

Multi-Layered Approach for Increased Security and Customer Confidence

Improving the overall security of consumer-facing services is vital to financial institutions. The risk of doing business with unauthorized or incorrectly identified persons in an Internet environment can result in financial loss and reputation damage. Online financial services customers need confidence that their financial institution is protecting confidential personal information and account access. Financial institutions therefore need to not only improve security, but bolster customer confidence in order to drive adoption of their online brokerage channel.

Scivantage has developed a suite of layered solutions that include customer-facing assurance, multi-factor authentication and risk evaluation services that improve security without increasing complexity for customers. The rapidly deployable solutions can be configured to meet the most demanding needs of financial institutions.

Scivantage's Multi-factor Authentication solution is a system where two or more different methods are used to authenticate a user to a web site. Using two or more factors as opposed to a single set of credentials (such as User Name/Password) delivers a higher level of authentication assurance.

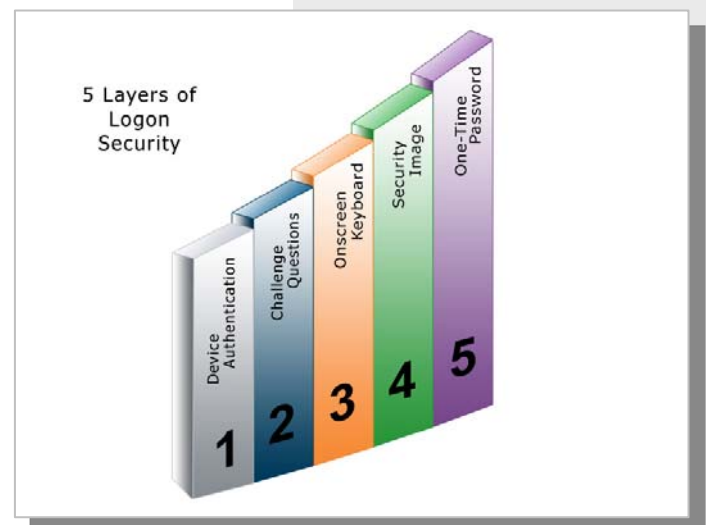
Available as a component of Scivantage Investor or as a standalone application that can be integrated into an existing third-party platform, the Scivantage Multi-Factor Authentication solution provides a set of strong authentication services, including these four critical components:

- ▶ Device Authentication
- ▶ Challenge Questions
- ▶ On-Screen Keypad
- ▶ Security Image

Offering flexible deployment options, this powerful solution requires no additional software to be installed on a customer's PC and it offers visible proof of increased security to raise customer confidence in the safety of the online brokerage channel.

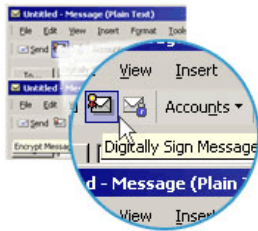
BENEFITS

- Multi-layer approach to prevent online fraud and identity theft
- Protects investor's personal data from intelligent attacks like phishing, key loggers, spyware, malware, man-in-the-middle
- Builds customer confidence and allows them to execute secure business transactions through online brokerage channel
- Proprietary methodology and technology built on a foundation of stringent security policies and rigorously tested technologies
- Modular design allows for rapid deployment and integration with Scivantage Investor or existing third-party platforms
- Solution suite continuously monitored and evolving to stay ahead of the latest fraud techniques



Scivantage's multi-factor, multi-layered security services provide unparalleled protection of a customer's online identity while maintaining the familiar user experience of entering a username and password.

▶ **Device Authentication**



The **device authentication** feature is designed to remember a customer's computer and assigns a unique identifier to each computer using a standard cookie encrypted with a set of data points about that particular computer's settings.

▶ **Challenge Questions**

The **challenge question** feature is comprised of two different sets of questions: secret questions where the user selects three questions and provides answers for each; and account-based questions where the system generates questions based on the user's account registration information. Embedded in this feature are three critical logic features:

- ▶ Randomness of answers, including the possibility of 'none of the above' being correct.
- ▶ Randomness of questions
- ▶ Questions are presented as images to limit the effectiveness of screen scraping malware by fraudsters

▶ **On-Screen Keypad**



The **on-screen keypad** feature has been employed to protect the user against key-logging malware. The user uses his mouse to enter their password on the keypad and then selects 'login' to gain access to the account. The keypad has been built using Flash so the feature itself, as well as the password provided, have been encrypted.

▶ **Security Image**

The presence of a user selected **security image** is a feature that has been employed by many banks in recent years and has been very successful. The purpose of the feature is to allow the site to be visually authenticated to the user. By seeing the image, the user can be certain that the site they are attempting to visit is the real site. We have embedded the image as part of the on-screen keypad flash object to prevent the possibility of the image being copied and used to fraudulently gain access to a user's account.