



ASIGNIO

Any Account. Any Device. One Signature.

THE COST OF KYC AND AML

Know Your Customer (KYC) technology and Anti-Money Laundering (AML) compliance are crucial elements of modern banking. Financial institutions are trusted to verify and authenticate customers' identities every time a customer uses their accounts and services. However, implementation is costly and ongoing monitoring can be difficult.¹ In a world where a digital data trail is both extremely valuable and extremely vulnerable, protection and authentication of a customer's identity is paramount.

A reported \$5.2 billion in fines were assessed against financial institutions for AML violations from 2009 to 2015.² To reduce money-laundering, fines, and improve compliance, financial institutions need to upgrade their security. But how?



in fines were assessed
against financial institutions
2009 to 2015

THE PROBLEM WITH KNOWLEDGE-BASED AUTHENTICATION

Passwords and other "knowledge-based" authentication methods are difficult to use, difficult to remember, and virtually impossible to secure. The constant need to change and update passwords makes for weaker security and even worse customer experience. While companies try to secure users' accounts with security questions, now such personal information is open to social engineering through social media sites like Facebook, LinkedIn, and others.

What if there was an authentication system that improved security, strengthened AML compliance, and provided better customer service?

Now there is: Asignio web-based signature authentication.

¹World Finance. <http://www.worldfinance.com/banking/kyc-regulations-challenge-the-banks>
²Credit Union Times. "AML/BSA Fines Total \$5.2B Over Six Years." <http://www.cutimes.com/2016/04/22/aml-bsa-fines-total-52b-over-six-years-gao?slreturn=1496790726>

BIOMETRIC BASICS

Rather than using a password that is easily stolen, hacked, or forgotten, biometrics utilize physical or behavioral traits to verify user identity. The pattern of a fingerprint or the inflection of a person's voice are unique traits that are inherent to an individual. Biometric security is safer than a password and is quickly becoming a part of everyday life.

HARD VS SOFT BIOMETRICS

Hard biometrics measure innate qualities that cannot be changed, such as fingerprints or the pattern of a retina. This kind of biometric security has become increasingly widespread through the proliferation of smartphones with built-in fingerprint scanners. While hard biometrics provide a new measure of safety, they also create a new security problem: once stolen or hacked, hard biometrics are forever compromised. There is no way for a user to change their fingerprints or their irises. Once a hacker acquires an individual's hard biometric data, it can never be used safely again.

Soft biometrics measure qualities like variances in handwriting or the inflection of a person's voice. These abilities are just as unique as a fingerprint, but with the added advantage that **what** the user writes or speaks can be changed if their account becomes compromised. No matter how many times the signature or spoken password changes, the user's unique handwriting or voice maintains consistent underlying characteristics for identity authentication.



CONSUMERS WANT BIOMETRIC SECURITY

Though financial institutions constantly struggle with weak KYC solutions and poor AML compliance, advances in biometric security provide new answers. What's more, customers are eager to use biometric security. A recent survey on MarketWired.com found that 79 percent of respondents want more biometric authentication methods to access mobile banking or payment applications.³ An additional 42 percent said they wouldn't use a banking or payment app which didn't offer biometric security.⁴



want more biometric authentication methods



wouldn't use a banking or payment app which didn't offer biometric security

Biometric security offers a way for financial institutions to differentiate themselves from their competitors and provide better security for their customers. A *New York Times* article found that after USAA offered biometric authentication in early 2015, it took less than a year for more than 1.7 million customers to begin accessing their accounts using biometric identity verification alternatives.⁵ And the number will only continue to grow.

³ MarketWired. <http://www.marketwired.com/press-release/eyeverify-survey-reveals-high-consumer-trust-biometrics-mobile-banking-payments-2214109.htm>

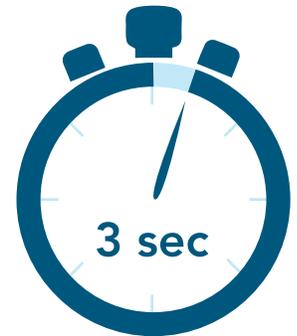
⁴ MarketWired. <http://www.marketwired.com/press-release/eyeverify-survey-reveals-high-consumer-trust-biometrics-mobile-banking-payments-2214109.htm>

⁵ NYT article. <https://www.nytimes.com/2016/06/22/business/dealbook/goodbye-password-banks-opt-to-scan-fingers-and-faces-instead.html>

THE ASIGNIO SOLUTION

Asignio is a handwriting-based biometric authentication system. Rather than hard biometrics like fingerprint or retina scans—which, once compromised, can never be replaced—Asignio uses cutting-edge soft biometric technology to measure more than 25 unique aspects of a person’s “*Asignio Signature*.” Each *Signature* can consist of a personalized set of characters or letters. When the consumer signs-in using their *Signature*, Asignio verifies their identity using three factors of authentication in under three seconds.

There is no need for specialized hardware like fingerprint or iris scanners. With Asignio’s cross-device capabilities, the only equipment needed to sign-in or authorize transactions is a touch-screen device.



3- factor authentication in under 3 seconds

ASIGNIO AND KYC

The Asignio on-boarding process confirms and protects the consumer’s identity, providing a layered security system firmly rooted in ID verification.

First, Asignio asks the user for a picture of a government-issued ID. During this one-time verification process, the ID is checked and confirmed independently. The verified ID is then matched to the user’s profile. This ensures a strong level of KYC for the financial institution, as Asignio links the consumer’s real identity to the correct account.

The user then creates their own *Asignio Signature*. This *Signature* is tied specifically to the user’s ID, thus providing an additional layer of security for both the financial institution and the consumer.

Asignio does more than meet standard KYC requirements. Asignio helps financial institutions know their customers *continuously*. Asignio provides a digital data trail of the user proving the financial institution’s AML compliance from onboarding and ID verification through each transaction sign-in and authorization.



ASIGNIO AND AML

Asignio's strong foundation in KYC authentication helps financial institutions crack down on AML violations. Because each user's *Asignio Signature* is tied directly to their ID, Asignio can verify and authenticate the identity of the user during each and every transaction.

Asignio uses a layered security system, utilizing both behavioral biometrics and geo-location. By tracking where the user signs in and how they typically use their account, Asignio can quickly respond to any red flags raised by unusual activity. Taken together, these security factors help financial institutions continuously know their customers and further combat AML fines.

ASIGNIO: SAFE, SIMPLE, SECURE

Asignio works hard to keep both the bank and the consumer safe through the use of the *Asignio Signature* and layered IDV. With Asignio's web-based, cross-device platform, consumers and financial organizations are secure in the knowledge that every sign-in is authenticated with the highest level of user validation, simplicity, and durability.

Any account. Any device. One *Signature*.

 **ASIGNIO**

