ALFEBA
PROCESSING SOLUTIONS

SEQUOIA MOSAIC 3000: RISK

(FRAUD PREVENTION PLATFORM)

Functional description

User's manual

Version 2.0

This page doesn’t contain any information

Content

This page doesn’t contain any information

Chapter 1. About the document

This chapter contains the next sections:

This page doesn’t contain any information

1.1. Purpose of the document

This document describes the functionality of the SM 3000 RISK, SM 3000 fraud prevention platform, and it place in the SM3000 processing solutions. This document was prepared for users of the SM 3000 RISK.

1.2. How to use this manual

The manual is designed to show the main functions of the Platform and to give a short description of the SM3000 RISK for users.

The terms, abbreviations and useful references to other documents about the SM 3000 system are provided at the final part of the document.

Terms and Abbreviations - a glossary of terms commonly used in the card processing and electronic funds transfer industry.

To know how to use the ALFEBA documentation, to find information about the register structure and graphic tags, used in the documentation, see the Manual 200100 «Documents register».

1.3. Classification

This document has been classified as External.

1.4. Document sheet

300001

1.5. Document contacts

In the case of questions or proposals about information presented in this document, you can contact Alfeba's Documentation Division by email doc@alfeba.com, by phone +598 2 208 31 42 or by mail, using the address: Av. Agraciada 2770, Montevideo, 11823, Uruguay.

1.6. Document history

Version	Date	Modification	Notes	Authors
1.0	17.07.2000	-	Init. Version	Natalia Bogorodskaya
2.0.	24.09.2020	s/w version released	Version released	Natalia Bogorodskaya

This page doesn’t contain any information

Chapter 2. About SM3000 RISK

This chapter contains the next sections:

This page doesn’t contain any information

2.1. General information

In this chapter we provide the principal information about SM3000 RISK of the Sequoia Mosaic 3000.

2.2. About SM3000 RISK

SM 3000 RISK is a fraud prevention platform built on a modular principle, which allows you to choose all the necessary functionality and at the same time optimize the cost of its acquisition.

The number of e-commerce transactions has increased dramatically in the past few years, as has the amount of associated fraud. The annual volume of fraud worldwide on debit and credit cards alone, according to VISA and MasterCard estimates, exceeded US $ 19,21 billion in 2019. On the other hand, the U.S. Office of the Comptroller of Currency estimates that the annual volume of money laundering worldwide has exceeded $ 2 trillion.

At the same time, not only is the volume of fraud increasing, but its varieties are becoming more complex and sophisticated. This poses a significant threat to financial institutions, merchants and processors and requires the timely deployment of more effective fraud monitoring and detection tools that can adapt to the ever-changing spectrum of banking services, as well as new types of fraud.

To achieve this efficiency, fraud detection and prevention tools must be seamlessly integrated into the organization's business structure and customer accounting systems, significantly improve and maintain customer service, and reduce costs by reducing fraud losses.

SM 3000 RISK, using internal algorithm, based on artificial intelligent, correlates the parameters of each transaction with data from a risk model configured against a transaction information base and from templates describing acceptable activities and, on the other hand, fraudulent or suspicious activity for cards included in the corresponding portfolio. After this it evaluates the risk for each transaction in real time and assigns it a score (scoring) using various sophisticated algorithms, parameter values and previously collected statistics. In addition, the SM3000 RISK clearly indicates the basis for each assessment so that analysts can make more accurate analyzes.

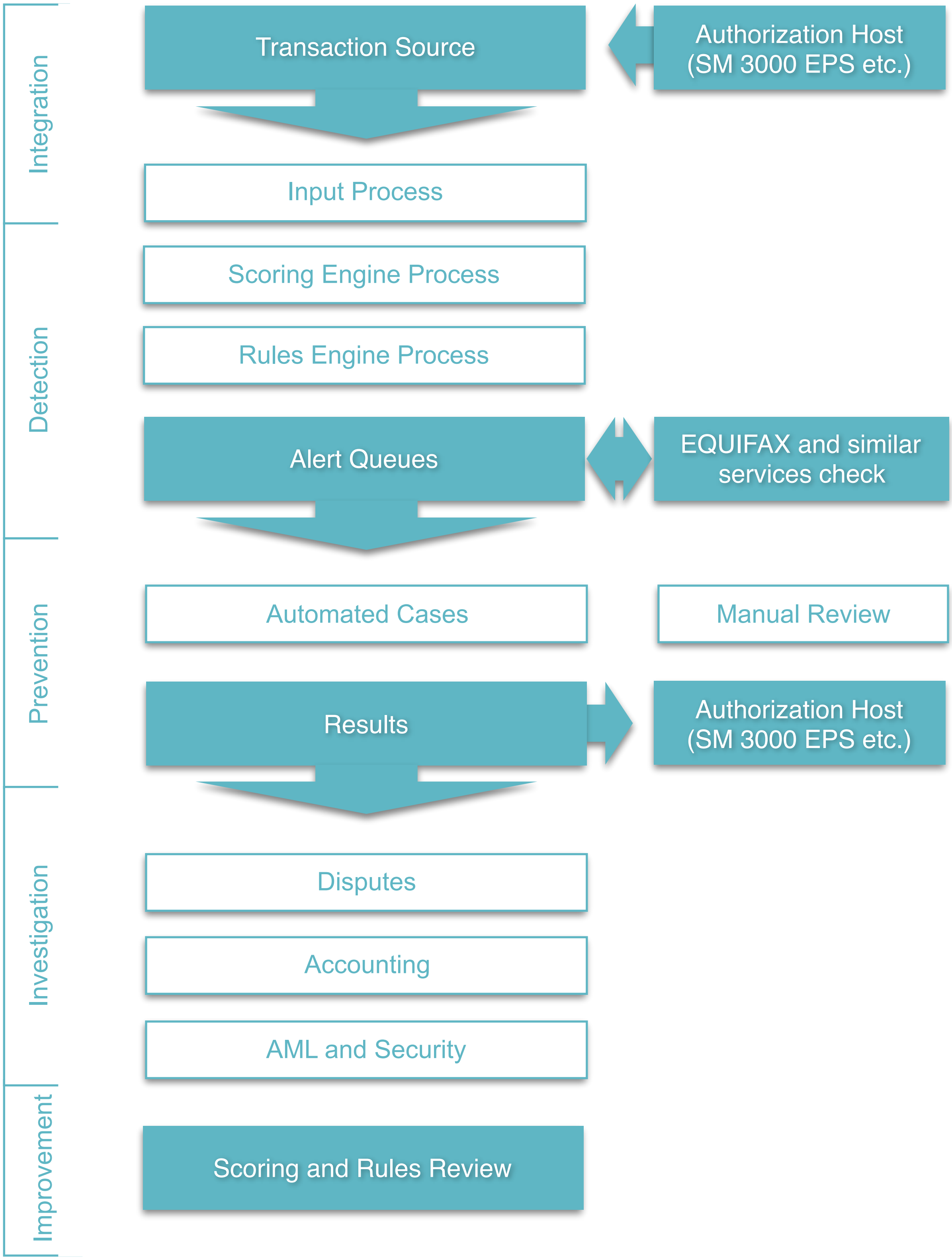
After evaluating the transaction, SM 3000 RISK passes it through a system of user-developed rules. The rules are created and enforced by employees of the relevant department through a simple user toolkit. This component leverages the expertise of the anti-fraud team by allowing new rules to be introduced in real time to counter new types of fraud and other violations as soon as they are identified.

A transaction whose scoring exceeds a user-specified threshold or triggers a rule triggers an Alert, which gets a certain priority and is queued for analysis by the corresponding analyst. A comprehensive toolbox allows department heads (supervisors) to manage analysts and alert queues to make the most efficient use of staff resources.

When suspicious or fraudulent activity is detected, the automated toolkit of the program allows you to ensure unconditional compliance with all the rules and regulations of the institution for investigations, refunds and the formation of appropriate reporting. The built-in core of automated workflow control ensures that all required activities are completed at a specified time. In addition, SM3000 RISK audits all activities, collects and stores statistics on losses from fraud - incurred and avoided - as well as on the effectiveness of the developed model and staff actions, providing the management of the institution with valuable information.

The SM3000 RISK workflow is demonstrated on the Picture 2.2.0.0.

Picture 2.2.0.0. SM3000 RISK workflow



As it shown in the Picture 2.2.0.0. the business processes are realized using the ISO 9000 standards and P-D-C-A algorithm and AML recommendations of the international financial regulators.

The SM3000 RISK is designed, using ISO 9000 standards and P-D-C-A ISO algorithm.

2.3. Fraud detection and prevention

Advances in technology have opened up new markets and expanded business opportunities. Ease of customer access to products and services has expanded the ability to attract customers in new directions. However, by creating new sources of income, this new environment has opened the door to new risks.

Criminals also took advantage of these opportunities and devised new, more sophisticated ways to commit fraud and money laundering, attacking the most vulnerable areas of information systems used in business. SM3000 RISK allows users to more accurately determine the degree of transaction vulnerability.

The system's ability to detect fraud with high accuracy enables analysts to quickly and efficiently respond to suspicious activity. SM3000 RISK quickly sends alerts: simultaneously with authorization processing, or in quasi-real time - a few seconds after attempting to commit a fraud. This allows analysts to take urgent measures to prevent or block high-risk transactions, which greatly reduces potential losses.

2.4. Card business cover

SM3000 RISK helps financial institutions to reduce fraud losses, enforce new anti-money laundering regulations, increase operational efficiency and reduce customer damage. The tool allows to implement the features that they need most and that provide the most value for the operations they do.

SM3000 RISK can be implemented individually or jointly with a SM3000 EPS, SM3000 IAP, SM3000 PAYMENTS or SM3000 CRYPTO. Modules for analyzing and supporting analysts' activities, ensuring the operation of rules allow generating notifications in real or quasi-real time via the user interface. Based on this, you can build a low-cost solution to reduce fraud and risk for the entire institution. A scoring system based on neural networks further increases the accuracy of fraud detection and reduces the number of false positives, which increases the efficiency of analysts. Investigation automation system reduces transaction costs. SM3000 RISK's online components further reduce the risk of loss by helping prevent fraud before it happens.

2.5. Rentability of usage

Financial institutions that use SM3000 RISK have seen significant reductions in fraud losses and fines for regulatory non-compliance. In many cases, SM3000 RISK users have recouped their software, hardware and additional staff costs in less than a year.

For example, a bank in the European region achieved an average of US $ 1 million in monthly fraud losses of the High-Risk e-commerce operations. Each card issuer saves over US $ 1,5 million in fraud losses every month. Card issuers usually reduce fraud losses in the first year of system operation by three to six basis points (losses in relation to total sales).

2.6. SM3000 RISK structural parts

The SM3000 RISK has three main internal structural parts:

1. Integration - network jobs core;
2. Detection;
3. Prevention.

To learn more about parts see sec. 3.3. The platform architecture.

2.7. SM3000 RISK integrations

Developed from the national processing center solution SM3000 RISK has traditionally a wide possibilities of the integration both with internal and external applications:

Internal ones:

- SM3000 EPS,
- SM3000 IAP,
- SM3000 PAYMENTS,
- SM3000 CRYPTO.

External ones:

- External authorization processing cores (SWITCHs): Way4, SmartVista, TransactPro, Compas+, Base24.
- Banking accounting systems (banking cores): BankXXI Century, TEMENOS.

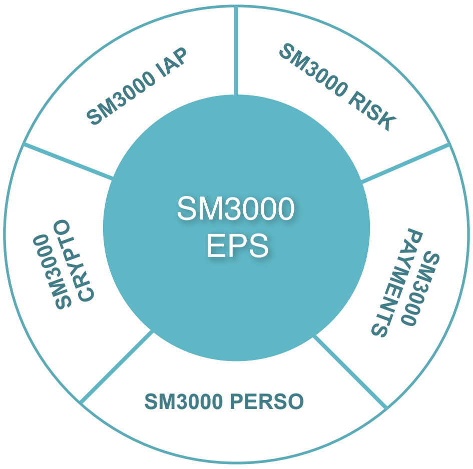
2.8. The place of SM3000 RISK in the SM3000 processing solutions

SM3000 RISK is a fraud prevention solution, which can be implemented with external authorization processing platforms and accounting systems.

The place of the SM3000 RISK you can find in the Picture 2.7.0.0.

Picture 2.7.0.0. SM3000 processing solutions structure

.



SM3000 EPS - is a on-line authorization processing core, developed for the Third party processors, national processing centers and banks - members of payment systems MasterCard, VISA and others. The Core processes cards issuing and acquiring banking programs, ATMs and POSs networks, has direct gateways to VISA, MasterCard and other processing systems. The full functional description of the SM3000 EPS see in the Manual SM3000 EPS. Functional description. The Core has integrations with core banking systems, TEMENOS, BANKXXI, DIASOFT and others banking accounting solutions.

SM3000 PERSO - is a personalization platform for the DataCard and NBS personalization stations. It supports NFC-based, contact chip and magstripe products personalization jobs. The full functional description of the SM3000 PERSO see in the Manual SM3000 EPS. Functional description.

SM3000 PAYMENTS - is a platform for consumer credits, on-line payments for credit, MO/TO transactions by credit, membership programs, bonus and discounts management for cardholders and merchants. The full functional description of the SM3000 PAYMENTS see in the Manual SM3000 PAYMENTS. Functional description.

SM3000 IAP - is a e-commerce solution that enables you to manage the payment transactions of your business. The platform supports multiple payment methods and integration methods.

SM3000 CRYPTO - is a full platform for the crypto currencies issuing and acquiring, including Merchant profile and mobile applications for users, crypto change offices and crypto stock exchange software, on the government and private level of the implementation. The full functional description of the SM3000 CRYPTO see in the Manual SM3000 CRYPTO. Functional description.

Between the mentioned platforms of the SM3000 processing solutions are local products, like a software for POS terminals (NEW POS and others), self-service terminals etc. Functional description of these products can be provided on demand.

Chapter 3. System information

This chapter contains the next sections:

This page doesn’t contain any information

3.1. General information

In this chapter we describe a system information of the Sequoia Mosaic 3000 RISK.

3.2. The system information

SM3000 RISK was created in a distributed processing environment and includes components for both fraud prevention and detection. Configuration options are available to monitor transactions in real-time to prevent fraud, or in near-real time, detecting fraud immediately after the first fraudulent transaction. Online monitoring of high-risk transactions enhances SM3000 RISK's fraud prevention capabilities. Transactions identified as particularly high-risk transactions can be isolated from the authorization flow and passed through online scoring (scoring) and online rule engines to prevent potential fraud before it occurs. The use of online scoring and online rule mechanisms significantly reduces the potential for fraud losses.

The interface with authorization systems is customizable. Transaction data and card database data are entered into the system to monitor suspicious activity as efficiently as possible. SM3000 RISK monitors actions through sophisticated analytical processing performed by a neural network-based scoring engine, combined with the operation of a system of expert rules.

Analytics for suspicious activity alerts are maximized with a powerful analysis and investigation support system that includes a fraud history database and workflow management system. The management components ensure efficient distribution of responsibilities among staff.

SM3000 RISK ensures that fraud investigations are conducted from their identification within the analysis and investigation support system to the completion and closure of the case, based on the workflow described for this purpose in the institution.

The monitoring capabilities of SM3000 RISK are enhanced by the addition of a scoring mechanism that is customized to the needs of the institution. Each transaction is passed through the SM3000 RISK scoring mechanism in the format of a message generated directly from the authorization system, or in a file format as part of periodically generated packages. The scoring mechanism analyzes the received transactions in relation to the current average values of the parameters on the corresponding card, in relation to the data of previous transactions for the holder, account or company, as well as in relation to the known patterns of fraudulent actions from the historical database of the model. Real-time monitoring of the highest-risk transactions uses the same network-based scoring logic, but selects the highest-risk transactions directly from the authorization process. Depending on the real-time evaluation, the transaction processing either continues or generates a refusal or a request to contact the issuer (Referral), which changes the course of the authorization process.

At the output of the scoring process based on neural network technology, a scoring estimate of the probability of fraud is formed - a value in the range from 0 to 999. The higher the score, the more likely the fact of fraud is. The transaction data and the score are then transmitted to the analysis and investigation server, where the score is compared with the set and threshold values of the corresponding parameters, and also checked in the expert rule system. If the score for authorization exceeds the threshold or triggers the rule, an alert is generated for the transaction (Alert). The alert is sent to the appropriate analyst through the queue mechanism, which is managed by the head of the department (supervisor).

Because SM3000 RISK has a modular architecture, there are many configuration options to choose from, from using online scoring and online rules to network scoring with customized model or offline rule-based analysis system.

3.3. Authorization interface

SM3000 RISK includes main components, presented in the Table 3.3.0.0.

Table 3.3.0.0. The SM3000 RISK main components

Name	Type
Scoring mechanism	On-line
System of rules	On-line

Existing authorization systems can be improved in order to transfer transaction and bank data (databases of holders, accounts or firms) to the SM3000 RISK platform.

SM3000 EPS system users are offered a standard software interface to the scoring engine.

In the authorization environment of the SM3000 EPS, an additional data file is used - the Scoring Engine File (SEF). This file contains cardholder and card data, including the cardholder's first and last name, his / her date of birth, ID number and other personal and financial information that is required by the SM3000 RISK scoring engine for risk assessment or the analysis and investigation support system for the purpose of creating strategies and displaying information on the screen. The SM3000 EPS data refresh process supports full and partial data refresh in the SEF file.

SM3000 EPS authorization modules have been enhanced to deliver an instance of each transaction to the SM3000 EPS system and to the SM3000 RISK. The operating interface then transfers the transaction and card data to the SM3000 RISK scoring engine.

The combined SM3000 EPS and SM3000 RISK configuration runs on the SM3000 EPS Network interface in quasi-real and real-time scoring modes. Working in real-time scoring mode, the authorization process additionally selects the most high-risk transactions and transfers them to the scoring mechanism for conducting fraud checks before authorization is completed. Synchronous scoring is typically used for transactions that are considered particularly high-risk.

The SM3000 EPS Network interface transmits a message from the authorization process to the scoring mechanism and back within a time not exceeding the time it takes to form a response to a request in financial transactions. The transaction is evaluated in a user-customized neural model that provides the authorization process with the necessary data to generate a response in terms of "accept", "reject", or "forward to the issuer". The authorization host system makes the final authorization decision based on this assessment.

In quasi-real-time mode, transactions are evaluated immediately after authorization. SM3000 EPS Network interface manages the flow of messages between the respective processes. SM3000 EPS Network interface and TCP / IP then can forward the scored transactions to the external systems for Analysis and Investigation within seconds of authorization, reducing the chance for a criminal to conduct multiple fraudulent transactions before being detected.

3.4. Scoring mechanism

The SM3000 RISK scoring engine can run on IBM, Sun Solaris, or with the AWS AMAZON Cloud platform. The scoring engine can be configured to operate in quasi-real-time, real-time, or batch mode, depending on the institution's risk management strategy and system procedures. The required hardware is provided and installed by the institution itself.

The main task of the SM3000 RISK scoring mechanism is to ensure accurate detection of suspicious actions of holders, cards or companies and generate an alert. For each transaction, SM3000 RISK calculates a score that is a measure of the likelihood that the transaction is fraudulent.

SM3000 RISK calculates scores in two steps:

- Stage of analysis of an individual behavior profile (Individual Behavior Profile) - SM3000 RISK highlights all changes in the actions of the holder, card or company by comparing their actions with the basic pattern of behavior of the holder, card or company. By examining all parameters of the account (transaction data, previous actions, changes in the way of use, change of address, etc.), SM3000 RISK is able to detect changes in a specific transaction of the holder, card or company.
- Network Phase - The tool's neural network compares the changes detected in the operation with information stored in the knowledge base of the system, called the "memory model", which stores the facts of fraudulent and normal behavior. The output of this processing is a score for the likelihood of fraud in the range from 0 to 999; the higher the score, the more likely the transaction is fraudulent. Unlike many other neural networks, SM3000 RISK explains the reasons for deriving a score by providing an appropriate list.

The assigned score is compared with user-defined thresholds. If the score exceeds one of the thresholds set in the analysis and investigation support system, an alert is generated for the transaction. Each alert is then sent to the appropriate analyst through a user-generated queue mechanism.

An accurate definition of fraud involves the ability to distinguish fraudulent behavior from normal behavior. SM3000 RISK uses a user-customizable model built from analysis of patterns of normal and fraudulent transactional behavior that have historically formed in an institution's portfolio. This allows the scoring engine to more accurately assess potential fraud, reducing the cost and time spent on processing false positives. This final model brings together the institution's databases of cards, accounts and firms, the regions in which they operate, and the actions of their clients, taking into account seasonal changes. With a customized model, institutions increase detection accuracy, reduce false positives, provide earlier detection of suspicious activity, and reduce fraud losses.

3.5. System of rules

SM3000 RISK system of rules contains rules and policies and also provides workflow management functions.

The rules are filter-type operators designed to highlight specially described situations that may indicate criminal actions. These operators are usually easy to understand - for example, transactions with high dollar amounts, transactions from specific points of origin, or with an amount exceeding a certain threshold. They can be more complex if they include multiple parameters and contain the necessary Boolean logic.

SM3000 RISK's user-generated queuing functionality is one of the key product features as it routes alerts to specific analysts based on user-defined rules and sorting criteria. SM3000 RISK's dynamic queue management mechanism allows risk administrators to assign priority levels, delegate certain types of transactions to analysts specializing in specific areas of investigation, and allocate resources based on availability of appropriate personnel and seasonal factors. This allows the workload of the investigative analyst team to be managed in a way that maximizes productivity and investigates alerts on a top-priority basis.

SM3000 RISK stores and maintains statistics on fraud losses, fraud loss reduction, analyst performance and the model. A wide range of the accumulated information can allow department heads (supervisors) to generate reports, manage workflow, assign queues and assign analysts. SM 3000 RISK can automate reporting at the level of a device, institution, network, settlements of one or several networks. To do it we prepare SM 3000 RISK to integrate with a Django or other similar products.

For further information on the Django SQL explorer see https://github.com/groveco/django-sql-explorer

It allows quickly write and share SQL queries in a simple, usable SQL editor, preview the results in the browser, share links, download CSV files, and keep the information flowing. It supports multiple connections, to many different SQL database types, a schema explorer, query history (e.g. lightweight version control), a basic security model, in-browser pivot tables, and more.

SM 3000 RISK tools enable institutions to understand how fraud is committed and how effectively the institution is fighting it. SM 3000 RISK contains utilities through which analysts can monitor how effective the model is in detecting fraud and how well analysts are in investigating detected fraud. Using the same toolkit, the management of the institution can perform the following actions:

- view account holders,
- add, modify and remove users,
- add, modify and delete data in the points of compromise table,
- analyze model performance,
- analyze the performance of analysts,
- form and distribute queues,
- define strategies for action,
- monitor work processes,
- generate reports on fraud reduction and operational performance.

3.6. SM3000 RISK advantages

The fraud models used in SM3000 RISK are refined based on information from the institution's own accounts, rather than from industry averages. This adaptive simulation technology improves the system's ability to detect fraud, providing maximum protection to the related funds. Fraud and suspicious behavior patterns can be tweaked or re-tuned to adapt to new or existing patterns of fraud, and institutions are free to tweak their patterns as often as they want. SM3000 RISK provides accurate fraud detection and protection for respectable customers.

3.7. Openness, flexibility, integrability

The SM3000 RISK and its components are natural extensions to existing SM3000 transaction processing applications. Users can expand the capabilities of SM3000 RISK by adding other applications and thus increasing its power.

3.8. Responding to your risk management needs

The SM3000 RISK is a multi-faceted application that can help institutions meet critical risk management and fraud containment needs. Moreover, the neural network technology used in the system helps institutions to detect and prevent existing and emerging types of fraud. SM3000 RISK responds to all of an institution's risk management needs - from collecting data from the production system to providing a user-friendly and intuitive interface for viewing information.

This page doesn’t contain any information

Chapter 4. SM 3000 RISK overview

This chapter contains the next sections:

This page doesn’t contain any information

4.1. General information

Banks and financial institutions need a risk management tool that can recognize existing fraud patterns across holders, accounts and merchant firms, and respond quickly to new fraud patterns. SM3000 RISK offers solutions for detecting fraud in credit cards, debit cards, business acquiring and at the enterprise level, and is also capable of detecting possible money laundering activities.

4.1.1. SM3000 RISK for Debit and Credit Card Fraud Detection

SM3000 RISK for Debit and Credit Card Fraud Detection monitors every financial transaction against known fraudulent activity and past customer behavior. Designed to protect the issuer, this solution reduces lost, stolen, skimmed, tampered and unreceived card losses by proactively monitoring online and offline transactions, card-less transactions, and mail / phone order transactions. This solution has a significant quality advantage over systems based on rule-based activity analysis, statistical score cards, and non-optimized neural networks.

4.1.2. SM3000 RISK for Merchant Fraud Detection

SM3000 RISK for POS and e-commerce monitors the received financial transactions and authorization activities of merchants operating under acquirers by comparing the history of the firm's actions and confirmed patterns of fraudulent actions with the current data on the merchant's activities. The system also makes it possible to recognize suspicious transactions of holders, thus protecting both acquirers and their outlets from many situations associated with fraud of holders in firms. The tool identifies high-risk retail outlets, collusive merchants, points of compromise, bogus bankruptcy schemes, and other known POS or e-commerce merchant fraud patterns through proactively monitoring business operations and credit card transactions. SM3000 has it own risk management system for the SM3000 IAP.

To learn more about e-commerce risk management see Manual 200101 «SM3000: IAP. Functional description».

4.1.3. ACI PRM for anti-money laundering

SM3000 RISK can be used for the Anti-Money Laundering protection. It is capable of recognizing and monitoring complex and varied methods of money laundering by various organizations. Money laundering scammers hide the origin of their funds by moving them through as many bank accounts and countries as possible, trying to pass them off as legal income. SM3000 RISK monitors all aspects of account activity, detecting complex behavioral patterns consistent with confirmed money laundering.

4.2. Functional features

Among the functional features are:

- Timeliness,
- A wealth of functionality,
- Adaptability,
- Ease of use,
- Interoperability and modularity,
- Open database architecture,
- Custom functions.

4.2.1. Timeliness

SM3000 RISK quickly generates suspicious activity alerts using its powerful and accurate network models to reduce fraud and limit its impact on respectable account holders. This, along with the ability to easily shape user-specific rules and enforce them in real time, allows institutions to quickly respond to new types of fraud. Customizable scoring and the ability to quickly introduce new rules are powerful differentiators for SM3000 RISK. Using these tools helps agencies to quickly identify and instantly stop known types of fraud.

4.2.2. A wealth of functionality

The presence of functions based on both neural technologies and rules is a distinctive feature of SM3000 RISK. Although the model acts as the mathematical intelligence of the tool, rules provide an invaluable tool for organizing a quick response to changes in the world of fraud and money laundering.

The combination of both of these features in real time provides a rare opportunity to prevent fraud before it happens. Scoring and applying rules in real time allows you to catch the highest-risk transactions and make decisions about the likelihood of fraud before authorization is granted.

4.2.3. Adaptability

SM3000 RISK is tuned to new cases of fraud with its flexible rules toolkit and model refinement capabilities. New rules can be easily formed to target new types of fraud that are still pending or are already present in the transaction base.

All models degrade over time. The model refinement procedure available in internal dispatcher gives institutions a tool to maintain the effectiveness of their neural model at the proper level. Supplementing the neural model with fresh transactional data on proven fraud cases can significantly extend its life. Both functions provide users with powerful tools to quickly respond to changes in the patterns of fraud in the databases of cards, companies and accounts.

The rules component is designed to be embedded in an institution's procedures, policies, and workflows. Adjusting the process diagram to the established operating procedures of the institution provides a significant increase in its operational efficiency.

4.2.4. Ease of use

SM3000 RISK has a user-friendly user interface developed in Java, with the help of which the task flow is managed, which increases the efficiency of analysts' work and greatly reduces the training time for new employees. It allows you to evaluate an account profile from different perspectives by combining current and past transaction data. The analytics workstation is designed to provide the most intuitive way to view account and transaction data. The system also maintains statistics on the status of the task queue, analyst performance, and model, providing management with valuable additional information.

A client application running through a Web server provides users outside of the system's own desktop with secure access to the application base and workflow management system. Connection to SM3000 RISK applications is carried out via the corporate Intranet or via the Internet.

4.2.5. Interoperability and modularity

SM3000 RISK interacts with the institution's existing authorization system, or with an external processing system. Its open architecture allows it to run on multiple platforms, including HP, IBM, Microsoft Windows, Sun Solaris or AWS AMAZON cloud solutions. The modular organization of SM3000 RISK allows institutions to implement the solution that best suits their needs, while maintaining low operating costs and maximizing the use of available functionality.

4.2.6. Open database architecture

SM3000 RISK is based on an open database architecture that the user can extend as needed. The product can integrate with external applications, which allows synchronizing their work with SM3000 RISK actions.

4.2.7. Custom functions

Once SM3000 RISK is installed and configured, facility staff can easily view alerts, track transaction activity, monitor work, and collect performance statistics.

To view alerts, analysts simply log into SM3000 RISK through the user interface, analyze the first alert in the highest priority task queue, view the displayed account and transaction information, and take the necessary action. Analysts can indicate that the account status is normal, set the account for monitoring (watch status), send an alert to another analyst, call the client, block the account, mark the transaction as fraudulent in the protocol, and write a comment on the account.

The alert analysis screen displays general account information that can be used to identify suspicious card use. The card information tab and the financial information tab contain additional account data.

4.3. Monitoring and detecting points of compromise

Copying (Skimming) data from a magnetic stripe card has become the fastest growing type of fraud affecting issuers of debit and credit cards. SM3000 RISK provides a set of features that enable financial institutions to effectively combat this type of fraud, reducing losses and other related costs. The great advantage of SM3000 RISK in this regard is its ability to highlight one or more facilities during the analysis of a series of transactions and then analyze other suspicious transactions that occurred at the same facility on the same day. As soon as it was possible to determine that a suspicious facility is indeed a point of compromise, the system allows the analyst to select "respectable" cards, which were also used for transactions at this facility during a given period of that day. The analyst can then either set a lock for the entire package of these potentially compromised cards, or place these cards in a table where special monitoring will be performed on them. The bank or financial institution can also enter into this table any other list of potentially compromised cards obtained from other sources (for example, from a payment system). This allows a financial institution to avoid such an expensive measure as re-issuing cards, only on the basis of the fact that they at some point came under suspicion of compromise.

4.4. Custom Environment (Add-In Framework)

SM3000 RISK uses an open, customizable programming environment that allows users to extend and override control button actions. This architecture allows you to export any information found in the SM3000 RISK database to another system on the host, or import the necessary information - for example, copies of receipts. With a single click of the mouse, analysts can assign a series of blocking codes so as to deny any future authorization requests (by pressing the block button) or forward all authorization requests in the future to the issuer's call center (by pressing the monitoring button). Analysts can also assign the formation of specialized reports or letters upon pressing the standard letter button.

The open, customizable software environment architecture in SM3000 RISK enables banks, financial institutions or third-party vendors to customize software, extending SM3000 RISK functionality to an incredible range.

An optional feedback mechanism in SM3000 RISK allows changes made on the alert screen to be communicated to the host computer. If feedback has been configured on the system, the feedback program will run in the server machine environment and transfer changes to the host. The feedback also maintains asynchronous communication with the host on all actions that the analyst performs on the account. If an interface with feedback is defined, then its use provides a significant flexibility in the response on each site in relation to the actual actions performed.

Chapter 5. Attachments

This chapter contains the next sections:

This page doesn’t contain any information

6.1. Terms and abbreviations

3

3D-Secure Is an XML-based protocol designed to be an additional security layer for online credit and debit card transactions.

A

API Application programming interface

Authorization Is an approval from a card issuer, usually through a credit card processor, that the customer has sufficient funds to cover the cost of the transaction.

B

BO Back-office, of the SM3000 IAP, where the Operator’s employers work to maintain the Platform jobs, as Merchants, Transactions, Agents, Reports and file exchange with a main Processing system.

C

Cardholder A person who owns a card, such as a cardholder of a credit card or debit card

ChargeBack Is a return of money to a payer. Most commonly the payer is a consumer. The chargeback reverses a money transfer from the consumer's credit card. The chargeback is ordered by the bank that issued the consumer's payment card.

F

FE Front-end, of the SM3000 IAP, where the cards authorizations are processed in on-line mode

I

IAP Internet acquiring platform. The Platform created as a separate application for the Payment operators and Payment facilitators.

ID Identification number (f.e. transaction ID or Merchant ID)

Incoming-File The data file, that Platform receives from the Bank’s processor

L

Light API The interface to connect the Merchant’s own platform to the SM3000 IAP

M

MasterCard MasterCard International payment system

Merchant A legal entity carrying out trading activities on the Internet using the software provided by the system

MPI Merchant Plug-in

O

Operator Payment operator or Payment facilitator, that uses SM3000 IAP

Outgoing-File The data file, that the Platform sends to the Bank's processor

P

PAN Primary account number, or simply a card number, is the card identifier found on payment cards, such as credit cards and debit cards, as well as stored-value cards, gift cards and other similar cards.

Payment Gateway A hardware-software complex developed and supported by a payment system that automates the acceptance of payments on the Internet.

Payment System Payment system between users, financial organizations and business organizations. Allows you to pay, bills and purchases, transfer money.

R

Refund A process in which a customer returns a product to the original retailer in exchange for money previously paid

Reversal The operation of crediting funds to the payer's account as compensation for the cancellation of the provision of the service or the poorly rendered service.

S

Service Merchant's service entry, registered for each MCC. It has its own parameters, fees etc.

SM3000 Sequoia Mosaic 3000. The processing platform of the cards issuing and acquiring processing, ATMs, POSs, e-commerce and m-commerce processing

System A payment system that allows you to transfer money, accept payment for goods and services through various payment gateways.

T

Transaction Within the framework of this service, a completely completed data exchange operation with a payment system, including debiting / crediting funds to an end user account.

V

VISA VISA International payment system

6.2. External documents references

The manual uses the links to the other documentation of the SM3000 IAP, listed below:

Document code	Document name	Document Purpose	Document category
200101	SM3000: IAP. Functional description	Describes main functions of the SM 3000 IAP	User’s manual

ALFEBA

Agraciada 2770 Montevideo 11823 Uruguay

Phone: + 598 2 2083142

E-mail: docs@alfeba.com

www.alfeba.com