passfaces™
STRONG AUTHENTICATION

Passfaces and the 2005 FFIEC Guidance

The Federal Financial Institutions Examination Council guidance for "Authentication in an Internet Banking Environment", published October 2005, highlights the importance of risk management in the provision of online financial services. Technologies are not themselves compliant or non-compliant with this guidance; it is the financial institutions that must demonstrate compliance. To that end, they seek out technologies that will help in executing the risk management strategies they determine to be necessary. The guidance does not require or endorse any particular technology as a solution. In fact the appendix nods to many new point solutions that can play a part in larger security solutions. It does recommend that banks implement enhanced authentication because the continued reliance on username/password alone is no longer considered sufficient to protect access to either personal information or financial assets. At the heart of this criticism is the fact that passwords are embarrassingly vulnerable socially: users share, lose, give away, and forget them. The document also acknowledges that the institutions must find solutions that are commercially reasonable. "An effective authentication method should have customer acceptance, reliable performance, scalability to accommodate growth, and interoperability with existing systems and future plans."[1]

Passfaces™ provide an alternative to the password that eliminates the social weaknesses discussed above while still providing an authenticator that is low in cost to distribute, scalable, and easily managed in consumer facing applications. Passfaces are easily recognized by the secret owner but are difficult to describe, and are all but impossible to guess or give away. According to cognitive psychologists, recognition is the strongest form of memory, as compared to recall or even cued recall. In fact, since the capacity to recognize familiar faces is so well developed, there is no need for the user to write down anything in order to use Passfaces reliably. This distinction is core to the Passfaces technology. And most importantly, like the password, they authenticate the presence of the person, not the presence of a hardware device or a piece of software.

This innovative technology provides an enhanced authentication that should be considered in any risk management strategy for online financial services. User confidence, the practicality and cost of the complete solution, and the value added to the defensive stance are all served well by Passfaces. What's new here is that this innate ability has never before been tapped as a means of authentication. Why introduce consumers to unfamiliar, often cumbersome, authentication tasks when you can harness a natural talent that is present regardless of age, education, or language?

The FFIEC guidance urges the exploration of new technologies and urges financial institutions and technology service providers to review and make use of those that add value within the business risk management profile required for safe online financial services. These are business decisions first and foremost. Passfaces is designed to provide improved security and enhanced customer confidence with almost no impact on existing system design. More information on how Passfaces can facilitate your business needs within the context of these federal guidelines is available at www.passfaces.com.

[1] FFIEC Guidance, Authentication in an Internet Banking Environment, October 12, 2005 FIL-103-2005, pg.3.