incode
REIMAGINE TRUST

Title: Know Your Voter: Transforming the Public Sector with Biometrics

The claims of voter fraud existed long before the allegations of potential fraud during the 2020 Presidential election caused great controversy, and those claims are still being disputed and investigated three years later. The unique conditions of this historical presidential election shed light on an important and long-standing issue: how are outdated election processes potentially enabling voter fraud, and what's the solution?

Voter fraud is loosely defined, but it can range from casting illegitimate votes to buying votes to swaying one side the other way.

Outdated systems and lack of consistency between governments, coupled with heightened fraudulent activity leads to this conclusion: many government agencies must catch up with technology and adapt to the evolving needs and concerns of voters and local/state governments, and the evolving risks. Adopting biometric authentication is one way to modernize the voting and election processes and help decrease the likelihood of fraud, by providing identity verification for each voter.

The process is straightforward and user-friendly: with their cell phone and a government-verified system, a voter takes and uploads a picture of their ID, takes a selfie, and gets verified remotely. This simple and fast verification can be used for in-person voting as well as for mail-in ballots and eventually, for voting in real time while remote.

Biometric authentication technology offers an array of benefits across a variety of industries, including online banking, e-commerce, sports and entertainment, gaming, and healthcare. Specific to the public sector, biometrics can be used to:

- Eliminate identity fraud
    - Biometric authentication accurately and instantly verifies a voter's identity both for registration and for casting a ballot to confirm he/she/they meet legal requirements for voting procedures through liveness detection. Utilizing a live selfie and a government-issued ID of the voter's choice, biometric liveness detection can confirm the voter is who they say they are in both photos and, conversely, if the person is attempting to submit a fraudulent vote by submitting a photo of a photo of their face, for example. In doing this, identity verification technology can execute numerous safe checks to verify voters' documents are real and up-to-date and access government databases for additional verification in doing so.
- Automate processes for maximum scale and privacy
    - Processing biometric data through fully automated verification allows governments to verify high volumes of personally identifying data in seconds. ID verification providers don't know a voter's party or how they voted, they simply ensure the identity of voter and ensure the person's privacy while on the Elections Office actually processes the ballot.
- Provide a seamless user experience and improve equitable service access
    - Rather than waiting in lines at spread out physical locations to submit votes, users cast ballots and authenticate their identity all in one place using their own unique identity.

- Break down siloes in local and national elections
    - Adopting biometric authentication creates consistency in the way government agencies verify each voter's identity.

Delivering government services requires a new level of trust, privacy, and safety for constituents. By reducing online fraud, increasing conversion rates, and protecting user privacy, biometric authentication turns identity into a guarantee of trust in a modernized government. However, as with any form of sensitive and personal data, it's imperative that biometric data is handled carefully and trusted by the use of auditable, best in class practices and procedures.

To build trust, organizations and the biometric technology partners they work with must be transparent in how they use voter data. Voters must be assured that their sensitive data isn't falling into the wrong hands or being used for exploitative purposes. The following list includes a few best practices for implementing biometric authentication and verification in election systems, on a local, state, or national scale:

- Establish trust with voters
    - Constituents are concerned about how government agencies will use their personally identifiable information (PII). Those who fear the misuse of their personal data may resist casting a ballot, much less providing information to government agencies. Both the agency and the identity solution provider must assure the constituent that their data will be used only for a specific delineated purpose, and that their privacy will always be protected. The identity solution itself plays a critical part in easing constituent concerns as it provides an audit trail of all data usage and prevents unauthorized individuals from accessing a constituent's personal information.
- Eliminate human access to data
    - There are three core benefits to enabling a fully automated identity verification system and eliminating human access to sensitive data. First, a fully automated identity verification system provides more reliable decision-making than humans for confirming identities. Second, the system protects constituent privacy and reduces fraud by eliminating human access to sensitive PII. Finally, the system provides instantaneous results, driving constituent satisfaction. Constituents do not need to wait, such as for people in remote call centers, to manually verify identity results. Manual verification can take days, or even weeks, and these delays have led to constituent dissatisfaction in identity verification implementations.
- Limit or prohibit storage of user images and un-encrypted biometric data entirely
    - Choosing an identity solution that limits data movement—or that does not store PII at all—will improve trust, privacy, and ease-of-use metrics. Limiting information (e.g., biometric data) to the device itself, or not retaining these data in the first place, reduces the chance of sensitive data being moved or shared outside intended boundaries. The identity solution should limit data interchange between systems to simple queries and affirmative/negative responses without transmitting sensitive data or requiring (or permitting) sensitive data to leave a government agency's secure environment. Additionally, a solution that processes on the edge (i.e., offline, and completely within the device) improves the speed and convenience of a transaction, enabling users to retrieve resources faster and without the need for Wi-Fi or cellular access.