Q/A with Matt Thompson

Senior Vice President and General Manager,
Public Sector, Socure

Low-Risk, Constituent-Friendly Identity Verification

Fast, accurate identity verification and fraud prediction allow constituents to engage with digital government more easily, confidently and equitably. In this Q&A, Matt Thompson, Senior Vice President and General Manager of Public Sector for Socure, explains how Socure sets a new bar for identity verification and fraud prevention in state and local government.

Q What should agencies look for in an identity solution?

A Identity verification generates excessive friction, inaccurate results and high costs to the government if you don't have the right solution. Knowledge-based assessment (e.g., responding to questions like "which of these streets do you live on?") is cumbersome, vulnerable to fraud, and has a high false-positive rate. Fraudsters can easily obtain the information, while legitimate users may not remember their answers to questions. Some solutions require constituents to scan a photo of their driver's license or submit a smartphone selfie, even for low-risk transactions. This creates an unnecessarily high-friction process and excludes people from access if the user doesn't have a high enough quality device or government-issued document handy.

Socure's identity verification platform creates the ideal balance between reducing friction and preventing fraud. It collects data from hundreds of sources and applies our machine learning (ML) models to calculate the likelihood of fraud within a transaction with the highest levels of accuracy in the industry. It automatically accepts transactions that are clearly not fraud and steps up requirements when transactions indicate higher risk, providing the agency with a human understandable explanation and audit trail of why the identity is being marked as good versus fraudulent.

Q How is Socure tackling unemployment fraud?

A Socure uses a layered approach where we focus on devices and email first to block obvious fraud early on. For example, we may deny repeated attempts to file unemployment applications from the same device or session. This reduces the velocity of an attack by forcing fraudsters to find a different computer or start a new session. Our identity verification platform also uses ML and third-party data to identify high-risk transactions and weed out more sophisticated types of fraud. It automatically increases friction on high-risk transactions by asking for document verification. At that point, most criminals abandon their schemes.

Q How does Socure help organizations with constantly changing attack vectors?

A Socure is constantly building new features and updating our models to adapt to the ongoing changes with fraud Tactics, Techniques and Procedures. We analyze fraud patterns across more than 2000 customers to take a network approach against the organized criminal networks attacking government systems. Our admin dashboard and no-code decision module allow agencies to quickly modify logic on their own as attack vectors emerge or change. There's no black box or custom coding, so they don't have to develop and push code. Self-service testing ensures confidence with each change.

Radical Accuracy in Identity

Socure™
socure.com