Asignio: The Signature Biometric

Asignio is a web-based biometric authentication platform which uses handwriting recognition technology to authenticate the identity of users. Asignio revolutionizes the user's experience and provides a new, more secure way to sign-in and authenticate identity. Asignio's omnichannel authentication platform utilizes the user's unique handwriting to authenticate transactions on all apps, websites, and accounts.

Any account. Any device. One *Signature*.

Asignio: Innovative Soft Biometric Authentication

Rather than use a password that is easily stolen, hacked, or forgotten, Asignio uses soft biometrics to authenticate its users. Biometrics measure the physical or behavioral traits of the user to verify identity. Hard biometrics, like fingerprints, are a trait that can never be changed. Soft biometrics, like handwriting recognition, are characteristics that can be changed.

The Asignio *Signature*

An Asignio *Signature* is a personalized set of letters, characters, symbols, or even a simple drawing. Asignio's proprietary software measures the *Signature* across three planes—x, y, and t (time). More than 25 different variables of a user's *Signature* (velocity, peak acceleration, etc.) are measured and compared to authenticate the user's identity during every transaction.

Signatures are easier to remember than passwords and take less than three seconds to sign and authenticate. Asignio can be used on any device with a touchscreen. The user can access their accounts on a desktop, tablet, or mobile device using just their Asignio *Signature*. Users can even login using desktops without touchscreens through simple QR code linking. With Asignio, users can make secure transactions anywhere, anytime, on any device.

Authentication

There are three recognized factors of security for authentication: "something you know," "something you have," and "something you are." Unlike its competitors, Asignio uses all three factors of authentication to keep its users secure. Asignio users create their own *Signature*, something that only the users know. When the user's devices are registered with Asignio, they become a physical token of security, something that only the user possesses. The user's unique style of handwriting (or biometric identifier) is the third factor of authentication. A person must possess all three of these factors in order to sign in to their account, keeping the user secure without compromising user experience.

False acceptance rates (FAR) measure how likely it is that a biometric system will accept a login or access attempt from a false or unauthorized user. Asignio's false acceptance rate (FAR) is 1 in 2.3 million, meaning that only 1 in 2.3 million unauthorized attempts would be successful. In contrast, the FAR for Apple's Touch ID on the iPhone is only 1 in 50,000.

Access

Unlike a fingerprint or retina scan, the Asignio *Signature* can be changed at any time. If a user fears their account has been breached, they can design a new *Signature* and re-secure their account within seconds. Asignio only stores biometric data pertaining to the user's master signature. Even if the master signature has been compromised, the user's specific biometric identifier (the way the user writes) stays secure.

Asignio utilizes machine learning to strengthen the security of the *Signature* over time. Asignio's proprietary software continuously adapts to the user's unique style of writing. The more a user signs their *Signature* to access their accounts or complete transactions, the better Asignio can learn the nuances of their handwriting. This helps Asignio authenticate that it is actually the user signing their *Signature* and not someone else.

Asignio and the General Data Protection Regulation (GDPR)

GDPR broadens the definition of personal data, tightens the rules for obtaining consent, and shifts ownership of this data from businesses to the consumers. The new regulations go into effect May 25, 2018. Companies may be fined up to four percent of annual global turnover for breaching GDPR.

Asignio provides an audit trail of user consent, from onboarding and through every transaction. Each customer's *Signature* is a unique biometric, allowing banks to prove customer consent each time the customer signs. Asignio ties all personal identifiable data, including a verified government ID, to the user's *Signature*. If the user ever requests that their data be deleted, all the company has to do is delete the user's Signature and all the data will delete with it.[1]

[1] http://www.eugdpr.org/gdpr-faqs.html

Asignio and the second Payment Services Directive (PSD2)

PSD2 requires stronger identity checks when paying online and mandates that all electronic transactions use at least two factors of authentication.[2] PSD2 goes into full effect January 13, 2018.

Asignio goes above and beyond the PSD2 requirements for 2-factor authentication. Asignio uses 3-factor authentication for every sign-in and every transaction. Companies with only one method of authentication can use Asignio as a form of step-up authentication and fulfill PSD2 requirements.

Asignio: Sign, Authenticate, Access

Asignio keeps companies and consumers safe through the use of the Asignio *Signature*. Machine-learning and Asignio's proprietary hand-writing recognition software allows Asignio to know the customer continuously, preventing money laundering and other fraud. Asignio helps companies meet new and upcoming industry standards in data regulation

With Asignio's web-based, cross-device platform, consumers and businesses know that every sign-in and transaction is authenticated with the highest level of user validation, simplicity, and durability.

Any account. Any device. One *Signature*.

Asignio

[2]http://www.bankingtech.com/774622/infographics-psd2-explained/