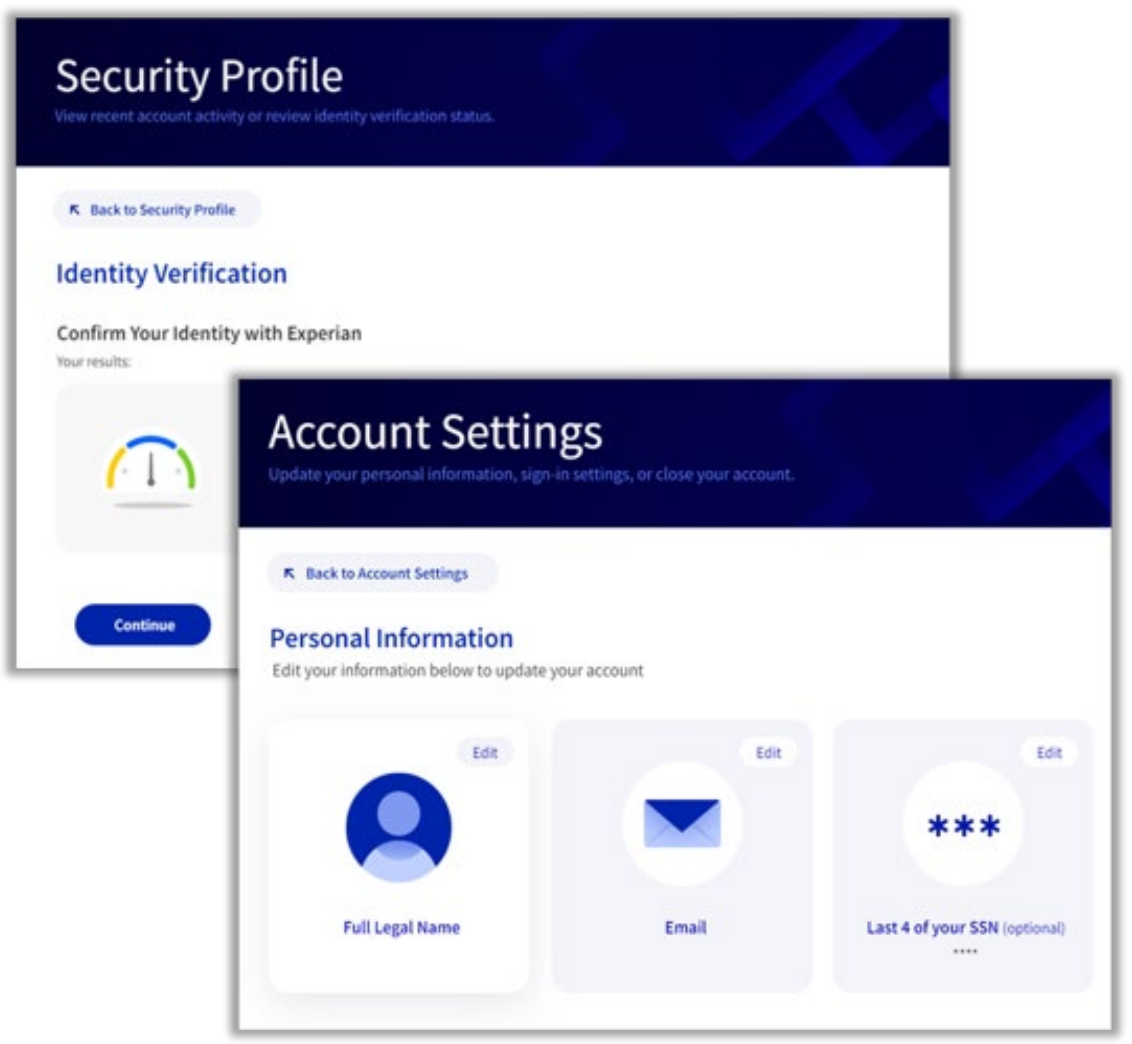
"Digital identity is the representation of who someone is in an online ecosystem and a critical extension of their legal or physical identity." - **Jordan Burris**, *former Federal Chief Information Officer* [5]

Balancing ease of access and cybersecurity – freedom and safety – has always been a moving target. In 2019, Governor Mike DeWine established the InnovateOhio Platform (IOP) by executive order to make state government an effective and efficient leader in using technology to improve customer service and save tax dollars. One of DAS IOP's first public product offerings was the OHID, a statewide digital identity for Ohioans and businesses to simplify and secure online access to state agency services. Today, OHID securely provides 5.3 million Ohioans (and the full state government workforce) with access to more than 1,200 agency applications and counting. But accurately verifying digital identify is not a one-and-done process. It takes a lot of work to get it right.

In early 2021, OHID began offering agencies the ability to leverage MFA and Experian identity proofing services to safeguard access to secure apps and data. On an app-by-app level, agencies could require users to verify their OHID account by passing a knowledge-based ID proofing quiz. These industry-best safeguards enabled IOP to weather the cyberattacks that became common during the pandemic. However, after onboarding several popular state programs and several million users, it became clear that Experian's heavy reliance on financial data was producing too many inconclusive results.

Two things were happening. Fraudsters were purchasing consumer data on the dark web and using it to pass ID proofing quizzes and take over OHID accounts. At the same time, Ohioans with limited or complex credit and financial histories were experiencing lower than average acceptance rates.

IOP knew it was essential to develop a holistic, data-centric approach to fraud detection and prevention by analyzing traditional and non-traditional aspects of a user's digital identity.



Above: OHID offers users multiple ways to secure their account.

3. World Password Day 2024 – Password Tips and Best Practices" by Steve Alder. May 2024. hipaajournal.com/world-password-day

4. "2023 Data Breach Investigations Report: frequency and cost of social engineering attacks skyrocket" by Verizon. June 2023. verizon.com/about/news/2023-data-breach-investigations-report

5. "Getting Digital Identity Right. The digital identity challenge for governments arrives at a time when threat actors are relentless" by Socure. June 2023. govtech.com/sponsored/getting-digital-identity-right

Implementation

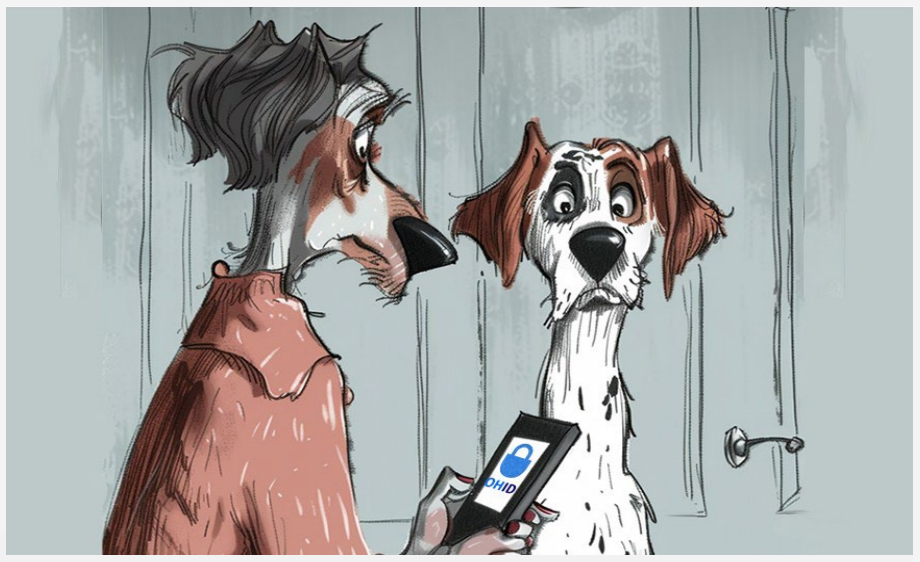
"Identity data can't be only financial. A lot of folks don't have a long credit history, so we learned we needed to look at other data sources." - **Remard Colston**, *InnovateOhio Platform Administrator*

During the 2023-2024 fiscal year, DAS IOP fulfilled a much sought-after need: increasing the security and resilience of the popular OHID platform. The three-phase rollout included integrating a new vendor, Socure, to block automated bot attacks and spam account creation and enhancing the identity proofing options available to OHID users.

Phase 1 prevented mass-creation of spam OHID accounts by bots and bad actors with the intent to exploit state agency programs and services. OHID wanted to secure the "front door" of the Platform from automated attacks. But it needed to be done without impacting the account opening experience for real people. To accomplish this, OHID implemented a security check during account opening that is invisible to the end user. Socure Device Risk and Email Risk uses machine learning to cross-references a plethora of email and device-specific variables and data sources to calculate a comprehensive risk score for the email address and device being used in real time. If a new user's risk score is too high, the system prevents them from creating a new account. This phase was intended to bring bot-driven account creation to a halt. With the front door closed on bot-activity, the team shifted focus to verifying the digital identity of OHID users.

OHID Increased its ID Proofing Accuracy by Analyzing New Data Sources

In Phase 2, the project team added Socure Digital Identity Verification to the OHID architecture and security framework.



"Remember how, before biometrics and behavioral analytics, you could hack peoples' accounts with leaked PII and a bot script?"

IOP could now leverage a stronger and more inclusive combination of data sources, like phone number history, address history, email account history, and real-time data from the device. This opened the door to assessing a user's identity without relying solely on credit history and financial data, which vastly reduced, but could not fully eliminate, the number of times Ohioans were referred to state agencies for manual ID verification.

Phase 3 added quick and accurate remote document verification to our ID Proofing process**.** However, the standard identity proofing process is still not foolproof. Some people's identities are hard to verify online, even when they are legitimate. Knowing this, IOP turned to another identity verification service provided by Socure: Document Verification (DocV). The tool verifies a person's identity by using AI to compare a live selfie to a valid government-issued identification. Both images are uploaded by the user and passed through a series of security checks in real time. These checks include the use of optical character recognition data and machine-readable zones (MRZ) to analyze and match "liveness" biometric data against the provided government-issued ID.

State agencies with secure digital services could leverage DocV to decrease the cost of digital identity verification by reducing the frequency of in-person document reviews by state employees. Additionally, users who successfully complete ID Proofing, either via the standard process or DocV, can then request access to secured applications enterprise-wide. This provided a cost-effective alternative to conducting in-person, manual document verification to positively identify someone.

DAS IOP partnered with the Ohio Department of Job and Family Services and the Ohio Department of Public Safety Bureau of Motor Vehicles to supply crucial user data that influenced project requirements and the overall user experience, making the journey as smooth as possible by automating redirects from the agency website to OHID identity proofing and back to the agency website.

With approval from state agency stakeholders, the project team was able to implement Socure DocV with a security logic that was custom-tailored for Ohio and Ohioans. To ensure a successful rollout, DAS IOP employed human-centered organizational change management practices to develop training materials and instructional job aids for support teams at the DAS Customer Service Center and respective agencies.

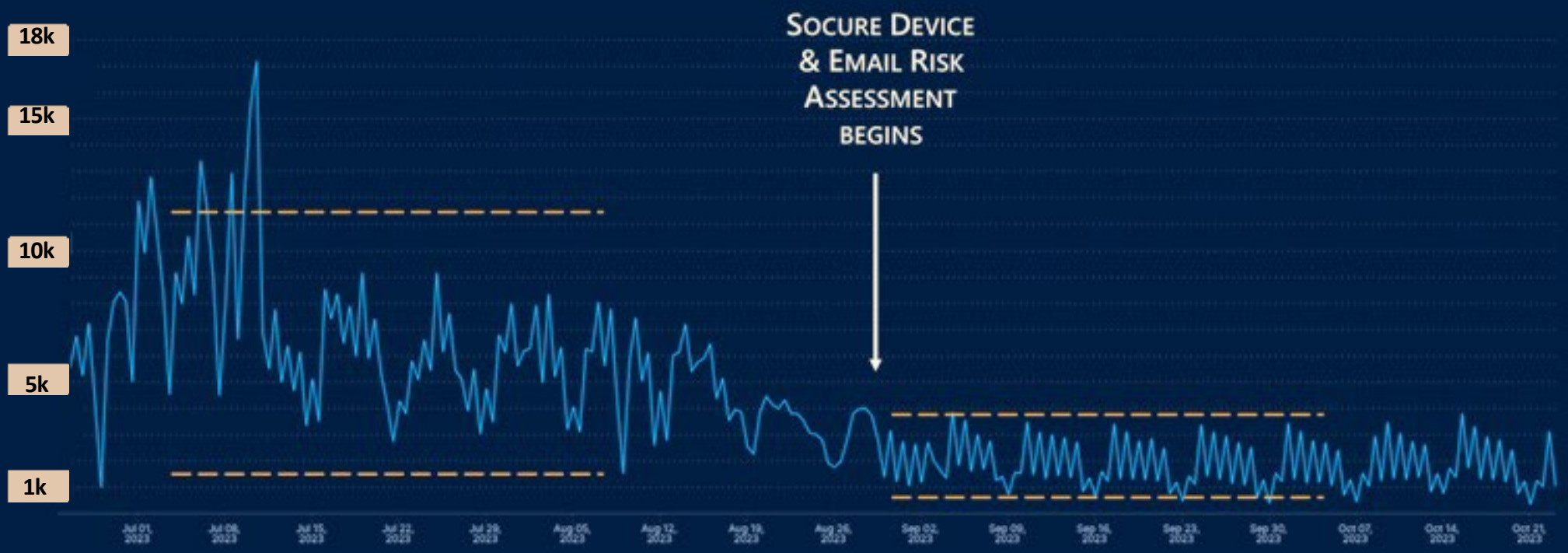
Impact

"Data is critical to having a resilient cybersecurity response, and so the quality and variety of your data sources is paramount." - **Holly Drake**, *Chief Information Security, State of Ohio*

Working alongside vendor partners, IOP developed a three-phase approach to target cyberattacks and malicious actors without negatively impacting the customer experience. With Socure identity verification and machine learning, IOP can more effectively detect and prevent fraudulent OHID account creation and malicious account takeover. IOP can also detect and block established fraud patterns, as well as identify newly emerging patterns. What's more, by regularly reviewing feedback from state agencies and data collected by Socure, IOP is fine-tuning its algorithms over time, ensuring that OHID account protection remains nimble and effective within our ever-changing threat-landscape.

Phase 1: Shut the Front Door on Fraud

Prior to Phase 1, daily OHID account creation varied from 1,000 to 17,000, largely due to bot-activity and malicious cyberactivity. Today, the daily average for new OHID accounts is around 4,500.



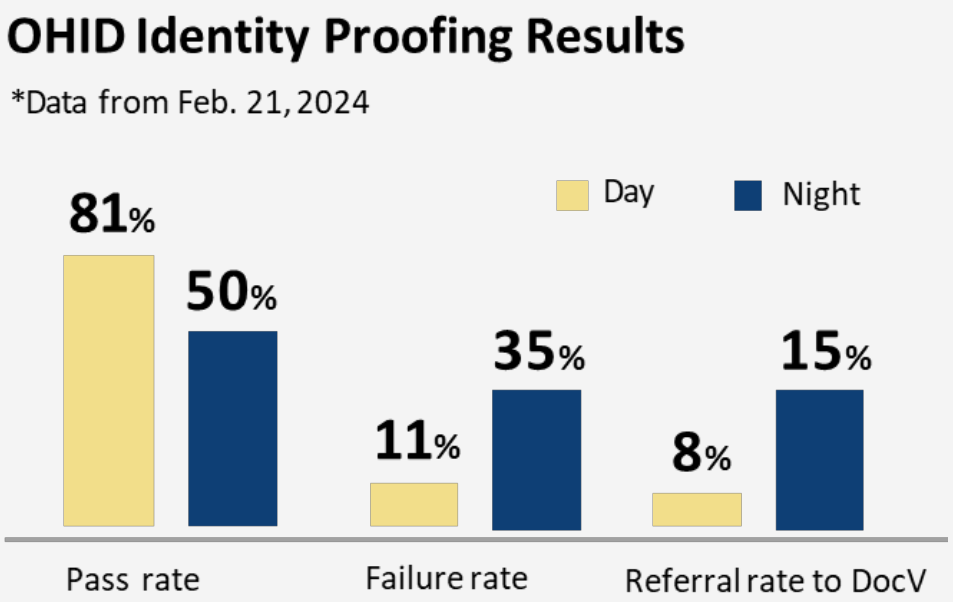
Innovate Ohio Platform

Until mid-2023, daily OHID account creation varied from 1,000 to 17,000 due to bots and other malicious actors who would create spam accounts they could use to apply for state services. The daily average for new OHID accounts holds steady at around 4,500 today after implementing an invisible security check to the new account flow that analyzed real-time data about each user's email and device they were using. By working with Socure to implement email and device risk assessment logic, IOP succeeded in minimizing bot–activity, nearly halting the creation of fake accounts.

Immediately after Phase 1 launched, a visible and cyclical OHID account creation pattern emerged. New account opening peaks on weekdays, during business hours, and plateaus overnight and on the weekend. This is consistent with normal user activity and human account creation.

Phase 2: Strong Data Variety Improves ID Proofing Outcomes

IOP switched its identity proofing vendor to Socure, in large part because the company is known for gathering its data from a combination of strong and inclusive data sources, including phone number history, address history, email account history, and real-time data from the device being used and draws on a repository of 530 million good and bad identities.

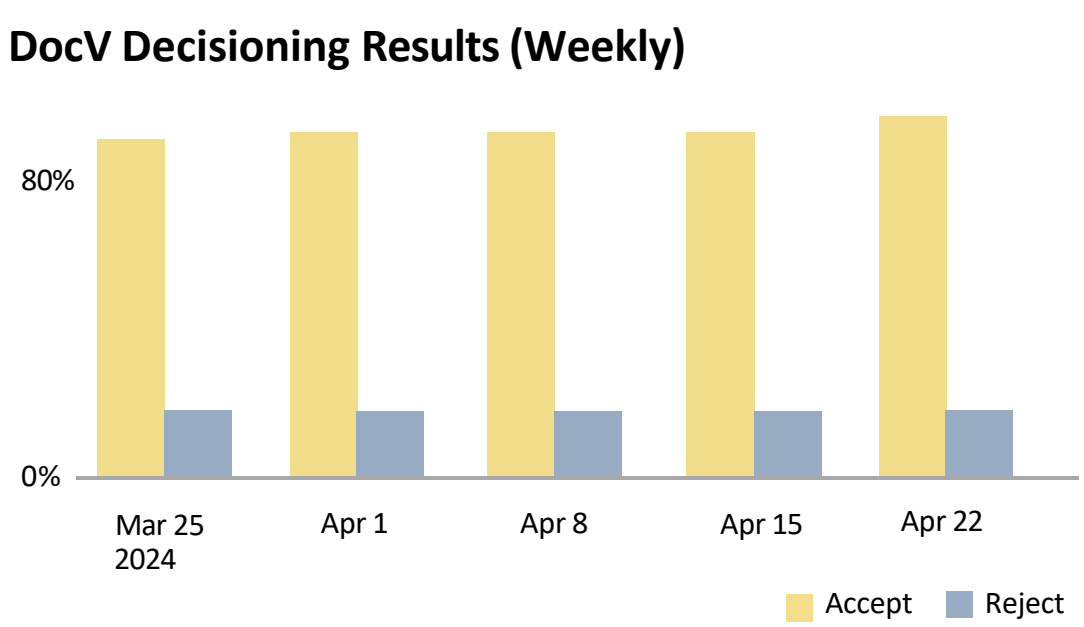


Also in phase 2, the project team implemented stricter overnight logic for ID proofing, when cyberattacks are more common. Since rollout, people using ID proofing through OHID have an average daytime acceptance rate of 81 percent. At night, when fraudsters are more active, the acceptance rate for successful ID Proofing attempts drops to 50 percent, in line with expectations.

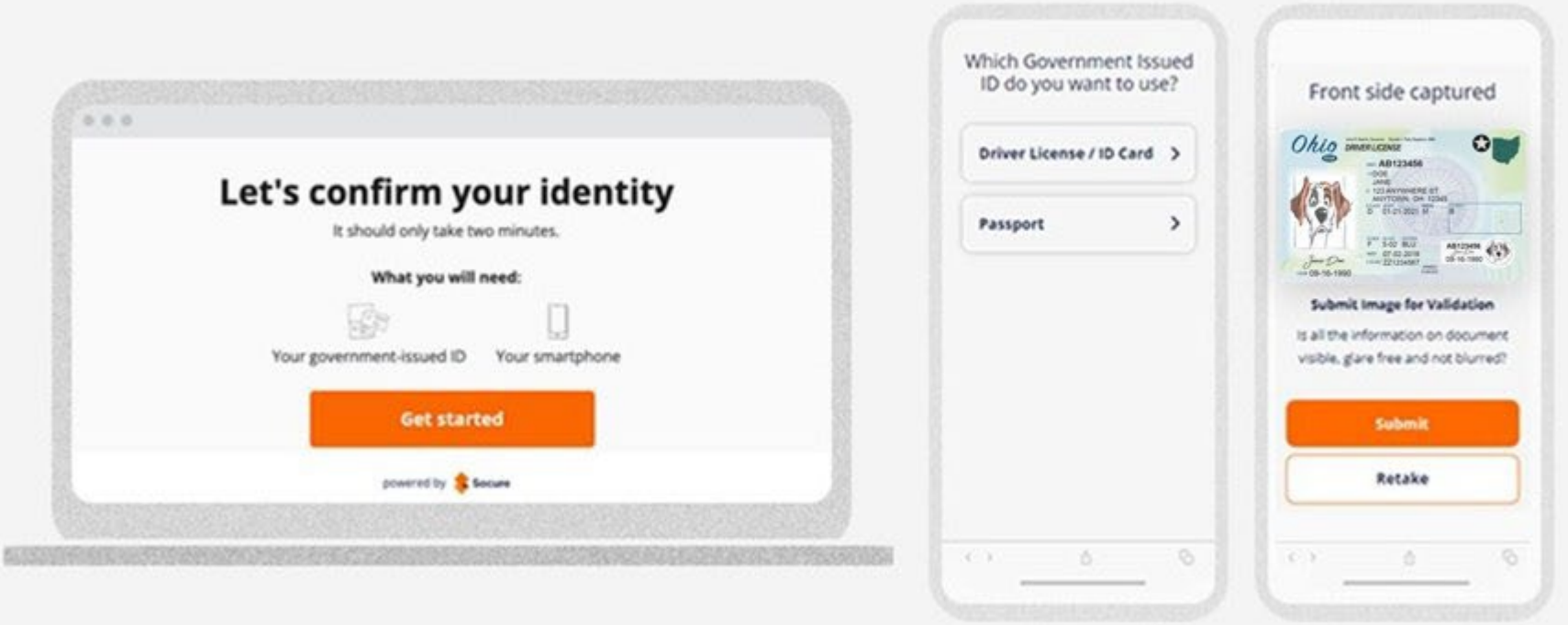
Phase 3: Inclusive ID Proofing with Smartphones and Verified Biometrics

The final phase introduced a quick and accurate process for remote document verification. This software solution would act as a self-service remediation process for OHID users who narrowly fail their initial attempt at ID proofing. Instead of heading to the agency's local office, these users who are presented with the option can use DocV to reattempt identity proofing – with an 80+ percent success rate on average.

This is because Socure DocV goes beyond matching the selfie to an authenticated government-issued ID. It assesses the validity of inclusive identity elements, including biometric and device data, to ensure they match the person presenting the ID. By adding this secondary ID proofing service, IOP was able to improve the online ID proofing success rate, even for hard-to-verify constituents, dramatically reducing our rate of referral in key demographics. DocV uses intuitive instructions to guide users through the process in about 15 seconds. Ohioans who are successfully verified are returned to the agency application they wanted to access. Anyone who is rejected retains the option to work directly with the agency to manually verify their identity.



There are two additional aspects of DocV that are worth noting. The first is the level of accuracy the AI analysis process offers. It can accurately verify identity even if the license or passport photo is an older one, or if the person underwent plastic surgery or developed facial scarring. The second item of note is the relatively high abandon rate for people who are referred to DocV. The abandon rate is reflective of actual fraudsters who give up because they are unwilling to attempt a biometric assessment.



Above: A peek inside the DocV verification process.

Conclusion

The State of Ohio continues to set its sights on finding the place where ease of access and cybersecurity meet. Armed with Socure identity verification and powerful machine learning, we are closer than ever. Based on feedback generated by Socure and collected from state agencies, IOP can hyper-tune our algorithm over time, adjusting it to become even more effective. Accurate and intuitive digital identity verification enables the State of Ohio to secure and protect sensitive data from bad actors while expanding public access to the growing library of digital state services on which Ohioans rely.