Industry Overview

The threat landscape around financial data security continues to escalate. International tensions and state sponsored terror groups and cybercriminals attempt to undermine the public regarding security and sustainability of markets and online trading.

While there has been much focus on application and network hardening, over 81% of data breaches result from exploiting weak or stolen credentials.[1] Efforts to enforce long and complex passwords or requiring users to periodically change their passwords always results in a negative user experience and increases the risk users will write down their passwords. Couple this with two-thirds credential re-use[2] and the massive number of data breaches across all industries, and IT security professionals must now operate with the assumption that nearly all their customer/user credentials are already known to the hacking community or can be easily discovered.

With almost all retail and business banking being done on-line, the need to provide both seamless user access and increased authentication security has never been higher. Furthermore, higher risk transactions beyond the login require additional scrutiny within applications.

What Should You Do?

Guidance from FFIEC clearly states that IT Security should implement a risk-based, layered security approach.

In June of 2011, the Federal Financial Institutions Examination Council (FFIEC) updated their position on adequate controls for authentication and minimum expectations for authentication of web and mobile authentication in a supplement to their *Authentication in an Internet Banking Environment* guide. The FFIEC recognized that a layered security, risk-based approach is necessary and must move beyond simple device identification, such as IP address checks, static cookies and challenge questions derived from customer enrollment information, to complex digital device fingerprints and other out-of-wallet authentication factors.

The reality is that all security professions know this. So why don't all on-line services implement a layered security approach that directly addresses 95% of the problems? The answer is simple: all but one available marketplace solution has one or more serious drawbacks.

- The licensing fees of most adaptive solutions are simply out of line with protecting thousands or millions of accounts.
- The solutions upset users by requiring them to jump through additional hoops every time they log in resulting in a poor user experience and negative brand halo.
- The solutions require physical tokens which are expensive and impractical to deploy and manage with large user groups.
- The solutions lack the ability to align transaction and/or user risk with the appropriate additional layers of authentication and the capability to monitor and evaluate risk analytics.

aPersona's Adaptive Security Manager™

aPersona's Adaptive Security Manager™ (ASM™) is an affordable *and* scalable, adaptive multi-factor authentication solution. ASM™ provides adaptive learning using patent-pending Patterns of Behavior (PoB) technology and a customized set of factors that can be dialed-in and tuned to reach any required level of risk and compliance. These additional factors include:

- 3D Behavioral Modeling (Device Forensics, Geo Spatial, Time)
- Public and Private Network Behavioral Geo Location
- Progressing Invisible one-time-use Soft Tokens
- Behavioral Device Forensics (ASM™ device IDs consider over 100 device factors including IoT connected devices on mobile)
- Behavioral Learning by user, device, transaction and security policies
- Security Policy Thresholds

[1] 2018 Verizon Data Breach Report

[2] Ibid.

- User-specific behavioral risk level over-rides
- “Man-in-the-middle” Detection
- “Jail Broken” Device Detection
- Real-Time Risk Analytics

aPersona operates with multiple modes, including invisible adaptive learning, invisible monitoring risk without challenging users, and full adaptive risk challenge mode which is nearly always completely invisible. Adaptive Security Manager™ can be deployed on premise or in the cloud with a very small resource footprint, monitor transactions from any number of applications, challenge where needed, and is continuously learning. Thus, ASM is able to match your data risk requirements, reduce your data breach exposures, and easily adapt to changing regulations over time all at a price point that scales well to millions of users.

The aPersona ASM™ allows identity and access security professionals to easily implement a layered security approach and exceed the authentication requirements of FINRA and the FFIEC while preserving a great user experience. Add to that the lowest total cost of ownership in the industry, and ASM™ delights IT professionals, risk management, and the CFO.

Industry Use Cases

Use Case 1: Web or Mobile Banking Portal Login
Brokerage client, Ima Smarty, needs to log into her client management portal from her home office so she can check her accounts and pay a few bills prior to heading into her office.

Ms. Smarty navigates to the secure web page for access to her accounts. She logs in using her username and password. Once her username and password are confirmed, aPersona ASM™ evaluates the transaction factors and verifies that her login pattern of behavior is allowed. Ms. Smarty is seamlessly allowed access into her portal. The whole process has been transparent to Ms. Smarty and occurs in milliseconds.

If the pattern is not recognized by ASM™ as one associated with Ms. Smarty’s normal behavior, she is sent a one-time password via email, SMS, or phone call to confirm her identity. Once confirmed, the system learns the confirmed scenario as a valid pattern of behavior for Ms. Smarty for future logins.

Use Case 2: Fraudulent Web or Mobile Banking Portal Login
Somehow Ms. Smarty’s credentials have been purchased on the black market by a cybercriminal looking for easy money.

With a small amount of effort, the fraudster tries Ms. Smarty’s credentials on banking portals. He gets a hit and attempts access. However, because ASM™ does not recognize this pattern of behavior via its adaptive multi-factor evaluation, a one-time password is sent to Ms. Smarty. This alerts her to the fraudulent attempted access and ASM™ reports the thwarted fraud attempt to the Bank’s IT Security department.

She notifies the helpdesk immediately. The helpdesk fraud team is able to view the ASM™ reports and sees not only the IP address of the fraudster, but multiple machine forensics from the fraudster’s computer. The fraudster has been stopped and Ms Smarty’s

personal data and accounts are safe! She also has a tremendous sense of security and pride and loyalty knowing she has chosen a bank that is concerned about her security and taken steps to ensure her information is kept safe.

Use Case 3: Fraudulent BillPay Payee

Ms. Smarty unwittingly opened an email attachment she thought was from a legitimate source causing her computer and browser to be compromised.

With a small amount of effort, the fraudster opens a parallel online banking session using Ms. Smarty's computer as the proxy. He attempts to add a fraudulent company as a BillPay payee. However, Ms. Smarty's bank has implemented a layered security approach using the aPersona® ASM™. Because ASM™ recognizes that this payee is being configured manually rather than one selected from the known payees to the bank, a one-time password is sent to Ms. Smarty asking for confirmation to add this BillPay payee. This stops the fraudster in his tracks, and alerts Ms. Smarty to the fraudulent attempted access and ASM™ reports the thwarted fraud attempt to the Bank's IT Security department.

She notifies the helpdesk immediately. The helpdesk fraud team is able to view the ASM™ logs and see that someone has compromised Ms. Smarty's computer. She is told to disconnect her machine from the Internet immediately and take her computer to an IT professional for remediation. The fraudster has been stopped and Ms Smarty's personal data and accounts are safe! She also has a tremendous sense of security and pride and loyalty knowing she has chosen a bank that is concerned about her security.

For more information on how aPersona's Adaptive Security Manager™ can help your organization exceed the authentication requirements of FFIEC and NCUA today, contact us at 1-919-584-5098 or sales@apersona.com.