



Transaction Monitoring and Investigations Policy

Paysafe Internal – for Paysafe internal use only

Date Issued	9 th November 2017
Issue Number	2.0
Review Date	Annually
Published on	Policies and Procedures Jam page

Copyright © Paysafe Group

All rights reserved. This document and the information it contains, or may be extracted from it, is subject to the terms and conditions of the agreement or contract under which the document was supplied to the recipient's organisation.

None of the information contained in this document shall be disclosed outside of the recipient's own organisation without prior written permission of Paysafe Group, unless the terms of such agreement expressly allow.

In the event of a conflict between this document and a relevant law or regulation, the relevant law or regulation shall be followed. If the document creates a higher obligation, it shall be followed as long as this also achieves full compliance with the law or regulation.

Use of language

Throughout this document, the words '**may**', '**should**' and '**must**' when used in the context of actions of Paysafe Group or others, have specific meanings as follows:

- (a) '**May**' is used where alternatives are equally acceptable.
- (b) '**Should**' is used where a provision is preferred.
- (c) '**Must**' is used where a provision is mandatory.

Note that alternative or preferred requirements may be qualified by Paysafe Group in another referenced document.

Paysafe Group and the companies in which it directly or indirectly owns investments are separate and distinct entities. In this publication, however, the collective expression '**Paysafe**' and '**Paysafe Group**' may be used for convenience where reference is made in general to those companies. Likewise, the words '**we**', '**us**', '**our**' and '**ourselves**' are used in some places to refer to the companies of the Paysafe Group in general. These expressions are also used where no useful purpose is served by identifying any particular company or companies.

In this document, **third party** means any individual or organisation you come into contact with during the course of your work for us, and includes actual and potential clients, customers, suppliers, distributors, business contacts, agents, advisers, and government and public bodies, including their advisors, representatives and officials, politicians and political parties.

NOTE: All printed copies of this document are NOT COPY CONTROLLED and are to be used for INFORMATION ONLY as printed copies will not be automatically updated. Not to be shown outside Paysafe. This document may not be disclosed to any external party without the permission of the document owner.

INTERNAL

Summary:

The purpose of this Compliance Policy is to set out the process relating to ongoing transaction monitoring and investigation and act as a reference to enable to make accurate decisions.


Review and maintenance

This Policy will be reviewed and maintained by the Head of Policy and Assurance at least on an annual basis. The provisions of this policy can be amended and supplemented from time to time by the Senior Vice President, Compliance.

Supporting Policy

Global Compliance Policy

Document Approval

Date approved	Approved by	Signed by	Signature
9th November 2017	Elliott Wiseman General Counsel and Chief Compliance Officer	Maximilian von Both Senior Vice President, Compliance	

NOTE: All printed copies of this document are NOT COPY CONTROLLED and are to be used for INFORMATION ONLY as printed copies will not be automatically updated. Not to be shown outside Paysafe. This document may not be disclosed to any external party without the permission of the document owner.

INTERNAL

TABLE OF CONTENTS

1. INTRODUCTION	5
2. WHO DOES THIS POLICY APPLY TO?	6
3. PAYSAFE’S APPROACH TO TRANSACTION MONITORING	6
4. ONGOING TRANSACTION MONITORING	8
4.1. Review and update of Paysafe money laundering and terrorist financing typologies	9
4.2. Review and update of automatic systems rules	10
4.3. Information Sources	10
5. INVESTIGATIONS	11
5.1. When do we carry out investigations?	12
5.2. AML/CTF initial investigation	12
5.3. Compliance Department investigation	12
6. COMPLIANCE SPOT CHECKS	13
6.1. Compliance reports to the responsible MLRO	14
7. HOW WE HANDLE AND RETAIN THE RECORDS OF ALL CHECKS CARRIED OUT BY US	14

NOTE: All printed copies of this document are NOT COPY CONTROLLED and are to be used for INFORMATION ONLY as printed copies will not be automatically updated. Not to be shown outside Paysafe. This document may not be disclosed to any external party without the permission of the document owner.

INTERNAL

1. Introduction

It is Paysafe's policy to conduct all of our business in an honest and ethical manner.

The purpose of this Compliance Policy is to clearly set out the:

- essential transaction monitoring of threats and patterns by Paysafe to prevent money laundering and terrorist financing and to detect suspicious transactions; and
- processes to be followed when transaction monitoring systems detect potentially suspicious activity.

This Compliance Policy must be followed unless there are exceptional circumstances justifying a variation.

If an employee considers that this Compliance Policy is not applicable for an activity covered within the scope of this document, the individual must seek permission from the responsible MLRO or their approved delegate before deviating from this Compliance Policy.

A failure to follow this Compliance Policy could severely harm Paysafe's reputation, financial standing and possibly breach the terms of the licences necessary to operate our business. Any such failure may result in disciplinary action or termination for any employee found to have breached this Compliance Policy and may constitute a criminal offence.

This Compliance Policy supersedes all previous group policies setting group policy regarding transaction monitoring and investigations and is supplemented by the *Transaction Monitoring and Investigations Guidance Notes*. It should be read together with the:

- Paysafe Code;

NOTE: All printed copies of this document are NOT COPY CONTROLLED and are to be used for INFORMATION ONLY as printed copies will not be automatically updated. Not to be shown outside Paysafe. This document may not be disclosed to any external party without the permission of the document owner.

INTERNAL

- Global Compliance Policy;
- Customer Due Diligence Policy;
- Merchant and Distributor Due Diligence Policy; and
- Escalation and SAR Policy.

This Compliance Policy primarily focuses on European regulations, and sets a minimum group-wide standard, based on the strictest law within the EU. If specific local regulations, outside of the EU, require higher standards or stricter provisions, the local entity will always comply with such local regulations. Less strict rules will only be implemented if they have a clear legal basis, are accepted by local supervisory authorities (where appropriate), and are approved by the responsible MLRO.

A glossary of defined terms is included at section 8 of this Compliance Policy.

Where can I find further information?

Further explanation of the detailed business processes described in this Compliance Policy can be found in the supporting *Transaction Monitoring and Investigations Guidance Notes*.

2. Who does this Policy apply to?

This Compliance Policy applies to all Paysafe employees.

3. Paysafe's approach to transaction monitoring

Paysafe is committed to:

- establishing processes and controls so that we can monitor our

NOTE: All printed copies of this document are NOT COPY CONTROLLED and are to be used for INFORMATION ONLY as printed copies will not be automatically updated. Not to be shown outside Paysafe. This document may not be disclosed to any external party without the permission of the document owner.

INTERNAL

user accounts (customers, merchants and distributors) and transactions on an on-going basis;

- having clearly documented processes which are easily accessible and understood by our employees;
- having documented service levels in place with any third party service providers who provide ongoing transaction monitoring services and monitoring performance against these agreements;
- ensuring that our staff are trained on their responsibilities and can carry out their role effectively;
- carrying out ongoing monitoring, audits and reviews to confirm that our processes are effective and comply with applicable law and that senior management are regularly updated on the findings of these reviews.

This Compliance Policy applies to the ongoing transaction monitoring of users (customers, merchants and distributors) for **all** Paysafe businesses and is split into the following areas:

- Ongoing transaction monitoring;
- Investigations;
- Compliance spot checks; and
- Document and data retention.

NOTE: All printed copies of this document are NOT COPY CONTROLLED and are to be used for INFORMATION ONLY as printed copies will not be automatically updated. Not to be shown outside Paysafe. This document may not be disclosed to any external party without the permission of the document owner.

INTERNAL

4. Ongoing Transaction Monitoring

Paysafe monitors all transactions (by customers, merchants and distributors) on an on-going basis using a risk-based approach. The intensity of our monitoring depends on the level and nature of the risks identified by Group Compliance. Where a higher risk of money laundering or terrorist financing is detected a more enhanced and focused approach is used and stricter thresholds and measures are implemented.

Paysafe's transaction monitoring systems can detect suspicious activity based on money laundering and terrorist financing typologies and indicators. Based on our risk assessment of products, users, countries and delivery channels, we have identified potential high risks for Paysafe which we mitigate through stringent transaction monitoring.

Our monitoring processes consist of ongoing transaction monitoring through both assurance checks and automated transaction monitoring using rules that reflect our experience of potentially suspicious transactions by:

- use of our known money laundering, terrorist financing and other illegal activity typologies (see *Escalation and SAR Policy*);
- identifying discrepancies between submitted and detected data (for example the IP addresses used and the user's country or origin);
- cross referencing submitted data against that for other accounts (for example credit cards used by multiple holders); and
- use of systems that interface with third party sources to detect

NOTE: All printed copies of this document are NOT COPY CONTROLLED and are to be used for INFORMATION ONLY as printed copies will not be automatically updated. Not to be shown outside Paysafe. This document may not be disclosed to any external party without the permission of the document owner.

INTERNAL

criminal activities.

If you identify potentially suspicious behavior, you **must** follow the process set out in *Escalation and SAR Policy* to determine if any Internal SAR must be made.

We monitor transactions both in real time (i.e. when a transaction is about to take place) as well as after the event, when the transaction has already been executed. For this purpose Paysafe has defined several thresholds and rules and implemented automated reports with predefined criteria.

As such, our transaction monitoring processes are designed to detect suspicious activities based on money laundering and terrorist financing typologies and indicators. The implemented thresholds, rules and reports are also based on the Compliance Department's risk assessment.

4.1. Review and update of Paysafe money laundering and terrorist financing typologies

The Compliance Department is responsible for ensuring that the money laundering, terrorist financing or other illegal activity typologies that relate to Paysafe products are updated to reflect our ongoing experience.

As such, the Compliance Department **must** confirm to the responsible MLRO each quarter that the:

- typologies being used to identify potentially suspicious activity are current and standardized across our businesses to the extent appropriate given our risk assessment;

NOTE: All printed copies of this document are NOT COPY CONTROLLED and are to be used for INFORMATION ONLY as printed copies will not be automatically updated. Not to be shown outside Paysafe. This document may not be disclosed to any external party without the permission of the document owner.

INTERNAL

- these typologies are reflected in our systems' rules.

Further information on these typologies is set out in *Escalation and SAR Policy*.

4.2. Review and update of automatic systems rules

Monitoring **must** include a review of any applicable systems rules to ensure that:

- the rules remain relevant and current;
- new rules are incorporated into the system promptly and effectively;
- the rules are correctly applied; and
- our systems are operating effectively.

In addition, the output of alerts from the systems **must** be sample checked on a quarterly basis to ensure that the triaging of alerts is conducted in line with the set parameters.

4.3. Information Sources

Paysafe uses the following information sources to detect high-risk behavior:

- Data Warehouse (DWH) – data source which aggregates a multitude of transactional and master data collected from Paysafe's operations.
- ThreatMetrix – data source which is an integrated online platform used for rule definitions on risk scoring of paysafecard individual transactions and the review

NOTE: All printed copies of this document are NOT COPY CONTROLLED and are to be used for INFORMATION ONLY as printed copies will not be automatically updated. Not to be shown outside Paysafe. This document may not be disclosed to any external party without the permission of the document owner.

INTERNAL

of the monitored transactions.

- Actimize – an automated platform used for rule definitions on risk scoring of Neteller's individual transactions and the review of monitored transactions.
- Accertify – an integrated online platform used for rule definitions on risk scoring of Skrill's individual transactions and the review of the monitored transactions.
- Jade, paysafecard and Skrill Admin web interface – data source with account and registration information of customers
- YUNA Customer Care web interface – internal data source with account and registration information of YUNA customers.
- Salesforce – online platform for case management and administration of customers, merchants, distributors, and investigations (including police inquiries and complaints) with regard to the Paysafe products.
- LexisNexis Bridger Insight XG (BIXG) – hosted platform allowing access to watchlists for sanctions and PEP screening, as well as custom watchlists for high-risk or blacklisted individuals.

An analyst may also use publicly available information for further checks (e.g. web searches)

5. Investigations

NOTE: All printed copies of this document are NOT COPY CONTROLLED and are to be used for INFORMATION ONLY as printed copies will not be automatically updated. Not to be shown outside Paysafe. This document may not be disclosed to any external party without the permission of the document owner.

INTERNAL

As part of our transaction monitoring processes, Paysafe is committed to having effective and transparent procedures for the accurate and prompt investigation of suspicious activities.

Where can I find further information?

- Further information is set out in the *Escalation and SAR Policy*.

5.1. When do we carry out investigations?

An investigation into a user **must** be carried out by the Compliance Department when:

- an employee has escalated the matter following concerns they may have relating to the user's activity; or
- when Paysafe's automatic systems generate an alert warning of potentially suspicious activity.

5.2. AML/CTF initial investigation

AML/CTF cases are only referred to the Compliance Department after a thorough initial investigation by the relevant business.

The referral **must** contain full details of the investigation conducted using the template provided by the Compliance Department.

5.3. Compliance Department investigation

NOTE: All printed copies of this document are NOT COPY CONTROLLED and are to be used for INFORMATION ONLY as printed copies will not be automatically updated. Not to be shown outside Paysafe. This document may not be disclosed to any external party without the permission of the document owner.

INTERNAL

AML/CTF cases referred to the Compliance Department will be examined to detect any suspicious activity, following the procedures set out in the *Escalation and SAR Policy*.

Where can I find further information?

Further explanation of the investigative steps to be followed can be found in the *Escalation and SAR Policy*.

6. Compliance spot checks

As set out in the *Global Compliance Policy*, the responsible MLROs are responsible for the design and implementation of systems and controls necessary to mitigate the money laundering and the financing of terrorism risks presented by our businesses.

On behalf of Paysafe's MLROs, the Policy and Assurance Team has established risk-based internal compliance controls to ensure compliance of business processes with policies and guidelines. This includes the periodic spot checks of the following processes:

- Transaction Monitoring;
- Customer Due Diligence;
- Merchant and Distributor Due Diligence;
- Training and Awareness;
- SAR Reporting;

NOTE: All printed copies of this document are NOT COPY CONTROLLED and are to be used for INFORMATION ONLY as printed copies will not be automatically updated. Not to be shown outside Paysafe. This document may not be disclosed to any external party without the permission of the document owner.

INTERNAL

- PEP and Sanction checks;
- Policies and Procedures;
- Management Information;
- External Reporting & RFIs;
- Customer Complaints & Police Requests;
- Risk Assessment (e.g. Risk Matrix and Country Blacklist);
- Conduct (ABC, Gifts, Whistleblowing).

Checks are carried out on a risk assessed based - monthly, quarterly or yearly basis depending on the topic and the risks.

6.1. Compliance reports to the responsible MLRO

The Policy and Assurance team will report monthly to the responsible MLRO (or on an as needed basis):

- Number of spot checks
- Topics covered
- Overview of all checks performed
- Findings of the spot checks
- Measures taken or Recommendations

The responsible MRLO will then summarize the findings in his/her regular reporting to senior management.

7. How we handle and retain the records of all checks carried out by us

NOTE: All printed copies of this document are NOT COPY CONTROLLED and are to be used for INFORMATION ONLY as printed copies will not be automatically updated. Not to be shown outside Paysafe. This document may not be disclosed to any external party without the permission of the document owner.

INTERNAL

All documents, data and other information will be kept and held in accordance with the *Record Retention Policy*.

The contents of all checks and investigations **must** remain confidential to the Compliance Department, the responsible MLRO and General Counsel.

All action taken by the Compliance Department **must** be recorded.

NOTE: All printed copies of this document are NOT COPY CONTROLLED and are to be used for INFORMATION ONLY as printed copies will not be automatically updated. Not to be shown outside Paysafe. This document may not be disclosed to any external party without the permission of the document owner.

INTERNAL