WHITE PAPER

Cloud-Based Biometric Identity Proofing and Authentication Services for Mass Markets

Making Identity Fraud Prevention Truly Globally Accessible

AWARE

Cloud-Based Biometric Identity Proofing and Authentication Services for Mass Markets

Making Identity Fraud Prevention Truly Globally Accessible

Identity fraud: a trillion dollar problem

Some form of identity theft is at the heart of most financially-motivated fraud. A proliferation of personally identifiable information (PII) available through social media and other public sources is easily accessible to aspiring fraudsters, while the anonymity of Internet commerce and communication gives them plenty of cover. Illicit call centers troll for private identity data from unsuspecting consumers and untrained customer service agents. Identity fraud is increasingly committed by sophisticated criminal organizations operating beyond the reach of outdated laws that do not address such crimes. "Mega-breaches" resulting in theft of vast quantities of identity information occur with regularity; many we surely never hear about. Synthetic identity fraud, based on skillful creation of fictional identities, is a significant and fast-growing source of losses to fraud. In short, identity fraud and its derivative crimes cost banks, retailers, healthcare providers, governments, and ultimately consumers and taxpayers around the globe hundreds of billions of dollars every year, and this figure continues to grow.

> ***identity fraud and its derivative crimes cost banks, retailers, healthcare providers, governments, and ultimately consumers and taxpayers around the globe hundreds of billions of dollars every year***

Using biometrics to prevent fraud and protect identities

Biometrics are rapidly making their way into the mainstream as a means to help prevent identity theft and fraud. Most visibly, we see fingerprint sensors being integrated into smart phones as a more convenient mode of secure access to a device for its owner. These devices are increasingly enabling use of biometrics towards more secure mobile payment models that aim to avoid security pitfalls of credit cards. Biometric authentication functionality provided in the recent Microsoft Windows 10 release can be used to secure access to external systems and websites, supporting fingerprint, face, and iris modalities.

Use of biometrics is growing because our fingerprints, faces, irises, and voices have truly special properties that make them an effective barrier to fraudsters attempting to surreptitiously impersonate us. They are useful because unlike names, ID numbers, email addresses, and passwords, they are comparatively more unique, secret, permanent, consistent, difficult to reproduce, and—most notably—physically bound to us, which also happens to be very convenient.

Biometric authentication from a smart phone or computer essentially uses our biometrics like a password that is unique to us and cannot be practically transferred or stolen and then reproduced. Biometrics make fraudulent impersonation extremely difficult, particularly when used in tandem with other complementary security measures.

Biometrics are for more than just authentication

Biometric authentication on smart phones and other devices is effective and particularly useful to their owners to prevent their fraudulent use; biometrics are the password of the future. But from the perspective of a bank, government agency, or any organization aiming to broadly reduce its exposure to identity fraud, a more universal approach is needed to have a broad impact.

> ***from the perspective of a bank, government agency, or any organization aiming to broadly reduce its exposure to identity fraud, a more universal approach is needed to have a broad impact***

Here's why:

1. Much of identity fraud is committed using 'synthetic' identities that are not stolen but created. Authentication alone does not address this type of fraud.

2. Biometric verification does not verify the authenticity of identity data; only that the person verifying is the same who registered the data. Biometric verification on a device helps prevent a fraudster from using a stolen device to falsely claim the identity of the owner, but does not prevent them from establishing accounts with fraudulent information.

3. Penetration of smart phones is growing rapidly, but is still on the order of only 36% globally (GSMA Intelligence, 2015). In places where many people still don't use smart phones, other mechanisms are necessary to prevent identity fraud more universally.

4. Authentication on smart phones is device-specific and constrained to operate as implemented by device, OS, and application suppliers. While organizations aim to standardize architecture and interfaces, biometric functionality and performance will not be universal or configurable on these devices, and will not necessarily meet the security requirements of a particular application.

Fundamentally, there are many modes of identity fraud that simply can't be addressed by password enhancement, and types of accounts, applications, and environments that require more robust security and more trustable identity verification.

Biometric identity proofing ensures data integrity

More than just "something we are", biometrics allow us to permanently bind ourselves physically to digital information; a powerful capability that enables us to not only biometrically authenticate, but also to biometrically deduplicate; that is, to determine through biometric search whether someone is surreptitiously attempting to establish a false identity. Said another way, identity proofing with biometric search helps assure the integrity of our identity data: that one identity represents each person, that each person has only one identity, and that the identity data associated with a biometric can be trusted.

Robust identity proofing requires the enrollee to present identity documents and information in-person as part of an application or onboarding process. The process might additionally draw upon public and private data sources. A biometric enrollment and search performed as part of this process serves as a highly confident "duplicate check" to ensure that the applicant is not already registered in the system, perhaps with different identity information. If upon enrollment, a biometric search yields a match to an identity with different information than what is being claimed, there is reason for further investigation. This is the idea behind biometric identity proofing; a means to combat identity theft at its source by ensuring the integrity of identity data at the point of enrollment.

Once a duplicate check is performed, a biometric enrollment digitally links the enrollee's trusted unique record to them physically through their biometrics. These biometrics can then be used perpetually to prevent future attempts at false representation of their identity information by a fraudster. The process also establishes a high level of trust in the authenticity of the identity data associated with the enrolled biometrics, making them more useful for future biometric authentications. While biometric identity proofing requires additional effort to verify identity data integrity and detect duplicate enrollments, it provides yet another very effective barrier to fraud.

> ***identity proofing with biometric search helps assure the integrity of our identity data: that one identity represents each person, that each person has only one identity, and that the identity data associated with a biometric can be trusted***

In-band and out-of-band biometric authentication

Biometric authentication is referred to as "out-of-band" when it is performed via a parallel channel that is independent of that used for the activity or access being secured. For example, device-based biometric authentication typically employs an 'in-band' approach, given that the means of biometric authentication employs a serial workflow that is inextricably tied and dependent on the same device and communication

path as the transaction or access attempt.

In contrast, an out-of-band authentication is performed as a separate, parallel function to the transaction. There are different approaches. An authentication might rely on the user providing information provided via a separate, parallel channel, such as by sending an access code "out-of-band" in a text message or email that is then used to gain access. In another example, biometric authentication is performed out-of-band by an accompanying human being processing the transaction. Out-of-band mechanisms add yet another layer of security, requiring access to a device, e-mail account, or in the case of accompanied processing, physical presence (which also affords an opportunity for facial recognition by a human, document checks, etc.).

Device- vs. server-based authentication

The storage of the enrolled reference biometric and subsequent comparisons upon authentication attempts can take place either on the device or on a central platform. Each offers advantages and disadvantages in terms of security, performance, and functionality depending on the application, but both are likely to see widespread adoption.

In a device-centric model, a biometric comparison is performed on a device (e.g. smart phone), which can then be used to satisfy a cryptographic challenge/response between the consumer and the relying party (the party relying on the authentication, such as a retailer). A standard for a device-centric model of biometric authentication called "FIDO" has been drafted and broadly advocated, and will likely emerge as a dominant mechanism for biometrically authenticated logins and transactions on devices. Because device-based biometric authentication does not require central storage of biometric data, it can't lead to a large-scale breach where many biometrics are compromised at once. But a stolen device can also provide opportunities to attempt to defeat biometric security and commit fraud.

A centralized server-centric model requires storage of biometric enrollment data on a server or centralized platform, and transfer of biometric data to the server for comparison upon authentication attempt. This architecture might be employed where for whatever reason the mechanism offered by the device and/or application supplier is not suitable or adequate for a given application or environment, and more control of the biometric authentication process and performance is desired.

For both device- and server-centric models, there is concern that in the event that biometric data is compromised, an individual would be precluded from trustfully using their biometrics ever again, given their inherent permanence. But while it is possible that a physical biometric source (e.g. rubber finger) be reproduced from a compromised biometric template and then used to spoof an authentication, it tends to be a tedious, unreliable, and detectable process. Like all security mechanisms, biometrics are theoretically defeatible, but the barriers are high and are getting higher with new liveness detection technologies and other techniques that make spoofing unattractive to the vast majority of even the most talented and ambitious fraudsters.

Biometric Services

"Biometrics-as-a-Service" offerings promise to make robust identity fraud prevention truly universally accessible. A services-based subscription or pay-per-use alternative will gain adoption from a large segment of the market for the same reasons that support a $100 billion software-as-a-service (SaaS) market (Forrester Research, 2015): no upfront costs, predictable future costs, and the freedom to select from and switch to competitive offerings. Security is the fastest growing area of IT investment (IDG Enterprise, 2015), and the lower costs and risks of a services model promise to make biometrics-powered identity fraud prevention solutions accessible to a much larger percentage of the public- and private-sector organizations that need them. The nature of the services will vary; they might be public cloud-based or run on a single private server; they might include only biometric search and identity proofing or authentication; they might be based on a particular biometric modality. But they will change the landscape of high-performance biometric search and match, just as SaaS has changed the landscape of enterprise software.

> ***"Biometrics-as-a-Service" offerings promise to make robust identity fraud prevention truly universally accessible.***

A key feature of the Certibio service it is sufficiently flexible to accommodate a variety of customer requirements, in terms of functionality, performance, privacy, and security.

Certibio: Biometrics-as-Services in Practice

As the largest provider of digital certificates in Brazil, Certisign has gained a deep understanding of identity and security. It has led them to recognize the power of biometrics to address identity fraud, as is evident from the recent launch of biometric identity proofing and authentication services by their new subsidiary, "Certibio". As in much of the world, Identity fraud is a problem in Brazil where the service is launching, so there is demand for a service that is not only robust but also sufficiently flexible and scalable to address a variety of customers and requirements.

Certibio provides biometric identity proofing and authentication services to its customers, which might include banks, government agencies, retailers, or any other type of business that wishes to biometrically authenticate its employees and/or customers. By consuming these as services, Certibio customers avoid an upfront investment in biometric enrollment and data storage equipment and software and avoid the risk and costs of future maintenance and obsolescence.

The Certibio service emphasizes the value of identity proofing, which serves to ensure that the individual applying for an account is in fact who they claim to be, and that the biometrics that they collect are of high quality and bonded unambiguously to trusted identity information. They ensure that the biometrics they collect during the identity proofing process are of sufficient quality for reliable future authentications and that they are linked to reliable, professionally-vetted identity information.

Once a business signs on for services, biometric authentication equipment is installed at locations where authentication will be performed. Enrollees must bring proof of identity as specified by their sponsor. They are interviewed by a Certibio service agent, who performs the initial identity proofing process and also collects their biometrics. The system supports fingerprint, face, iris and voice biometrics. Once the enrollment process is complete, the collected biometrics are used to search the database for a previously enrollment. If one is found and the identity information is conflicting, then further investigation is warranted. If the information is not conflicting, then the enrollment is updated. The enrollee is issued a unique ID number.

Once the enrollee is in the system, they can be biometrically authenticated at customer locations, such as a bank. A bank might require that new customers for new accounts be authenticated using the Certibio system. The new customer simply submits their Certibio identification number and their biometrics are scanned. The bank officer receives back from Certibio the identity information provided upon enrollment. This identity information had been professionally vetted, so the bank can be confident that the identity information being presented is accurate. The bank might also require that the customer biometrically authenticate for certain types of transactions.

A key feature of the Certibio service it is sufficiently flexible to accommodate a variety of customer requirements, in terms of functionality, performance, privacy, and security. A few of the different choices available to customers follow, and new service capabilities and enhancements are already in the works.

1. Fingerprint, face, iris, and/or voice biometrics
2. Single modality or several modalities
3. Storage of biometric data in Certibio cloud, customer's private cloud/server, or use of existing government database

At the center of the multi-tiered Certibio system is a management platform, used to coordinate business logic and workflow across the system, as well as administrative functions. It serves as a central service between biometric collection workstations used for biometric enrollment, identification, and verification, and the various matching services available. These services include one-to-one biometric verification services provided by the government identity bureau, and biometric search and match services performed by Certibio. The Certibio biometric matching services are provided by the Biometric Matching Platform. Operating Platforms are used to manage the workstations.

There are two configurations available for customers: 1) Certibio-managed data and 2) customer-managed data. In the first configuration, Certibio provides all biometric matching and storage from a Biometric Matching Platform operating within the secure Certibio private cloud. Each platform is a custom-configured instantiation of Aware's Biometric Services Platform (BioSP™). The Certibio enrollment and verification workstations utilize Aware SDKs.

Looking Forward

The first wave of growth for digital biometrics came in the 1990s from demand for law enforcement solutions. The second came in the 2000s for border control, defense, and related security requirements due to new terrorism threats. Today we are in the midst of a third wave of growth derived from mass-market adoption of mobile devices and PCs equipped with biometric sensors used for password enhancement.

> ***A fourth wave of growth will come from biometrics used to assure the integrity of identity data, and biometrics-as-services will be a substantial component of this growth.***

A fourth wave of growth will come from biometrics used to assure the integrity of identity data, and biometrics-as-services will be a substantial component of this growth. Ongoing mass-market adoption of biometric authentication technology will help dispel the perception of biometrics as a privacy liability; biometrics will be increasingly recognized more accurately as a privacy asset that can be used to ensure our unique identifiers are in fact issued uniquely (one per person) and resistant to fraudulent use. In this way, biometrics will emerge an essential tool to combat identity theft at its source and suppress derivative opportunities to commit fraud.

Biometric identity proofing will emerge as a key identity fraud prevention approach; a means to validate the integrity of identity information at the time of collection. It will complement biometric authentication, enabling a higher degree of trust in the validity and uniqueness of the identity being claimed.

Biometrics-as-services provided on a subscription or pay-per-use basis will be increasingly adopted by organizations that demand better security and identity fraud prevention measures but for whom the costs and risks of deploying their own bespoke biometric solutions are a less attractive alternative.

About Aware, Inc.

Aware is a leading global provider of biometrics software products, services, and solutions. Our products include all the software components necessary to rapidly and cost-effectively build a solution to collect, manage, and utilize identity data for biometric identification and verification: SDKs, controls and applets; user interface applications for biometric enrollment and forensic analysis; fingerprint, face, and iris matching SDKs; text search and identity analytics SDKs; a middleware and workflow platform; and a cluster computing platform. These products fulfill critical biometric functionality for a variety of applications including border management, law enforcement, defense, intelligence, banking, and payments. Aware is a publicly held company (NASDAQ: AWRE) based in Bedford, Massachusetts.

Sources

Forrester Research. (2015). SaaS software subscription revenue by category.

GSMA Intelligence. (2015). The Mobile Economy.

IDG Enterprise. (2015). Computerworld Forecast Study.

AWARE

Please contact Aware or visit our website for additional information:

sales@aware.com
www.aware.com