Fraud Reporting Guide

Version: 1.1
23 August 2022

Global Processing Services
6th Floor, Victoria House, Bloomsbury Square, London, WC1B 4DA
Support Email: ops24@globalprocessing.com
Support Phone: +442037409682

For the latest technical documentation, see the Developer Portal.

Publication number: FRG-1.1-8/23/2022

Copyright

1 About This Document

This document describes how to use the GPS Mastercard fraud reporting facility to report fraud to Mastercard using the Fraud and Loss Database reporting service (previously known as the Mastercard System to Avoid Fraud Effectively (SAFE)).

Target Audience

This document is intended for GPS clients (Program Managers) who are using Mastercard.

What's Changed?

If you want to find out what's changed since the previous release, see the Document History section.

1.1 Related Documents

Refer to the table below for other documents which should be used in conjunction with this guide.

Document	Description
Chargeback Guide	Describes how to manage chargebacks using GPS.
Smart Client Guide	Describes how to use the GPS Smart Client to manage your account.

Other Guides

Refer to the table below for other relevant documents.

Document	Description
Mastercard SAFE Products User Guide	Explains the Mastercard System to Avoid Fraud Effectively (SAFE) and the SAFE Compliance Program.

2 Introduction

The Mastercard Fraud and Loss Database (previously System to Avoid Fraud Effectively (SAFE)) is a Mastercard repository of fraud transactions submitted by issuers. It is used for reporting, monitoring, and combating card fraud.

Mastercard requires issuers to report to the Fraud and Loss Database at the customer ID level all Mastercard transactions that the issuer considers to be fraudulent, even if the corresponding accounts are not closed or marked as fraud.

For issuers, Fraud and Loss Database reporting can be accessed directly via Mastercard Connect.

For other GPS customers, GPS provides an option on Smart Client to enable you to easily report a transaction as fraud to Mastercard. GPS sends a message to MasterCom using the MasterCom API.

2.1 MasterCom API

The MasterCom API offers Mastercard customers the ability to create and manage fraud reports in MasterCom. MasterCom is a system for dispute management and fraud reporting.

The MasterCom API is available to Program Managers and card issuers. GPS provides an interface to MasterCom via Smart Client, which means you do not need to develop your own MasterCom API integration. You need to opt in for the service with GPS. Please contact GPS Operations via JIRA.

Note: This service is only available in the MasterCom Europe/UK region. If you want access for another region, please contact both Mastercard and GPS to request this.

3 Using GPS for Fraud and Loss Reporting

Note: Access to Smart Client is required to use this service. In Smart Client, this service is still referred to as the **MasterCom SAFE report.**

3.1 Creating a MasterCom SAFE Report

You can use Smart Client to report fraudulent transactions to Mastercard.

To create a SAFE report:

1. Log in to Smart Client.
2. In the **Transactions** window, right-click the required transaction and select **Create MasterCom SAFE report**.

   The **Create MasterCom SAFE report** window is displayed.

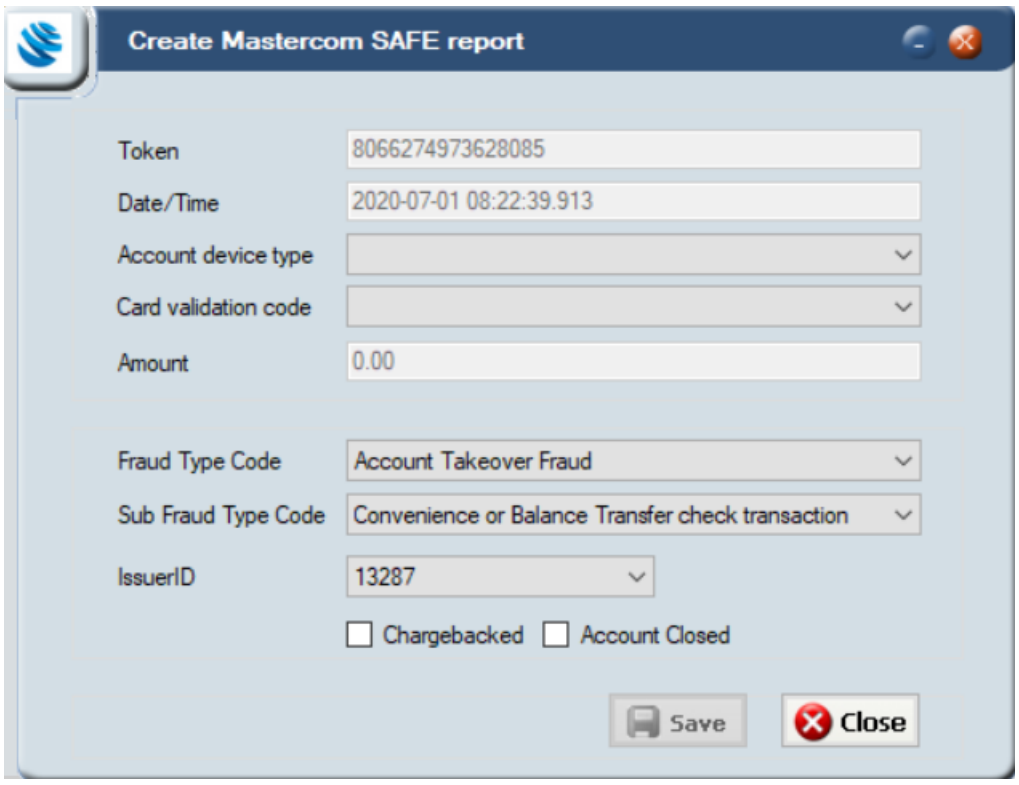

Figure 1: Create MasterCom SAFE Report Window

3. Provide all the details as per the instructions in the table below and click **Save**.

   The report is sent to MasterCom. A confirmation message is displayed, indicating if the SAFE Report request was successfully registered with MasterCom. In this case a *Claim ID* and *Fraud ID* are returned, which you can use to track the status of the request.

   If the SAFE Report request failed, a message box is displayed, providing details of the error. For example, an invalid claim ID. Please resolve the error and try again or contact GPS support.
4. To close the message box, click **OK**.

The created SAFE message is displayed in the **SAFE Report Details** window. See Handling Error Codes .

Option	Description
Token	Displays the unique token linked to the card PAN on which the transaction was made.
Date/Time	Displays the date-time stamp of the transaction.
Account device type	Select an option.
Card validation code	Select an option.
Amount	Displays the transaction amount.
Fraud Type Code	Select a fraud type option.

Option	Description
	Account Takeover Fraud Bust-out Collusive Merchant Card Not Present Fraud Counterfeit Card Fraud Fraudulent Application Lost Fraud Multiple Imprint Fraud Never Received Issue Stolen Fraud
Sub Fraud Type Code	Select a sub-fraud type code. Options include: Convenience or Balance Transfer check transaction PIN not used in transaction PIN used in transaction Unknown
Issuer ID	Displays the card issuer ID.
Charged Back	Tick this option if the transaction is Charged Back.
Account Closed	Tick this option if the account has been closed.

Handling Error Codes

An error code returned from MasterCom starting with '1' indicates errors from MasterCom; an error code starting with '5' indicates the error has occurred during GPS processing of chargeback request. You can try fixing the details and resending the chargeback request or contact GPS support.

3.2 Viewing SAFE Report Details

This option enables you to view details of all SAFE reports submitted to MasterCom.

1. From the Smart Client menu, select, **Card Activity > Safe Report Details**

   The **Safe Report Details** window is displayed.

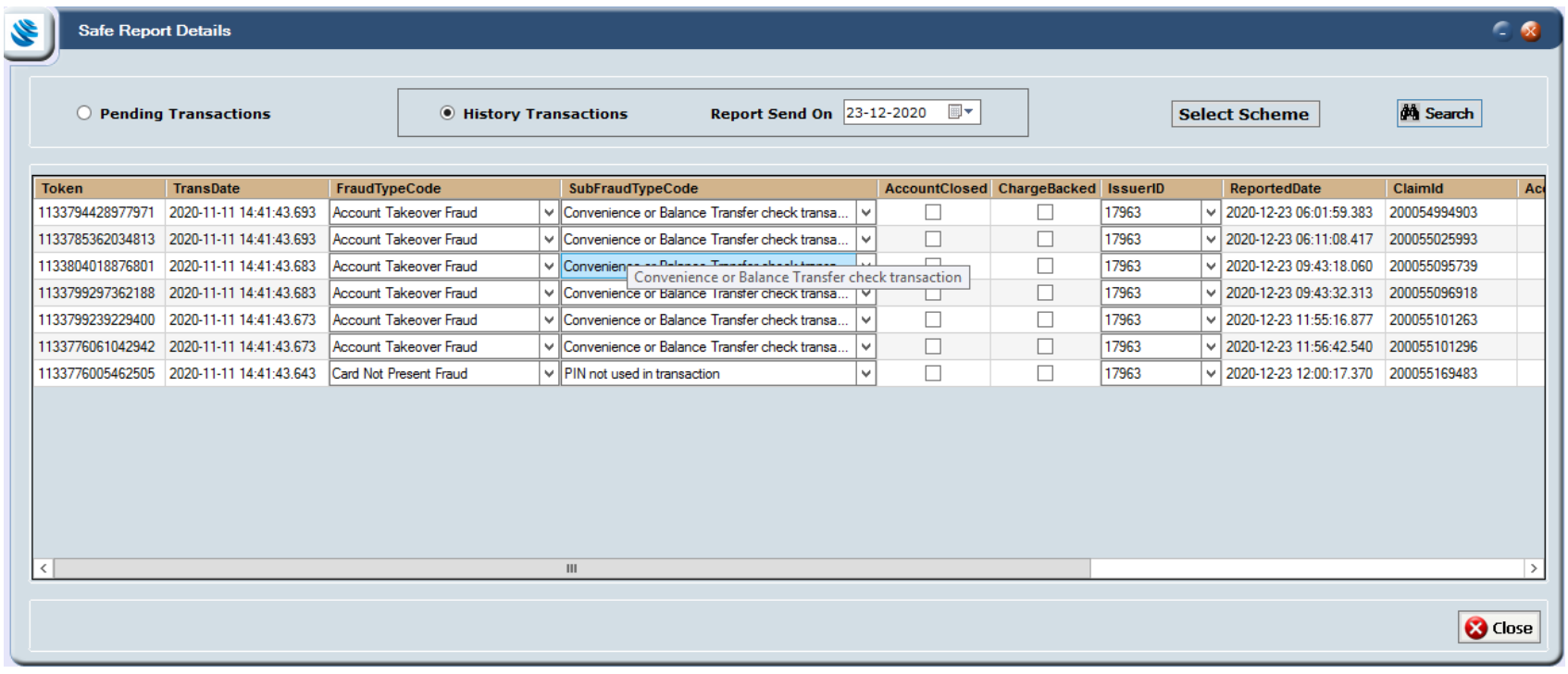

Figure 2: Safe Report Details Window

2. To view only pending transactions, tick the **Pending Transactions** option.

   Alternatively, to filter the list of historical transactions, tick the **History Transactions** option and select the **Date** range.
3. Click **Search**.

Contact Us

Please contact us if you have queries relating to this document. Our contact details are provided below.

Global Processing Services Ltd.

Support Email: ops24@globalprocessing.com

Support Phone: +442037409682

GPS Offices

UK Central Office	Singapore	Australia	Dubai, UAE
6th Floor, Victoria House	Republic Plaza	Stone & Chalk	EO 10, Ground Floor,
Bloomsbury Square	9 Raffles Place	Level 4, 11 York Street	Building 1
London	Singapore	Wynyard Green	Dubai Internet City
WC1B 4DA	048619	Sydney, NSW, 2000	Dubai, United Arab Emirates

Technical Publications

If you want to contact our technical publications team directly, for queries or feedback related to this guide, you can email us at: docs@globalprocessing.com.

Glossary

This page provides a list of glossary terms used in this guide.

C

Chargeback

Where a cardholder disputes a transaction on their account and is unable to resolve directly with the merchant, they can raise a chargeback with their card issuer. The chargeback must be for a legitimate reason, such as goods and services not received, faulty goods, or a fraudulent transaction. For more information, see the Payments Dispute Management Guide.

I

Issuer

The card issuer, typically a financial organisation authorised to issue cards. The issuer has a direct relationship with the relevant card scheme. For more information, see the Key Concepts Guide.

M

Mastercard Fraud and Loss Database

A Mastercard repository of fraud transactions submitted by issuers. It is used for reporting, monitoring, and combating card fraud. Previously know as: System to Avoid Fraud Effectively (SAFE).

MasterCom API

Mastercom API offers Mastercard customers the ability to create and manage dispute claims in Mastercom. Mastercom is a system for dispute management. All activities for any given dispute can be tracked within a single claim using Mastercom, including Retrieval Request and Fulfilment, First Chargeback, Second Presentment, Fraud reporting, Case Filing, and Fee Collection requests. All activities for any given dispute throughout its lifecycle can be tracked within a single claim.

P

PAN

The Primary Account Number (PAN) 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. The card's 16-digit PAN is typically embossed on a physical card. For more information, see the Key Concepts Guide.

S

Smart Client

Smart Client is GPS's user interface for managing your account on the GPS Apex system. It is also called Smart Processor GPS. Smart Client is installed as a desktop application and requires a VPN connection to GPS systems in order to be able to access your account. For more information, see the Smart Client Guide.

T

Token

Displays the unique token linked to the card PAN on which the transaction was made.

Document History

Version	Date	Description	Revised by
1.1	23/08/2022	New guide layout and HTML version now available	PC
1.0	21/07/2021	First version	WS