



## AuthenWare® Solutions for Financial Services - North America

### Background

Online banking is growing rapidly, and is creating new business opportunities for financial institutions. Unfortunately, online fraud is growing at an even faster pace, primarily due to user impersonation. The existing method of verifying a user through a username/password and challenge-response questions is simply not working. To prevent losses, avoid regulatory action and prevent erosion of end-user confidence, financial institutions are seeking better ways to ensure the security of online banking.

Since so many instances of fraud are based on the use of stolen credentials, a growing number of regulatory bodies and industry groups are calling for stronger authentication. Examples abound: the Federal Financial Institutions Examination Council (FFIEC) Authentication in an Electronic Banking Environment Guidance requires strong web banking authentication; Section 404 of the Sarbanes-Oxley Act (SOX) calls for stringent internal controls; the Gramm-Leach-Bliley Act (GLBA) Section 501(b) mandates that financial data be protected from unauthorized disclosure; the Fair and Accurate Credit Transactions Act (FACTA) Red Flag Rules Sections 114 and 315 target the prevention and detection of identity theft through strong authentication, and Payment Card Industry Data Security Standard (PCI-DSS) requirements were designed to enhance payment account data security. Each of these regulations calls for strong authentication, with a focus on two-factor or multi-factor authentication.

### Challenges

One of the most important challenges for financial institutions is to balance conflicting needs: deterring fraud, strengthening the relationship with online customers, and ensuring they are in compliance with regulations. For several years, it appeared that simply implementing two-factor authentication – using hardware tokens, digital certificates and the like – would be the answer. Unfortunately, not only do these methods not fully deliver on their promise, as evidenced by the increasing incidence of fraud, but they also present many hidden expenses including capital and deployment costs, and enormous help desk overhead. Customers find them cumbersome and error-prone, and are increasingly asking for an additional layer of biometric identification (such as those based on iris scans or fingerprints.) According to a recent study, fully 59% of Americans say they would support biometric identification, especially if it did not call for additional hardware to be installed on their systems.

### AuthenWare® helps you:

- Reduce fraud
- Improve overall security
- Provide optimal customer experience
- Reduce costs
- Satisfy regulatory requirements



## Solution

AuthenWare® is a breakthrough approach that meets this challenge head-on. A second-factor authentication system, it combines keystroke dynamics and other heuristics to cost-effectively meet the needs of both compliance and customer satisfaction.

AuthenWare finds and stops fraud in online banking and internal applications through advanced biometrics; working in concert with existing authentication and validation methods, it ensures that the user is the valid owner of the credentials presented. It adds a real-time online dimension to existing identity validation checks, yet it is completely transparent to customers, and it adds zero impact to the production implementation.

## How it Works

AuthenWare incorporates a breakthrough, multi-dimensional approach to validate identity. Using a series of security algorithms that record and measure a person's unique keyboard typing patterns, as well as other behavioral and environmental heuristics, the product creates a personal security pattern – known as the AuthenWare Singularity Pattern™ – that is as unique as the person's fingerprint. Based on a series of statistical singularities (aspects that distinguish one person from others), the pattern can even adapt to nuances in behavior such as those caused by too much caffeine, injured fingers, etc. Each time the valid user logs into their online banking system, their login characteristics are compared to the AuthenWare Singularity Pattern, and if it is mathematically similar, the authorized user is granted access. But for an imposter who has obtained usernames, passwords or other authentication information, access will not be granted, since their pattern will not resemble that of the valid user.

This innovative technology overcomes the limitations of other two-factor or multi-factor authentication approaches because it can be deployed instantly to massive numbers of customers, it requires no additional hardware, and it is totally unobtrusive. There is nothing to lose, nothing to forget, and no reason to call the help desk.

AuthenWare works in the background, ensuring that the person accessing a particular account is really the account owner and not an interloper.

### **AuthenWare in Action – Widespread Adoption**

A multi-national retail bank was sending tokens to online customers as a means of implementing stronger authentication than a simple username/password. This process was enormously expensive, at approximately \$30 per token; in addition, many users called the help desk each day to ask for assistance. In order to avoid the high costs and intense resources required to support the use of tokens, the bank selected AuthenWare. The bank's management team was pleasantly surprised to find that not only did costs drop, customer satisfaction soared and the incidence of fraud dropped significantly. The widespread adoption of the AuthenWare solution enabled the bank to meet regulatory requirements more reliably and consistently than with previous solutions, and at a lower cost.

## AuthenWare Reduces Fraud

Financial institutions find that adding keystroke dynamics to the authentication process can reduce fraud, protect private information, and elevate the security of online banking. Other biometric authentication methods rely on simplistic information such as identification of the client device or geolocation, but are easily spoofed by man-in-the-browser attacks. AuthenWare relies instead on an entire series of biometric security algorithms that reduce the possibility of spoofing to the lowest levels in the industry.

### **AuthenWare in Action – Consistent Application of Regulations**

An attacker put up a fake bank website and lured the user to the site, tricking him into giving up his username and password. The hacker later used those credentials to attempt to access the real user's bank account. Once the hacker had gone through the initial login process, AuthenWare compared his keystroke signature with the actual user's AuthenWare Singularity Pattern, and then notified the bank security team that something was amiss. The team was able to both protect the account and monitor the activity, making real-time decisions and gathering forensic information for further investigation. Not only was the bank in compliance with FFIEC and FACTA requirements for strong authentication, it was able to provide audit trails to demonstrate internal controls (Sarbanes-Oxley) as well as protection of personal data (Gramm-Leach-Bliley Act).

### **AuthenWare Improves Overall Security**

The AuthenWare use of multiple factors means that theft or impersonation of one authentication factor is mitigated by the strength of other factors. Because AuthenWare relies on a preponderance of evidence, there is no single point of failure. The results of the AuthenWare validation can be tied to secondary rules, such as those based on transaction value, creating an even stronger security safety net. In addition, the pattern that is produced through AuthenWare is not closely linked to personal information, so even if the database were to be compromised, the thief would have only have a portion of the information needed to perpetrate fraud. As an additional point of validation, the AuthenWare solution has been certified by the International Biometric Group and Common Criteria.

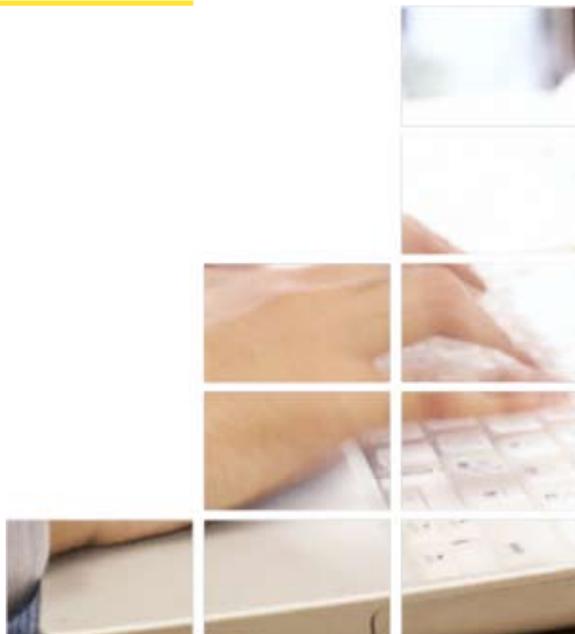
### **AuthenWare Provides Optimal Customer Experience**

No matter how effective an authentication scheme is, if it is not accepted by users it is useless. AuthenWare boasts an extremely high customer satisfaction rating. Because the technology operates in the background, unobtrusively, without requiring the user to buy, remember or do anything unusual, AuthenWare now has more than 70 million users around the world. Customers using AuthenWare see no difference in their everyday

---

*This innovative technology  
overcomes the limitations of other  
two-factor or multi-factor authentication  
approaches because it can be deployed  
instantly to massive  
numbers of customers,  
it requires no additional  
hardware, and it is  
totally unobtrusive.*

---



interaction with the online banking site. But in the background, AuthenWare is checking their keystroke patterns and other aspects of their behavior, and matching against a stored AuthenWare Singularity Pattern. Due to the statistical accuracy of the comparison, the system can even accommodate nuances in behavior such as those caused by medication, injury or fatigue.

### **AuthenWare Reduces Costs**

AuthenWare provides high confidence at a very low cost throughout the lifecycle. Acquisition costs are much lower than other biometric approaches, such as iris scanners or fingerprint readers, and it eliminates the logistical costs with these and other approaches such as digital certificates. Implementation is easy: simply install AuthenWare and integrate the rules into existing applications to support existing policies and practices. One of the biggest positive impacts comes with the reduction of help desk costs; by reducing false positives through advanced scoring algorithms, the reduction in help desk calls is dramatic. With AuthenWare, help desk calls are virtually nonexistent.

#### **AuthenWare in Action – Low Total Cost of Ownership**

A bank augmented its traditional username/password scheme by adding downloadable digital certificates to a user's home computer. This approach worked until the user decided to login to his bank account from another computer. The authentication system detected that the user was logging in from an unusual system. Before AuthenWare, the bank would have had to send a series of challenge-response questions to the user, or generate and transmit an out-of-band one-time password. With AuthenWare, those intermediate steps were not necessary. AuthenWare checked the typing pattern and applied other heuristics, and was able to validate the user. Only when the user attempted a transaction that exceeded a specific value did the bank need to send an out-of-band message.

### **AuthenWare Satisfies Regulatory Requirements**

AuthenWare not only satisfies the requirements of FFIEC, GLBA, SOX, FACTA and other regulations, it does so in a way that fosters user adoption and actually increases the level of compliance. The easier an authentication method is to use, the more likely users will embrace it as part of doing business, and will not seek to bypass it. This makes it much easier for financial institutions to apply regulations much more consistently, and to support regulatory compliance at a much lower cost. AuthenWare boasts more than 70 million users worldwide, a testament to its ease of use and transparency and, ultimately, utility.

### **Conclusion**

Financial institutions have long recognized that, in the war on fraud, verifying user identity is the weakest link. The old methods of verifying identity are not working, but most newer multi-factor approaches that seek to satisfy regulatory requirements engender customer dissatisfaction – and fail to stop fraud in the bargain. AuthenWare provides a breakthrough approach to reducing fraud while actually strengthening the institution's relationship with its online customers. It works in concert with existing products, approaches, policies and practices to achieve the right balance of reducing fraud risk while instilling customer confidence in online banking. Moreover, it provides the same level of confidence for any internal application as well.

### **About AuthenWare®**

AuthenWare® Corporation is a leading cybersecurity software provider focused on fighting identity theft. The Company's innovative tokenless authentication system delivers strong security through a combination of keystroke dynamics, behavioral and environmental characteristics to minimize identity theft, web fraud and other system vulnerabilities. The AuthenWare solution creates a unique personal security pattern that recognizes authorized users while keeping hackers out. AuthenWare is headquartered in Miami, FL, with offices around the world. Tens of millions of people use the company's products every day in a variety of industries, including financial services, government, healthcare, telecommunications and online retailers.

For more information, visit [www.authenware.com](http://www.authenware.com).



### **AuthenWare Corporation**

1221 Brickell Avenue, 9th Floor  
Miami, Florida 33131  
T: +1 305 377-8768  
F: +1 305 374-6146  
[info@authenware.com](mailto:info@authenware.com)  
[www.authenware.com](http://www.authenware.com)