

Security Solution for Financial Institutions

Access one of the industry's most comprehensive anti-fraud and risk analysis solutions fully integrated within the eBanking and Business Banking platforms. The Security solution not only helps financial institutions detect unusual activity or security breaches, but allows your institution to respond in real-time and even proactively prevent emerging fraud.

eValidation Engine

First Data has provided an ASP solution to financial institutions for more than 10 years, which has allowed us to gather and analyze an incredible amount of data history. Our eValidation Engine is based on mathematical formulas including rules-based expert systems and logic systems, which evaluate a user's typical Internet banking activity including time, location, frequency, browser footprint and session activity. These profiles serve as the basis for validating "unusual" transactions or behavior. The eValidation Engine's strength builds upon itself, becoming more refined and "smarter" with extended system usage.

Identity Verification

This feature allows an Individual User Profile to be evaluated when a user logs into the Internet banking system. When logging in, the user's profile will be compared to current activity. Activity that deviates from the individual's normal profile will be ranked based on the user's "difference in behavior" score.

- Difference in behavior scores defined as High Risk will be reported in real-time to your financial institution for further review and investigation.
- A daily report will be provided to your financial institution detailing behavior for all Internet banking logins the prior day.

Dual Authentication

First Data also provides financial institutions the option to implement additional authentication for any level login behavior before a user gains access to the eBanking and Business Banking solutions.

The following options are available within Dual Authentication to securely identify the user with strong two-factor authentication:

- Present the user's security question(s), which must be answered correctly in order to gain access to the system.
- E-mail a randomly generated one-time PIN (OTP)/ Security Code that must be entered in order to gain access to the system.
- Authentication levels can be implemented differently for retail users and commercial users.
- Authentication levels can be configured to be required at login or just within transactional Internet banking pages such as Bill Pay or Wire Transfers.

Alerts

eBanking allows for a user-based anti-fraud solution called Alerts. This feature provides an external e-mail notification to the user in the event that pre-set limits are exceeded. Users can set their own parameters for transactions that would be deemed "unusual." We also send external e-mails (out-of-band notification) to the user whenever their passcode, e-mail address, and/or their security question or answer is changed. These types of alerting systems are excellent communication tools and can assist in the early identification of fraud.

Intrusion Detection System

Our intrusion detection solution monitors the eBanking system for patterns of application events presumed to be malicious. This is a Signature-Based intrusion detection solution, meaning it identifies intrusions by watching for patterns of application events that appear to be abnormal. This alert method watches for a number of invalid Internet banking and Information Manager logins over a specific period, determines if the number of invalid logins goes beyond particular thresholds for the period and signals an alert throughout the overall monitoring system. An invalid login is a login that is attempted but did not succeed for any reason.

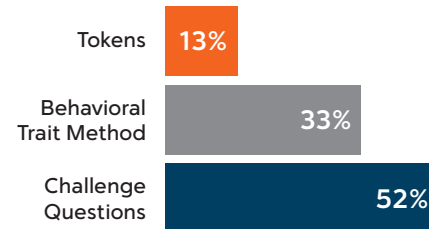
At this time, our technical staff members are alerted that a threshold has been reached and an automated analysis program is automatically initiated. The Intrusion Detection System consists of the following processes:

- Alert mechanism
- Automated analysis, action, recommendation and notification
- Further analysis and action
- Data warehousing and analysis

Large Transaction Report

The Large Transaction Report identifies large online transactions so financial institutions can easily identify and follow up with particular account holders to ensure these online activities were authorized by them and are not fraudulent. To create this daily report, the system reviews all online transactions for the business day and lists the specific details about the financial institution's larger transactions that were successfully processed.

Authentication Choices Preferred by Consumers



– from Javelin Strategy and Research

Benefits

- Meets multi-factor authentication recommendations from regulators
- Additional authentication protects your account holders without the added cost of hardware or tokens
- Allows your institution to easily conduct risk analysis of your Internet banking data
- Gives your account holders the control to set their own parameters for being alerted

A Global Leader in Electronic Commerce

First Data powers the global economy by making it easy, fast and secure for people and businesses around the world to buy goods and services using virtually any form of payment. Serving millions of merchant locations and thousands of card issuers, we have the expertise and insight to help you accelerate your business. Put our intelligence to work for you.

For more information, contact your First Data Sales Representative or visit firstdata.com.