Socure

WHITE PAPER

Socure's Privacy Practices: A Resource for Public Sector Privacy Officers

Government privacy officers have much to consider when evaluating service providers that handle personally identifiable information in support of an agency's mission. We provide this whitepaper to promote transparency about Socure's data handling practices and to support your impact assessments.

Officers also must understand why identity verification is critical to agency missions, as well the mechanics of a solution, and how it comports with public sector compliance obligations (e.g., Act of 1974, E-Government Act of 2002) and other related guidance (e.g., The NIST Privacy & Cybersecurity Frameworks, NIST SP 800-53 Rev. 4, and NIST 800-63-3 Digital Identity Guidelines). This paper will answer questions a officer may have and serve as a resource to help understand how Socure's products work and how they fit into public sector obligations.

In the virtual world, fraud is easy. As more transactions were forced online by the pandemic, it has become indispensable for public sector organizations to provide reliable and accessible online resources while protecting against misuse of those very resources. Data-driven, automated identity verification is an important gateway for entry and hence, the protection of agencies' online platforms. Socure's solution works simply and quickly for as many people as possible so that they can enroll in and access the online services they need. Socure also empowers the government agency to know who they're dealing with online so that the agency is not deceived by fraudsters and can streamline interactions with constituents.

Technically, it's simple. People submit their identifiers—name, address, phone, email, and Social Security number (SSN), and sometimes their government-issued ID. Socure uses those few identifiers, as well as additional backend data about IP address and the device being used, to enable access for those who qualify, reject fraudsters, and identify suspicious activity.

PRODUCT OVERVIEW

Identity verification is about answering these questions:

Is this a real person?

Are they who they say they are?

How does Socure use consumer data?

The individual applying for access enters the necessary identifiers on the agency website, which then sends that data along with IP information and device data to Socure. The information is processed through Socure's in-house data analytics models and verification sources within a secure ecosystem maintained in accordance with the principles of least privilege and role-based access control. It's a tight loop of information, with each element solely dedicated to our identity verification and fraud prevention purposes. We never share information for marketing or other purposes.

What data does Socure collect from the individual and how does it comport with the data minimization principle?

Individuals undergoing identity verification may have to submit one or all of the following attributes: name, address, date of birth, SSN, email, government-issued ID card, and phone number. Socure also checks IP address and device details, which are important for detecting suspicious activity. The IP address and device information can indicate that the internet activity is coming from a suspicious location or device that doesn't match to the individual.

In line with the data minimization principle, these data elements are highly relevant and necessary for identity verification and fraud prevention purposes. Socure only uses data that has proven to help verify the identity or conversely, to suss out fraud. Together with Socure's predictive analytics techniques, this data enables the system to do more with less PII. We constantly monitor our performance rates and dynamic fraud trends to ensure that we are using information that is highly relevant and useful for identity verification and fraud prevention purposes. Socure does not monetize PII from individuals enrolling in associated systems, nor do we use it for any marketing purposes.

In a commitment to **transparency**, Socure provides this and other resources for agency privacy offices to really understand the identity verification service they will be using to protect constituents and agency portals.

In a commitment to **purpose limitation**, Socure only uses PII for identity verification and fraud prevention purposes.

What data sources do your solutions leverage and why?

Socure leverages data from a variety of authoritative sources, which enables us to create a complete picture of applicants and root out fraudsters before they can create an account.

Data sources include:

- Public records
- The Social Security Administration (note: public agencies cannot avail themselves of eCBSV)
- Credit headers and credit application data
- Mobile network operators
- Internet service providers
- • Email, phone, and address insight providers

What makes your solution different from other identity vendors, specifically those that leverage credit bureau data?

Socure products are designed to be hyper-accurate in verifying the identity of individuals without making their online experience difficult. Before Socure, online identity verification relied on consumer report lookups to determine if a person really existed. However, solely relying only on credit-based systems is inherently flawed. The credit system is not inclusive by nature: it does not guarantee information on each individual and often leaves out younger persons, immigrants, "thin credit," "credit invisible," or other historically disenfranchised populations. Designed to promote certain financial services, it is limited to those who apply for those credit services. It was never intended to be a dependable source of identity verification or fraud prevention. In fact, it's even become an open door for the creation of synthetic identities, which occurs when a fraudster applies for credit with information that the bureaus have not seen before, leading them to think it's a new individual and, create a new credit file for them. The next time the credit bureau sees the individual, they now have a credit file and appear legitimate. There are no safeguards to prevent this creation of synthetic identities, nor to identify or remove them, thus perpetuating a cycle of fraud.

Socure, however, uses dynamic, machine learning (ML) that keeps up with the ever-evolving nature of fraud. This contrasts with a rules-based approach which looks at one factor first, such as an SSN, then another factor, such as presence of a credit report, and then applies additional rules that require constant updating by humans and can result in the blocking of legitimate people. Instead, Socure looks at thousands of qualities of the identifiers and then looks to see how they correlate. Is this name associated with a real person and not a fraudster? Does the name match with the phone or email provided? Altogether, what are the indicia of goodness and what are the indicia of fraud?

In sum, our dynamic and correlative approach is more inclusive of a wider range of people and is best suited to catch the most challenging fraud attempts.

Does Socure use information provided by individuals for any other purposes?

Individuals that submit information for access to agency resources will only have that information used for that purpose—an expectation that everyone should have when sharing personal information. However, it's well-known that many online businesses take personal information and use it for purposes other than the original intent, including selling the information. Since Socure only uses personal information for identity verification and fraud prevention purposes, and does not otherwise monetize data, our practices hew to that important expectation.

Federal Officers must comply with the Act of 1974 and the E-Government Act of 2002 (PIA requirement)—how can Socure's products help them comply with those laws?

Socure works with agency officials to ensure use of our solutions comports with the agency's collection of personal information that may be subject to the Act of 1974. Agency programs that leverage identity verification solutions may have requirements to conduct a Impact Assessment (PIA) under the E-Government Act of 2002. Socure has conducted a PIA using a federal agency's template and can provide that and any other necessary information about its products to fit into agency PIAs, as appropriate. In doing so, Socure can support agency officers in addressing federal requirements including those in the NIST SP 800-63-3, Digital Identity Guidelines.

How do your products provide notice to individuals?

Socure works with its customers to make sure that notice and consent are conducted in a transparent manner. As a solutions provider to government agencies, Socure provides those agencies with clear explanations of what the products and services do with personal information so they can provide that information to applicants. Ultimately, it's up to the agency to properly notify applicants.

In a commitment to **collection limitation,** Socure focuses on innovation in order to perform identity verification with minimal PII and only that which is proven to be useful in verifying identity and preventing fraud.

In a commitment to **accuracy**, Socure constantly tests, monitors and improves its results in order to identify individuals as accurately as possible while preventing as much fraud as possible. We ask agencies to participate in this virtuous cycle through regular account reviews and automated feedback data.

In a commitment to **risk minimization**, Socure uses in-house data sources to the greatest extent possible, avoiding the risks of sending PII out to vendors, and curtails the retention of PII by all vendors.

Socure advertises the use of Machine Learning and Artificial Intelligence. What exactly does that mean and how does it provide better results?

Fighting digital crime has long been about realizing the fraud, recognizing the patterns, and then designing a defense. This is a constant cycle. To keep pace with fraudsters, Socure employs a team of data scientists and machine learning (ML). It's faster, it scales, and it sees all the angles. People often confuse machine learning with artificial intelligence (AI). AI is the ability for a computer to simulate intelligent behavior and even reasoning. But that simulation is only possible if the computer is taught how and what to simulate and this is where ML comes in.

ML is a subset of AI that uses algorithms and statistical analysis to discover patterns and build models that drive AI's responses to inputs. Models are built on predictors, or mini algorithms, that react to the individual elements presented in a task. The more data a learning engine can train on, the more accurate its models and predictors. In an open-loop, continual-learning mode, the engine keeps acquiring and learning from data. To date, Socure has seen over 1 billion records and is able to prevent 96% of third-party identity fraud in the riskiest 10% of transactions. This technology enables Socure to conduct better identity verification—with the same data sources other companies use—because the ML is always getting smarter.

How does Socure approach redress for people who cannot get verified?

Socure works with agencies to determine the best remedy for those who cannot be verified. Ultimately, it's the agency's responsibility to create this process; however, Socure will share industry best practices with agency officials on how to do this.

I'm reluctant to allow third parties to retain constituent data. Is this a required feature of your product? What benefits accrue to your customers by allowing retention of data and what is the retention period?

For government customers, retention is not required. However, we strongly recommend agencies think through the troubleshooting and audit implications, and impact on machine learning fraud prevention benefits before opting out of any retention. Socure works with its customers to determine what data retention is necessary or permissible according to federal or state requirements. Socure has worked with customers in financial services, HR/payroll, and online gaming to meet the stringent regulations in those sectors and will do the same for public agencies. For instance, data retention will permit agencies to audit and troubleshoot the performance of their identity verification transactions, including reviewing success rates of people being able to access important digital services.

Retaining some of the records also gives Socure and the agency the opportunity to improve the decision-making processes. For example, there could be a customer experience design that prevents people from progressing in the digital process, such as a dialogue box that is confusing. Another example could be internet access in rural areas that requires high bandwidth, hindering the ability for residents to use certain internet services. We can also use success and failure data to ensure that people of all locations and demographics have equal access to your online resources.

Just as important, our ML relies upon new and ongoing identity verification transactions in order to get smarter. To stay ahead of dynamic fraud trends, it's important to provide feedback and correction to our models so that they are aware when an individual's PII is being used to commit identity theft or other types of fraud.

What does Socure mean by "feedback data"? Is it personal information? How will it be used and protected?

Feedback data refers to follow-up information that our customers share on the fraud results of their transactions. They validate the accuracy of Socure's results and inform us the kind of fraud result. Feedback data allows us to fine-tune our models so that they respond more accurately to the real, dynamic fraud trends that our customers experience. Feedback is securely processed and stored in the same manner as other customer data.

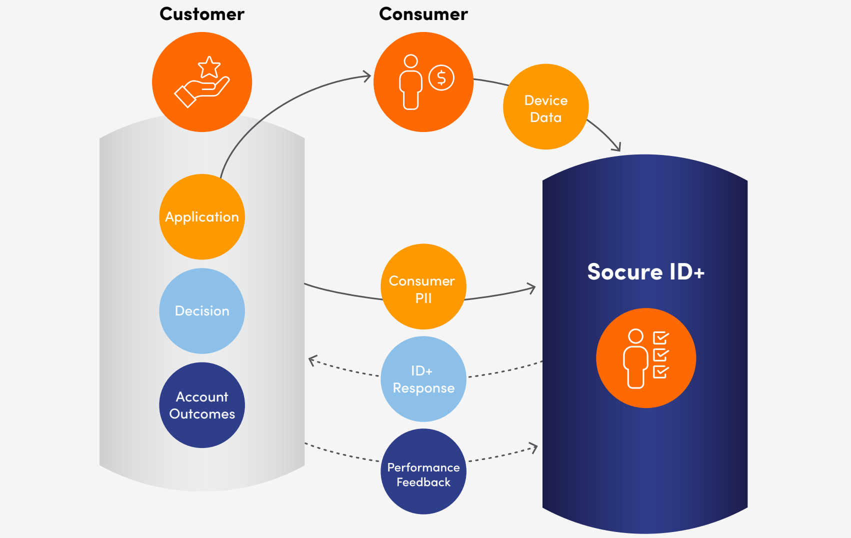
What does the Socure Privacy Program look like?

Socure's privacy program includes legal, compliance, and technical staff, as well as external advisors around the world. They advise on the entire information lifecycle, from personal information collection, use and disclosure, and retention. This includes advising on product development, data acquisition, and vendor risk management. The scope of the privacy program covers all personal information, including employee and consumer privacy compliance, and expands to international issues. This is all possible due to vigilant regulatory monitoring and ongoing engagement with the global privacy community. The privacy program works closely with our Data Governance Council to ensure the implementation of privacy rules and policies. External privacy statements are published on the Socure website. Finally, all Socure employees undergo privacy and security training at onboarding and on an annual basis.

How does Socure ensure data security?

Socure institutionalizes its data security standards and practices in its internal policies and contracts with third parties. Socure's fully hosted (AWS) cloud platform has been assessed against and currently complies with the following industry security standards: StateRAMP Moderate (Authorized), TX-RAMP Moderate (Authorized), System and Organization Controls (SOC) 2 Type 2, International Organization for Standardization (ISO) 27001, 27017, 27018, 27701, Web Content Accessibility Guidelines (WCAG) 2.1 Level AA, and NIST Identity Assurance Level 2 (IAL2). Socure is compliant with FedRAMP requirements and has been assessed by a FedRAMP-approved third-party assessor (3PAO) as compliant with FedRAMP security controls, is listed as FedRAMP Moderate In Process, and protects data in accordance with these stringent security requirements.

Socure: Real-Time ID+ Data Flows



Learn how Socure can help you grow and power financial inclusion.

Connect with us today.

About Socure

Socure is the leading platform for digital identity verification and trust. Its predictive analytics platform applies artificial intelligence and machine learning techniques Socure is the leading platform for digital identity verification and trust. Its predictive analytics platform applies artificial intelligence and machine learning techniques with trusted online/offline data intelligence from physical government-issued documents as well as email, phone, address, IP, device, velocity, date of birth, SSN, and the broader internet to verify identities in real time. The company has more than 2,300 customers across the financial services, government, gaming, healthcare, telecom, and e-commerce industries including four of the top five banks, 13 of the top 15 card issuers, the top three MSBs, the top payroll provider, the top credit bureau, the top online gaming operator, the top Buy Now, Pay Later (BNPL) providers, and over 250 of the largest fintechs. Marquee customers include Chime, SoFi, Robinhood, Gusto, Public, Stash, DraftKings, State of California, and Florida's Homeowner Assistance Fund. Socure customers have become investors in the company including Citi Ventures, Wells Fargo Strategic Capital, Capital One Ventures, MVB Bank, and Synchrony. Additional investors include Accel, T. Rowe Price, Bain Capital Ventures, Tiger Global, Commerce Ventures, Scale Venture Partners, Sorenson, Flint Capital, Two Sigma Ventures, and others.

Socure