

Risk Monitoring

Contents

RISK MONITORING: AN INTRODUCTION	2
CHAPTER 1. RISK MONITORING: GENERAL PRINCIPLES	3
CHAPTER 2. CONFIGURING CARD RISK MONITORING RULES	5
Configuring Rules for All Cards	5
Use of Risk Management Schemes while Configuring Rules	7
CHAPTER 3. ANALYZING SUSPECT OPERATIONS	8
List of Suspicious Transactions	9
List of Transactions Grouped by Rules	11
List of Transactions Grouped by Cards	12
Creating the List of Suspicious Transactions	12

Introduction


The WAY4 system provides system users with periodic on-line risk monitoring according to specified parameters. The monitoring module (CSA – Card Suspect Activity Monitoring) computes the degree of risk presented by suspect operations and, on the basis of such computations, transactions perceived as suspect may be declined automatically.

This document is intended for security officers involved with risk monitoring of card operations.

When working with this document, it is recommended that users refer to the following resources in OpenWay's documentation series:

- Risk Management
- Documents
- WAY4™ Products. Service Packages
- WAY4™ Dictionaries

The following conventions are used in the document:

- *Italic* indicates a form field;
- [Square brackets] indicate form buttons, e.g. [Approve];
- → indicates the next item to be selected in the sequence of User Menu items, e.g. "Full → Issuing → Contracts Input & Update";
- <Angle brackets> indicate shortcut keys available in DB Manager, e.g. <Ctrl>+<F3>;
-  indicates a warning against a possible wrong action;
- The symbol ✓ is placed next to information that points to options for optimizing system functions and other important possibilities.

Chapter 1. Risk Monitoring: General Principles

Every operation must be verified according to risk criteria defined by a set of rules. Rules include those set for all bankcards as well as those set by parameters in the Risk Scheme and relating to a certain card contract or to the Service Package of that contract.

The rules determining which operations are considered suspicious can be configured through special forms provided by the system (see "Configuring Card Risk Monitoring Rules").

Risk Scheme parameters may define the general parameters given for all bankcards, if the parameter name in the general parameters is identical to the one set in an individual Risk Scheme.

Rules may place a threshold on the amount requested during an operation or on the number of operations. When this limit is exceeded, the system will consider the operation to be suspicious.

All the criteria of the monitoring module are configured by combining the programmed rules of operations and variable parameters.

The programmed rules of operations include the identification, by the system, of such transgressions as the following:

- Changes in the country of use for operations on one bankcard within a certain time interval;
- Repeated operations on one bankcard on one device belonging to the same merchant within a certain time interval;
- Operations which decrease the card account's amount available by a certain percentage of the original amount;
- Repeated and successive attempts to execute an operation with a single bankcard with corresponding decreases in the amount requested within a set time interval.
- Repeated unsuccessful attempts at entering PIN.

The variable parameters are as follows:

- The amount of an operation or the percentage of the account balance;
- The observed period;
- The number of authorized operations;
- The characteristics of the location of an operation, such as the country the merchant category, the merchant;
- The responses to certain transgressions, such as blocking a card or notifying the card owner of a performed operation.

As a result of verification (see "Analyzing Suspect Operations"), suspicious operations are registered in a special form and may be declined with a negative response code.

The record registering the suspicious activity will have status "Active". When the circumstances surrounding the suspicious activity are clarified, the user may choose to change the status to "Inactive" or "Closed".

Chapter 2. Configuring Card Risk Monitoring Rules

Configuring Rules for All Cards

Risk monitoring rules are configured in the form found at "Full → Stop List → Merchant Stop List" (see Fig. 1).

Card Risk Monitoring Rules											<< < > >>			9 of 11	
Group Code	Area	Merchant Bant	SIC	Ans Condit	Spc Condition	Resp Code	Actio	Date From	Date To	u (Ho	mit Cui	mit Amnt	%	Lim	
Risky Country					Check Usage	Successfully complete	Yes	26/10/2004	00/00/0000	24				0.00/15	
Amount Fitting					Amount Fitting	Successfully complete	Yes	26/10/2004	00/00/0000	24				0.00/15	
The Same Merchant					The Same Mercha	Successfully complete	Yes	26/10/2004	00/00/0000	24				0.00/15	
Risky SIC Group				POS Key Ent		Refer to card issuer	Yes	26/10/2004	00/00/0000	24				0.00/15	
Risky SIC			7995 Casino			Successfully complete	Yes	26/10/2004	00/00/0000	24				0.00/15	
Single Amount						Do not Honour	Yes	26/10/2004	00/00/0000	0	USD			800.00/15	
Change Country					Change Country	Successfully complete	Yes	26/10/2004	00/00/0000	24				0.00/15	
Amount Fitting		ANY_BIN			Amount Fitting	Successfully complete	Yes	05/04/2005	00/00/0000	0				0.00/0	
Utilization					Utilization	Successfully complete	Yes	26/10/2004	00/00/0000	24				80.00/0	
Total Amount						Successfully complete	Yes	26/10/2004	00/00/0000	2	USD			1,000.00/0	
Utilization 6h					Utilization	Successfully complete	Yes	10/06/2004	00/00/0000	6				90.00/0	

Fig. 1. The grid for configuring card risk monitoring rules

To enter parameters, use the form "Full Info for <name of rule>" (see Fig. 2), opened by clicking on the [Full Info] button in the "Merchant Stop List" form.

Full Info for [Empty]		
Parameter Group Code: <input type="text"/> Comment: <input type="text"/> Risk Scheme Rules Switch Tag: <input type="text"/> Activated For Scheme (Single): <input type="text"/> Scheme (Group): <input type="text"/>	Criteria Merchant BIN: <input type="text"/> Trans Cond: <input type="text"/> SIC: <input type="text"/> Area: <input type="text"/> Merchant Name: <input type="text"/> Special Parm: <input type="text"/>	Limits Limit Interval: <input type="text"/> 0 (Hours) Limit Curr: <input type="text"/> Limit Amount: <input type="text"/> 0.00 Limit Number: <input type="text"/> 0
Actions Resp Code: <input type="text"/> Successfully completed Event Type: <input type="text"/> Suspect Factor: <input type="text"/> 1,000 Activity Period: <input type="text"/> 12/12/2005 <input type="text"/> 00/00/0000 Activity Tag: <input type="text"/>		

Fig. 2. The form for viewing and entering full rule criteria information for monitoring a suspicious activity

This form for viewing and entering rule criteria contains the following fields grouped in several blocks:

- **Group Code** – the unique rule code to be indicated in the WAY4 Process Log when a transaction is registered in the suspicious activities list;
- **Comment** – additional information about a criterion; if TRCITY= <city name> tag is entered into this field, the criterion will work only for documents where the TRANS_CITY field is filled in with this value. In other words, this criterion will be checked only for transactions that take place in the indicated city;

The fields of the "Risk Scheme Rules" group are used for configuring criteria common for a group of cards or that for a single card. If a criterion is supposed to work for all cards, these fields must be left blank. The use of the fields of the "Risk Scheme Rules" group is described in "Use of Risk Management Schemes while Configuring Rules".

The "Criteria" group includes fields intended for fine-configuring risk monitoring parameters:

- *Trans Condition* – the criteria of completing an operation (see the "Transaction Conditions" paragraph of the "Documents" document).
- *SIC* – the cod defining sales outlet type (SIC/MCC) as regards the nature of business (see the "'SIC Group' Dictionary" section in the WAY4™ Dictionaries Administrator manual).
- *Area* – the name of the area where the transaction was executed (see chapter "Country Area Support" in the WAY4™ Dictionaries Administrator manual).
- *Merchant BIN* – the merchant BIN assigned by the payment system whose device was used to execute the transaction. The field can contain either the direct BIN value or one of the following values:
 - ON_US – the transaction will be checked against this rule only if it is executed on a merchant device registered in the system;
 - FOREIGN – operation will be checked against this rule only if it is executed on a merchant device NOT registered in the system;
 - ANY_BIN – operation will be checked against this rule whether the merchant is registered in the system or not.
- *Merchant Name* – the name of the merchant whose device was used to execute the transaction;
- *Special Parms* – field to indicate conditions checked through programmed rules; the system can use the following programmed rules:
 - CHANGE_COUNTRY (Change Country) – change of country when executing a transaction on a single bank card within a specified time interval;
 - THE_SAME_MERCHANT (The Same Merchant) – repeated transactions on a single bank card on a device belonging to one merchant within a specified time interval;
 - AMMOUNT_FITTING (Amount Fitting) – repeated attempts to execute a transaction on a single bank card with successive decreases in the amount requested within a specified time interval;
 - UTILIZATION (Utilization) – transactions that result in the amount available decreasing by a certain percentage of the current amount available.
 - INVALID_PIN (Invalid PIN) – multiple attempts at entering PIN.
 - The rule "Check Usage" is used as follows: if the transaction fulfills the rule parameters at authorization, the system checks whether usage limiter with "Risk Rule Redefine" has been assigned for that contract. If this limiter is present, then the system activates a counter according to its parameters (on working with and configuring limiters see the "Usage Limiters" section of the "WAY4™ Products. Service Packages" document). When the counter limit is reached, the limiter will be activated and the transaction will be registered as suspicious.

The "Limits" group includes fields intended for setting the following threshold values:

Limit Interval (Hours) – a time interval in hours, during which operations involving a card are analyzed according to the rule; the system analyzes operations involving a certain card over the indicated number of hours;

- *Limit Curr* – the currency used for setting the threshold value of the total amount of operations;
- *Limit Amount* – a numeric value used for setting the threshold value of the total transactions. This field may be filled in with the following values:
 - The total transactions amount for a certain defined period of time (with the exception of cases when the *Special Parms* field is assigned UTILIZATION value);
 - A percentage of the available amount on a card – when the *Special Parms* field is assigned UTILIZATION value;
- *Limit Number* – the threshold number of operations. When this number is reached, each next transaction is considered suspect.

The "Actions" group includes the following fields:

- *Resp Code* – a system response code given after analyzing a transaction; putting a negative response code in this field allows suspicious transactions to be declined automatically.
- *Event Type* – the name of a system event, which must be opened for a card when it is involved in a transaction considered suspect;
- *Suspect Factor* – a factor by which the significance of a risk criterion may be increased;
- *Activity Tag* – the field may take one of the following values: "Yes" – the rule is used for analyzing operations; "No" the rule is not used;
- The *Activity Period* fields are used for defining a period of time when a certain rule is either active or not.

The value of the CH_ST_LST tag affects calculation of the total amount of authorisations for the period set in risk monitoring parameters. This tag is specified in the *Additional Criteria* field of the "Full Info For..." form opened by clicking the [Full Info] button in the "Merchant Stop List" form (Full → Stop List → Merchant Stop List). The parameter value is a comma-separated list of codes corresponding to CREDIT_HISTORY.credit_status table record statuses that will be analysed in this rule.

Use of Risk Management Schemes while Configuring Rules

The system allows the use of Risk Management Schemes for assigning a single rule to a group of contracts or to a single card.

The following configuration must be set up to create additional risk rules for a group of cards or for an individual card:

- Register a Risk Scheme, Configuring Risk Schemes is described in the "Risk Management Reports Setup" section document;

- Regardless of whether the additional rules are for a group of contracts or an individual contract, the following actions are taken:
 - A Service Package is assigned a Risk Scheme (see the "WAY4™ Service Packages" document). In this case, all operations for all contracts using this Service Package will be analyzed according to the indicated rule.
 - A contract is assigned a newly created Risk Scheme (see document "Issuing Module"). In this case, operations for this contract will be analyzed according to the selected rule.
- In the "Full Info for <rule name>" form (see Fig. 2), the following fields, included in the "Risk Scheme Rules" group, must be filled in:
 - *Switch Tag* – this field may take one of the following two values:
 - ♦ "Activate For" – means that the rule is active for contracts where a Risk Scheme is indicated in the *Scheme (Single)* field or multiple Risk Schemes indicated in the *Scheme (Group)* field;
 - ♦ "Inactivate For" – means that the rule is inactive for contracts where a Risk Scheme is indicated in the *Scheme (Single)* field or multiple Risk Schemes indicated in the *Scheme (Group)* field;
 - *Scheme (Single)* – a field with a drop-down list for indicating a single Risk Scheme;
 - *Scheme (Group)* – a text field where multiple Risk Scheme codes, delimited by semicolons (;), are indicated.

This means that the fields included in the "Risk Scheme Rules" groups are used for configuring links between a rule and a group of contracts.

Chapter 3. Analyzing Suspect Operations

The "Monitoring" user group (see Fig. 3) is intended for analyzing suspect operations.

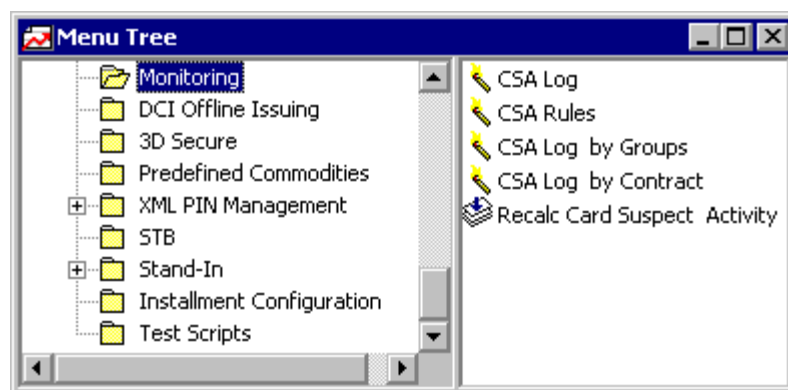


Fig. 3. User Menu for risk monitoring

In the following situations, transactions are verified according to rules registered in the system:

- During authorization;
- During posting of documents;

- While verifying all operations during a set time interval at user request.

During verification, the system analyzes information:

- According to rules configured for all transactions;
- According to rules configured for the Risk Scheme assigned to a corresponding card contract and/or Service Package.

As a result of transaction analysis, the system creates a special table in the database containing records on suspicious transactions.

List of Suspicious Transactions

To view the list of suspicious transactions registered in the system, select the "Monitoring → CSA Log" menu item, which will result in the opening of the "CSA Log" form and the one subordinate to it (see Fig. 4).

Registration Date	Contract	Risk Level	Channel	Amount	Curr	Trans Type	Trans Country	Return
16/04/03 20:10:16	5413330107540297		EPI	30 000,00USD		Retail	Afghanistan	Expired can
23/04/03 14:16:46	5413330132334682		EPI	200,00USD		Retail	Algeria	Not sufficien
23/04/03 14:17:38	5413330132334682		EPI	100,00USD		Retail		Not sufficien
23/04/03 14:18:58	5413330132334682		EPI	70,00USD		Retail	Algeria	Successful
24/04/03 11:34:56	5413330107540297			111 111,00USD		Credit	Russia	Chain not fc
24/06/03 12:22:55	5413330153196572			800,00RUR		Retail	Russia	Successful
19/06/03 16:43:52	5413330153196572		Internal	800,00RUR		Retail	Russia	Successful
20/06/03 16:38:06	5413330102992758		EPI	120,00USD		Retail	Iraq	Successful
20/06/03 18:07:18	5413330102992758		EPI	321,00USD		Retail	Iraq	Successful
24/06/03 11:38:06	5413330102992758		EPI	13,00USD		Unique	American Samoa	Successful
24/06/03 11:44:24	5413330153196572		Internal	6 000,00RUR		Retail	Russia	Not sufficien
24/06/03 11:46:02	5413330153196572		Internal	5 000,00RUR		Retail	Russia	Not sufficien
24/06/03 11:56:18	5413330153196572		Internal	4 500,00RUR		Retail	Russia	Not sufficien

Group Code	Risk Level	Risk Value
Risky Country		0,0000
Total Amount		0,966667
Single Amount		0,973333

Fig. 4. Grids for viewing information on registered suspicious transactions

The grid "CSA Log" contains the following transaction data:

- *Registration Date* – date and time when the transaction was registered as suspicious;
- *Contract* – card contract number;
- In the *Risk Level* field, an indicator bar is displayed showing the transaction's general risk level; the indicator's color and size depend on the value set in field *Risk Value*. Black indicates a very low risk level, blue is a low risk, green is a medium risk, orange is a high risk and red is a very high risk level.
- *Channel* – name of transaction message channel, for example, "VISA", "EPI", "Our ATM", "Our VISA Cards" and so forth;
- *Amount* – transaction amount;
- *Curr* – currency amount;
- *Trans Type* – transaction type;
- *Return Code* – system return code;
- *SIC Code* – code determining the type of retail outlet (SIC/MCC); the value is taken from the list of registered codes in the "SIC Codes" table ("Full → Configuration Setup → Main Tables → SIC Codes");
- *Trans Condition* – conditions in which the transaction will be executed; the list of transaction conditions is described in the document "Documents";

- *Risk Factor* – a general coefficient assessing the risk level of an operation (from 0 to 1) which is calculated on the basis of all risk levels from individual rules (see the description below of the child form of the "CSA Log" form;
- *Status* – status of the record on the suspicious operation; this field may take on the value "Active", "Inactive" or "Closed".

To change the status of a record, select that record in the "CSA Log" form and click on the [Status] button. In the "Suspicious Card Activity Status" grid (see Fig. 5) indicate the new status in the *New Status* field, add comments, if need be, in the *Comment* field and click on the [Proceed] button.

Fig. 5. Form for changing the status of a suspicious activity record

To analyze a transaction, click on the [Messages] button in the "Suspicious Card Transactions" grid. By this command, the screen will display the grid "Messages for Suspicious Card Transactions" (see Fig. 6), containing messages formed by the system during document posting.

Messages for Suspicious Card Transactions		<< < > >>	1 of 9	b x
	Message Name	Type	Date	
→	Risky SIC Group	vWarning	24/06/2003 11:56:18	
	Threshold = 2; Actual = 2; Usage = 100.00%	vWarning	24/06/2003 11:56:18	
	EVENT=EVNT_CODE;	vWarning	24/06/2003 11:56:18	
	Threshold = 3; Actual = 3; Usage = 100.00%	vWarning	24/06/2003 11:56:18	
	051-Not sufficient funds available	Error	24/06/2003 11:56:18	
	Total Amount	vWarning	24/06/2003 13:01:40	
	Threshold = 1,000.00; Actual = 5,100.00; Usage = 510.00%	vWarning	24/06/2003 13:01:40	
	Single Amount	vWarning	24/06/2003 13:01:40	
	Threshold = 800.00; Actual = 4,500.00; Usage = 562.50%	vWarning	24/06/2003 13:01:40	
Query				

Fig. 6. Grid showing system messages

In the *Message Name* field in the "Messages for Suspicious Card Transactions" grid, three rules by which the transactions were deemed suspicious are shown in bold letters with this information: the rule's threshold value, the actual transaction value, and the usage value showing the percentage by which the threshold value was exceeded.

To access data on the card contract for which the transaction was executed, select its record in the "CSA Log" form and click the [Card Info] button.

To access information for the document on the suspicious operation, select its record in the "CSA Log" form and click on the [Doc-Full] button.

The child form for the "CSA Log" form displays details on how the rule determined the operation to be suspicious. The child form may be accessed from the "CSA Log" form by clicking on the [Rules] button and contains the following fields:

- *Group Code* – rule code;
- In the *Risk Level* field, an indicator bar is displayed showing the general risk level of the operation; the indicator's color and size depend on the value set in field *Risk Value*. Black indicates a very low risk level, blue is a low risk, green is a medium risk, orange is a high risk and red is a very high risk level.
- *Risk Value* – a general coefficient assessing the risk level of an operation (from 0 to 1) in the rule; the coefficient is calculated as the ratio between the actual document parameters and the threshold parameter while taking into account a certain criteria weight.

To view full information on the rule by which the operation was deemed suspicious, select the rule in the child form of the "CSA Log" form and click on the [Rule] button.

To access the list of documents through which the operation was deemed suspicious, select the rule in the child form of the "CSA Log" form and click the [Docs] button.

List of Transactions Grouped by Rules

In order to analyze the quantity of registered suspicious transactions, grouped according to rules, select the "Monitoring → CSA Log by Groups" menu item and, in the dialog form "Date From - To" (see Fig. 7), indicate the time beginning and ending the analysis period. Click on the [Proceed] button.

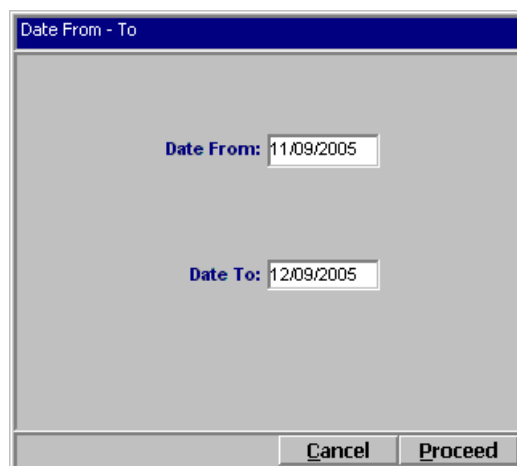


Fig. 7. Form for indicating the time period for which the data will be analyzed

The screen will display the "CSA Log by Groups" form (see Fig. 8), which will contain information on the quantity of registered suspicious transactions according to each rule defined in the system.

	Group Code	Number of Docs
→	Amount Fitting	5
	Amount Fitting2	0
	Change Country	3
	Risk Country	0
	Risk SIC	0
	Risky Country	0
	Risky SIC	0
	Risky SIC Group	0
	Risky SIC_Group	0
	Single Amount	0
	The Same Merchant	2
	Total Amount	0
	Utilization	0

Ins Del Query Rule Docs

Fig. 8. Form for viewing suspicious transactions by rules

Full rule information may be viewed by clicking the [Rule] button in the "CSA Log by Groups" form.

To view the documents that were deemed suspicious according to the given rule, click on the [Docs] button.

List of Transactions Grouped by Cards

To analyze registered suspicious transactions grouped by cards, select the "Monitoring → CSA Log by Contract" menu item and, in the dialog form "Time From - To", indicate the start and end date of the data analysis period, and click on the [Proceed] button.

The screen will display the "CSA Log by Contract" form (see Fig. 9), which will display information on the quantity of registered suspicious transactions by each card registered in the system.

	Contract	Number Of Docs
→	5413330132334682	17
	5413330107540297	12
	5413330102992758	3
	5413330153196572	7

Ins Del Query Docs

Fig. 9. Form for viewing suspicious operations by card

Documents that were recognized as suspicious by card can be accessed by the [Docs] button in the "CSA Log by Contract" form.

Creating the List of Suspicious Transactions

To create the list of suspicious transactions, start the "Monitoring → Recalc Card Suspect Activity" procedure. In the "Time From - To" dialog form (see Fig. 7), indicate the time interval within which the transactions will be analyzed, and click on the [Proceed] button.

This procedure removes all registered records as to suspect transactions for the period and, on the basis of the analyses of operations according to current rules, creates a new list of transactions.