

SmartGuard



Card Fraud Monitoring and Prevention

As cybercrime grows increasingly serious, payment systems are being attacked using skimming devices and malware designed to steal card data. For this reason, financial services organizations are becoming increasingly vigilant about protecting end users from identity theft and fraud. As part of SmartVista's end-to-end e-payments solution, SmartGuard helps issuers and acquirers monitor online payment transactions to prevent fraud before it occurs.

The solution provides a comprehensive toolset including user-defined rules technology and neural network-based monitoring for efficient and timely detection and online blocking of suspicious transactions. SmartGuard technology quickly adjusts to detect new types of fraud, dramatically reducing the risk of financial loss and increasing the efficiency of a bank's overall security and risk management system.



Key Features

SmartGuard provides a range of valuable features designed to help acquirers and issuers efficiently detect fraud before it occurs.

Online and Offline Data Monitoring

SmartGuard tracks both online and offline transactions for a holistic picture of data monitoring. The solution monitors transactions from both traditional and emerging delivery channels such as POS and ATM terminal devices, e-commerce, and m-commerce etc. by looking for atypical patterns such as a sudden, high volume of chargebacks or merchant retrieval requests that indicate suspicious activity. Configurable actions are then assigned to detect and prevent fraud before it occurs, such as:

- ↗ Placing suspicious transactions in the queue for further investigation
- ↗ Alerting operators and customers to questionable transactions
- ↗ Declining suspicious transactions
- ↗ Blocking the card

Risk weighting is assigned to each transaction, helping issuers make decisions about when and where to intervene to mirror internal risk management policies. When suspicious activity is detected, SmartGuard sends alerts to issuers, acquirers, or cardholders by email or SMS text.



- Tracks online and offline transactions for a holistic picture of data monitoring
-
- Tracks and filters 100 percent of all payment transactions
-
- Useful to both issuers and acquirers
-
- Monitors cardholder, merchant, and card activities
-
- Fully configurable rules-based system
-
- Neural network “learns” from transaction history and fraudulent spending patterns

Fully Configurable Rules

SmartGuard monitors transactions during authorization, based on a set of configurable rules. Banks can flexibly set and modify these detection rules based on the history of earlier detected fraud cases and other banks' experiences. List configuration is straightforward and does not require an IT specialist. Rules may be simple or complex—configured to monitor multiple combinations of parameters at the same time such as merchant location, transaction time, and the historic transaction profile of the card and whether a card was present at the time of transaction. Rules can also be configured for a group of cardholders, a group of merchants, a group of ATM or POS terminals, or specific accounts. SmartGuard can be fine-tuned down to the individual card level to prevent the maximum number of fraudulent transactions without declining genuine transactions.

100 Percent Tracking

Unlike some fraud management systems that base decisions on transaction sampling, SmartGuard monitors all process transactions with minimal degradation in service levels.

Smart Technology

SmartGuard is built upon neural network technology that "learns" from transaction history and previous, customer spending behavior. These spending patterns are based on statistical data of cardholders and cards, compiled to monitor suspicious activity and errant behaviors, reducing the risk of fraud.

With 5M cards issued per month, Alfa-Bank saves approximately 1M USD thanks to SmartGuard. This figure includes the account balances saved due to timely blocking of cards in cases of fraud detection, as well as the money saved from blocking cards due to analysis of third-party issuers and acquirers' messages.



Local Stop Lists

Local stop lists help make authorization decisions in stand-in mode.

Transaction Reporting

Statistical reports are provided to adjust and configure rules to maximize fraud monitoring efficiency. Reporting parameters may be changed or adjusted, depending upon the information required, such as how many suspicious requests were identified by each operator.



We will transform your payments business

Business Benefits

◇ Minimize reputational risk

SmartGuard allows users to quickly adjust to detect new types of fraud, reducing the risk of brand damage and increasing the efficiency of a bank's overall security and risk management system.

◇ Implement a proactive fraud prevention strategy

SmartGuard helps enforce proactive detection and prevention to reduce losses associated with fraud.

◇ Reduce operational costs

SmartGuard minimizes direct losses related to fraud and then decreases the operational costs related to dispute resolution and retrieval requests. SmartGuard reduces the incidence of fraudulent transactions, directly impacting the bottom line.

◇ Comply with international payment schemes' regulations

SmartGuard helps protect business from penalties imposed by the major card schemes such as Visa, MasterCard, American Express, and others due to excessive chargebacks and failure to comply with schemes' rules.

◇ Easy integration

Easy integration with additional SmartVista modules, such as SmartSwitch, reduces operational costs by providing a single interface to manage all SmartVista solutions. Adding a module is fast and easy and the end result is a fully integrated system that works in unison.

Technical Considerations

Platforms

SmartVista is an open platform solution that operates on industry-standard platforms such as IBM Power System (system P), HP Integrity System and NonStop, SUN SPARC, IBM Power System, and the x86_64 platform. SmartVista therefore runs on modern operating systems such as HP-UX, IBM AIX, SUN Solaris, IBM 1 (i5/OS) and NonStop Kernel (OSS). SmartVista also supports Linux (RedHat Linux, SuSe Linux, and OEL Linux).

Technologies

SmartVista uses industry-standard databases such as Oracle and DB2 together with Java-enabled Oracle Weblogic and IBM Websphere. You can count on 24x7 support from these vendors to maximize use of existing IT resources. SmartVista leverages the latest Oracle and IBM innovations to deliver high scalability, maintainability, and predictability during implementation and operational processes.

Third-party Applications and Libraries

SmartVista supports the most popular browsers—IE8, and Firefox 3 and to comply with various IT policies. Also, with a comprehensive set of Jasper Reports, SmartVista provides flexible and easy-to-use tools that allow you to modify and enhance the look and feel of reports without assistance from BPC.

For more information about SmartATM or other SmartVista solutions, please visit BPC Banking Technologies at www.bpcbt.com