White Paper

Addressing New Identity Fraud Challenges and Embracing Innovative Solutions

AWARE

781.687.0300 | sales@aware.com | www.aware.com

Aware is a leading global provider of software products and solutions for biometric identification and authentication. They are used for variety of applications including financial services, enterprise security, border management, and law enforcement. Aware is a publicly held company (NASDAQ: AWRE) based in Burlington, Massachusetts.

The Challenge of Stopping Identity Fraud

In the era of the rising of digital transactions, identity fraud has become a persistent and escalating threat with significant consequences for individuals, businesses, and governments globally. The proliferation of personally identifiable information (PII) through social media and public sources, coupled with the anonymity of online interactions, has empowered fraudsters. Over the years, the landscape of identity fraud has continued to evolve, necessitating advanced strategies to combat this trillion-dollar problem. While past approaches may still hold relevance, new technologies and tactics are shaping the future of identity fraud prevention.

Using Biometrics to Prevent Fraud and Protect Identities

Identity theft continues to be the primary cause of financially motivated fraud. With the proliferation of digital operations and the ease of online transactions, sophisticated criminal organizations exploit vulnerabilities in the system, often operating beyond outdated legal frameworks. Large-scale data breaches continue to cause frequent incidents of significant identity theft, with many remaining undetected. The rise of synthetic identity fraud, where fictional identities are meticulously constructed, presents a significant and rapidly growing challenge.

Biometrics: A Crucial Tool in the Fight Against Identity Fraud

The integration of liveness detection into mainstream security practices has accelerated over the past few years. Facial recognition technology embedded in smartphones has become a standard for secure access. Additionally, liveness authentication capabilities in operating systems have paved the way for secure access to external platforms using facial, voice, and iris recognition. Liveness detection possesses unique attributes that make an effective barrier against fraud, offering an additional layer of security beyond traditional authentication methods.

Beyond Authentication: The Expanding Role of Biometrics

While biometric authentication on personal devices has gained traction as a user-centric measure, a more comprehensive approach is necessary to tackle identity fraud globally. Recognizing the limitations of relying solely on device-based authentication, cloud-based biometric identity proofing and authentication services emerge as a promising avenue. This shift aims to address the diverse challenges of identity fraud in various scenarios, including the financial sector, government agencies, and retail establishments.

Here's why:

SYNTHETIC IDENTITY FRAUD:
The prevalence of synthetic identities requires strategies beyond simple authentication. Biometric verification alone doesn't tackle this form of fraud effectively.

IDENTITY VERIFICATION:
Biometric verification confirms the identity of the person authenticating, not the authenticity of the identity data itself. This gap leaves room for establishing accounts using fraudulent information.

DEVICE PENETRATION:
The use of smartphones is still on the rise and a substantial portion of the population uses them regularly. Universal solutions are necessary to combat identity fraud across all demographics.

STANDARDIZATION AND SECURITY:
Authentication on smartphones is limited by the device's implementation, its operating system, and the application providers. Standardizing architecture and interfaces are the goal of organizations, but biometric functionality and performance cannot be universally configured on these devices. Moreover, these constraints can lead to security issues for particular applications.

Fundamentally, relying on stronger passwords is not enough to ensure security. Robust security and trustworthy identity verification are necessary for various types of accounts, applications, and environments.

Biometric Services: A Path Towards Universal Accessibility

Biometric as a Service provides a comprehensive solution to prevent identity fraud, with easy accessibility. They democratize the industry by reducing costs, providing predictable expenses, and fostering competition among providers. These services cater to diverse needs, host clouds, supporting various biometric modalities, and transforming the identity verification industry.

Biometric Identity Proofing Safeguarding Data Integrity

Biometric identity proofing safeguards data integrity by verifying identity data during enrollment using biometric data and comparing it against existing records. This process flags duplicate enrollments and prevents fraudsters from establishing false identities, establishing trust in the authenticity of enrolled biometric data and making it an effective preventive measure against identity fraud.

In-Band and Out-of-Band Biometric Authentication

Biometric authentication can be done either in the same communication channel as the transaction (in-band) or through a separate, independent channel (out-of-band). Both methods provide enhanced security, with out-of-band authentication adding an extra layer of protection through diverse access channels.

Device vs. Server-Based Authentication

When it comes to authentication, it is important to decide whether to store and compare biometric data on the user's device or a central server. FIDO, which is device-centric, conducts comparisons on the device itself, reducing the risk of mass breaches. However, stolen devices can pose fraud risks. On the other hand, the centralized server model involves storing data on a server for control, which can lead to trust concerns if biometrics are compromised. Nevertheless, counterfeiting biometrics is a complex task, and with new tech and anti-spoof measures, it is challenging for fraudsters to exploit biometric security breaches.

Strengthening Identity Fraud Prevention

A leading bank in Latin America implemented biometrics to enhance its security measures against vector attacks and ensure a seamless and secure customer authentication experience. By adopting biometrics, they avoid the upfront investment in biometric enrollment and data storage equipment and software, eliminating the potential risks and costs associated with maintenance and technological obsolescence. This strategic move aligns with their commitment to safeguarding customer identities and transactions.

The Aware solution emphasizes the critical importance of identity proofing to establish the identity of individuals applying for new accounts and transactions. This ensures that the collected biometric data is of high quality and securely linked to trusted identity information, minimizing any ambiguity or potential errors. The system supports a range of biometric modalities, including fingerprint, face, iris, and voice recognition, offering flexibility and comprehensive security options.

How Aware solution solved injection attack at leading bank in Latin America:

ENROLLMENT AND IDENTITY PROOFING:

Upon signing up for the bank services, customers are directed to the authenticator. During this process, customers provide proof of identity in accordance with the bank's requirements. The solution steps conduct identity-proofing and collect the necessary biometric data. This data is vetted and linked to the customer's identity information. When customers enroll in the bank's services, they go through an identity proofing process. This involves providing proof of identity and collecting biometric data, which is verified and linked to the customer's identity information.

DATABASE SEARCH AND VERIFICATION:

The collected biometric data is stored securely within the bank's server. When a customer initiates a new account application or a transaction requiring biometric authentication, the system searches the database for existing enrollments. If any conflicts or inconsistencies arise, further investigation is triggered. However, if the information aligns without conflicts, the enrollment is updated and assigned.

SEAMLESS CUSTOMER AUTHENTICATION AND MATCHING:

Customers can effortlessly authenticate themselves using their mobile devices by submitting their personal biometric data. If the customer's identity information matches, it is retrieved from the system, ensuring accurate and trusted identification.

CUSTOMIZABLE SECURITY OPTIONS:

The application offers a range of customization options to adapt to different customer requirements, performance benchmarks, privacy preferences, and security needs. These options include selecting specific biometric modalities, choosing single or multiple modalities, and deciding whether to store biometric data in the bank's private cloud or server.

PERFECT USER EXPERIENCE:

The solution's backbone is a sophisticated management platform coordinating security and workflows with seamless user experience.

The leading bank in Latin America has strengthened its security infrastructure against vector attacks, fraud, and unauthorized access by integrating Aware's solution. This not only enhances customer trust through accurate identity verification but also provides the flexibility to adapt to changing security needs and technological advancements, ensuring a resilient and seamless banking experience for its valued customers while prioritizing innovation and security.

Looking Ahead: The Future of Biometrics in Identity Fraud Prevention

As we navigate the complex landscape of identity fraud, it is evident that biometrics have emerged as a pivotal weapon in the fight against this pervasive threat. The fraud prevention advancements represent crucial strides toward a more secure and resilient digital ecosystem. However, the journey doesn't end here; instead, it continues to evolve as technology, fraud tactics, and user expectations undergo transformation.

The path for biometrics in identity fraud prevention is paved with opportunities and challenges. As we peer into the future, several key considerations come to light:

CONTINUOUS INNOVATION: The realm of biometrics is far from static. Innovations will continue to redefine what's possible. From multi-modal biometric fusion to AI-driven behavioral analysis, the next wave of technologies promises even more accurate, adaptable, and user-friendly solutions.

EVOLVING THREAT LANDSCAPE: Fraudsters, too, will adapt. As biometric systems become more sophisticated, so will attempts to breach them. We must anticipate evolving attack vectors and stay ahead by enhancing not only the strength of our defenses but also the depth of our vigilance.

PRIVACY AND ETHICAL CONCERNS: With the growing reliance on biometric data, privacy and ethics will remain at the forefront. Striking the balance between security and individual rights will require ongoing dialogues and careful considerations to ensure that biometric solutions remain both effective and respectful of personal privacy.

INTEROPERABILITY AND STANDARDIZATION: The adoption of biometrics across industries and platforms calls for increased interoperability and standardized practices. Collaborative efforts will be instrumental in establishing cohesive frameworks that enhance security while reducing user friction.

NEXT GENERATION OF USER-FRIENDLY DEVICES: The success of biometric systems hinges on user acceptance and education. Empowering users to understand the nuances of biometric technology, its benefits, and potential limitations will foster a more informed and cooperative user base.

REGULATION AND GOVERNANCE: Regulatory bodies worldwide are grappling with the implications of biometric technology. As these frameworks mature, they will provide essential guidelines for organizations to ensure ethical use, data protection, and compliance with evolving legal landscapes.

Finally, as we continue to address identity fraud challenges and embrace innovative solutions, the role of biometrics will be pivotal. They have the potential to revolutionize the way we authenticate, verify, and interact in the digital realm. While we can't predict every twist and turn, one thing is clear: the path forward involves safe technology, adaptability, and a steadfast commitment to securing the identities of individuals, businesses, and governments around the globe.

AWARE

781.687.0300 | sales@aware.com | www.aware.com