



Advanced Authentication Frequently Asked Questions

Product Overview

Q: *What is Advanced Authentication?*

A: Advanced Authentication (formerly referred to as PassMark Security) is a new module to substantially increase security of the Internet Banking, Cash Management and Bill Pay applications. This solution is intended to meet the guidance released in October 2005 by the Federal Financial Institutions Examination Council (FFIEC), which specifically states that financial institutions regulated by FFIEC agencies should move beyond single factor password authentication.

Q: *Why did Fidelity introduce this new module?*

A: Online security is something that Fidelity ePayments' takes very seriously. We are committed to providing the most technologically advanced security options in the industry. Online 'phishing' and 'pharming' attacks have become the latest tools of fraudsters attempting to leverage technology to gain access to personal and private financial information. Fraudsters use information gained through various scams and match it with "phished" information to gain unauthorized access to consumer's data and accounts. By offering Advanced Authentication and other security enhancements, Fidelity is taking an active role in helping financial institution clients to combat these emerging fraud techniques.

In selecting our advanced security approach, Fidelity's objective was to deliver a solution that is convenient, consumer friendly, flexible, and capable of addressing consumer concerns. The solution also had to be adaptive to address the evolving threats for years to come and allow Fidelity's clients to stay competitive in their markets. In addition, we looked for partners with a proven deployment record and financial institution clients deployed in production. After reviewing the leading security solution providers, Fidelity chose to incorporate the PassMark Security (now RSA Security) technology into its Online Banking and Bill Pay solutions.

The integrated Fidelity solution delivers transparent authentication utilizing device identification and real-time, risk based authentication techniques. This prevents a fraudster from using stolen login credentials by requiring a second factor of authentication. In addition, the system validates the online banking site to the user with personalized images and phrases. This helps the customer know when it is safe to provide login credentials.

Q: *What are the key features of Advanced Authentication?*

A: The Advanced Authentication solution provides Risk-based and Site-to-user authentication as part of its layered online security system:

- **Risk-Based Authentication.** This is a behind-the-scenes technology that positively identifies a user's computer and treats it as a credential, turning the computer into a reliable "second-factor" for authentication as required by the new FFIEC guidelines. The system then continues to perform a comprehensive real-time risk assessment of each subsequent login and assigns a risk score based on the likelihood of that login being fraudulent. When an activity is deemed high-risk, the user may be challenged with a

secondary form of authentication.

- **Site-to-user Authentication.** This is a mechanism for inspiring consumer confidence in the online channel. This is achieved by ensuring users that they are transacting with your genuine online banking website through the use of a personalized image and phrase that has been selected by the user and becomes the shared secret between the user and the financial institution. Users are instructed to only enter their password after the financial institution has proven its authenticity by displaying the image and phrase, thus deflecting phishers from easily harvesting passwords.

Q: *What are the benefits of incorporating Advanced Authentication into my current Online Banking and Bill Pay service?*

A: In addition to providing one of the best possible multi-factor user experiences, the increased consumer confidence from the “visible” site-to-user authentication has been shown to directly result in higher bill pay adoption, increased consolidation of assets, and a greater likelihood of embracing other online financial services, thereby driving down costs for the financial institution.

Advanced Authentication Implementation

Q: *If my institution has already purchased Advanced Authentication, when will my implementation begin?*

A: Implementation will begin during the month of November 2006. The integration project is nearing completion with plans to beta the new module in production this month. Once the beta process is complete, implementations will be performed on a controlled schedule to balance the number of clients and users rolled out on the throughout the remainder of the year. Implementation will be prioritized based on each financial institution's contract date and desired implementation date. Clients will be notified of their implementation schedule within the next 2 weeks.

Q: *What is the first step in the Advanced Authentication implementation process?*

A: An Implementation Project Manager will contact your institution to start the implementation process. Upon completion of the introduction call, the Project Manager will e-mail a project plan listing timeline, key deliverables, and estimated go-live date.

Q: *What will the Advanced Authentication implementation process include?*

A: The implementation process will include a project plan listing items such as: initial Online Banking site set-up and enrollment configuration, demo site updates, data mapping and infrastructure review, customer migration, as well as customer maintenance and ongoing support training.

Q: *How long is the average Advanced Authentication implementation?*

A: Advanced Authentication implementation project timelines are expected to be fairly short. The average timeframe is expected to be 30 days from start to finish.

Training and Marketing

Q: *What type of training will my institution receive regarding Advanced Authentication implementation?*

A: During the implementation process, your financial institution will receive a new client upgrade and product launch training session, which will cover topics such as a product overview, administrative functions, and customer maintenance and support. This training will be conducted online at no charge to your institution.

Q: How will my institution train our employees?

A: Fidelity will provide a free online 'train-the-trainer' webinar class that will review the Advanced Authentication product in relation to what your employees need to know. Each institution will also receive a copy of the training presentation to conduct themselves at their convenience. For those institutions participating in an end user marketing program, a professional Fidelity trainer will perform the online employee training session at no charge for the financial institution employees.

Q: What end-user marketing materials are available to help my institution market Advanced Authentication?

A: Fidelity offers an extensive end user marketing program to all institutions purchasing the Advanced Authentication product. Our marketing experts help each institution manage the campaign from beginning to end. We'll also help train your employees and monitor the campaign results.

Items included in the marketing program are as follows:

- Announcements and communication to existing Online Banking and Bill Pay users
- Complete branch campaign including brochures, posters, and more!
- Direct mail piece, newsletter articles, and online marketing collateral

See the Marketing Resource Guide for additional detail.

Ongoing Support

Q: Once my site is live with Advanced Authentication, who does my institution contact for questions and ongoing support?

A: Upon launch of your Advanced Authentication service, your current Online Banking Account Manager will also assist you with any ongoing questions, assistance, or support related issues. Your Implementation Project Manager will introduce you to your assigned Support Representative prior to your service going live.



Please feel free to contact your Fidelity Strategic Account Manager [SAM] with any questions. If you need to verify the contact information for your SAM, please contact Paul Wiggins at 678-576-4243 or paul.wiggins@fnf.com.