



Escalation and SAR 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 assist all employees by clearly setting out the processes that must be followed if anyone has knowledge, suspicion or reasonable grounds for suspicion that Paysafe product is being used for money laundering, terrorist financing or other criminal activities.


Review and maintenance

This Policy will be reviewed and maintained by the Paysafe 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 Paysafe 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	6
2. WHO DOES THIS POLICY APPLY TO?	7
3. NOMINATED OFFICER – PROCEEDS OF CRIME ACT 2002 (POCA)	8
4. WHAT IS SUSPICIOUS ACTIVITY?	8
4.1. Money laundering and terrorist financing	9
4.2. Our experience	9
4.3. High-risk activities	9
5. OUR INTERNAL REPORTING PROCESS	11
5.1. Suspicious activity identified	12
5.2. Who is the responsible MLRO?	13
5.3. Investigative steps to be considered	13
5.4. Content of an Internal SAR	16
5.5. Failure to make an Internal SAR	16
5.6. Tipping off	17
6. OUR EXTERNAL REPORTING PROCESS	17
6.1. Who is responsible for external reporting?	17
6.2. MLRO review	18
7. COMMUNICATION AND DISCLOSURE OF INFORMATION	19
8. ONGOING MONITORING OF SAR ESCALATIONS AND DECISIONS	19
9. GLOSSARY	20
APPENDIX 1	22

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

INTERNAL SAR CHECKLIST	22
APPENDIX 2	24
KEY TRAITS OF AN E-MONEY LAUNDERER	24
APPENDIX 3 FURTHER GUIDANCE ON SUSPICIOUS ACTIVITY	26
APPENDIX 4	33
FURTHER GUIDANCE ON SUSPICIOUS ACTIVITY	33

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 assist all employees by clearly setting out the processes that must be followed if anyone has:

- suspicions that a Paysafe product is being used for money laundering, terrorist financing or other criminal activities;
- reasonable grounds to suspect that any attempted, upcoming, ongoing or previously conducted transaction involving Paysafe products may constitute criminal conduct or have involved the proceeds or funding of criminal 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 written 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 *Escalation and SAR Policy* and may constitute a criminal offence.

This Compliance Policy supersedes all previous group policies regarding Escalation and SARs and is supplemented by the *Escalation*

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

and SAR Guidance Notes. It should be read together with the:

- Paysafe Code;
- Global Compliance Policy;
- Customer Due Diligence Policy;
- Merchant and Distributor Due Diligence Policy; and
- Transaction Monitoring and Investigations 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 Global Compliance Policy can be found in the supporting *Escalation and SAR Guidance Notes*.

Please also see the *Transaction Monitoring and Investigations Policy*.

2. Who does this Policy apply to?

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

This Compliance Policy applies to all Paysafe employees, directors and non-executives as well as all other workers who work with us (whether as consultants, secondees, volunteers, sponsors or otherwise).

3. Nominated Officer – Proceeds of Crime Act 2002 (POCA)

Paysafe Group has the responsibility to appoint a Nominated Officer in accordance with the Proceeds of Crime Act 2002 (POCA), of sufficient seniority.

The POCA is an Act of the Parliament of the United Kingdom which provides for the confiscation or civil recovery of the proceeds from crime and contains the principal money laundering legislation in the UK.

Paysafe nominated the VP Regulatory Compliance team as a Nominated Officer who is responsible for:

- receiving reports of suspicious activity from any employee in the business;
- considering all reports and evaluating whether there is - or seems to be - any evidence of money laundering or terrorist financing;
- reporting any suspicious activity or transaction to the National Crime Agency (NCA) by completing and submitting a Suspicious Activity Report;
- asking the NCA for consent to continue with any transactions that they've reported, and making sure that no transactions are continued illegally;

4. What is suspicious activity?

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

4.1. Money laundering and terrorist financing

Whilst there are specific definitions of “money laundering” and “terrorist financing” set out in the relevant legislation, in Paysafe we define money laundering and terrorist financing together as:

“Possessing, or in any way dealing with, or concealing, the proceeds of any crime. It also involves similar activities relating to, terrorist funds, which include funds that are likely to be used for terrorism, as well as the proceeds of terrorism.”

4.2. Our experience

We have found a number of recurring money laundering, terrorist financing or other illegal activity typologies that relate to Paysafe products. These almost all relate to various types of fraudulent activities that are “predicate offences to money laundering” (i.e. crimes which underlie money laundering) or other illegal activity including terrorist financing.

Based on our experience, we have identified certain activities that we treat as suspicious or high-risk (or very high-risk). If we identify such activity, we will investigate further and, if appropriate, notify the relevant authorities following the process set out in this Compliance Policy.

4.3. High-risk activities

A transaction is treated as high-risk or suspicious if it does not fit behavioral patterns associated with the average member (customer, merchant or distributor) of Paysafe products. Behavioral patterns derive from historical data

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

available to Paysafe. Transactions may also be defined as high-risk based on an analyst's experience whenever new or evolved fraud patterns have been identified.

A high risk or suspicious transaction **must** be investigated to see whether it shows one of the following components:

- fraud, theft or other known illegal activity;
- breach of the contract terms between Paysafe and merchants (or distributors);
- breach of the contract terms between Paysafe and customers;
- patterns of activity that cannot be explained for legitimate commercial reasons and that appear consistent with money laundering or other criminal activity.

These patterns of activity do not always indicate that suspicious activity has in fact taken place. You **must** always, however, investigate such observed suspicious patterns to determine what the causes of the pattern are likely to be.

Depending on the risk associated with the patterns (e.g. the volume of money involved, or a high degree of similarity to a recent activity already determined to be suspicious), we **may** choose to block involved vouchers, accounts or customers while we carry out our investigation.

We will file a SAR, following the process set out in paragraph 5 below, when we have:

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

- suspicions that a merchant, distributor or customer account is being used for money laundering, terrorist financing or other criminal activity; or
- reasonable grounds to suspect that any attempted, upcoming, ongoing or previously conducted transaction involving Paysafe products may constitute criminal conduct or involve the proceeds or funding of criminal activity.

You **must** ensure that you are familiar with the guidance included in this Compliance Policy:

- Appendix 2 sets out the key traits of an e-money launderer.
- Table 1 of Appendix 3 gives further guidance (based on our Paysafe business' experience) of key traits of suspicious activity.
- Appendix 4 explains some of the key money laundering, terrorist financing and other illegal activity typologies that we are aware of.

5. Our internal reporting process

There is a statutory obligation on all employees to report suspicious transactions, activity or content.

This Compliance Policy sets out the policy that **must** be followed to escalate concerns that an account may be being used for money

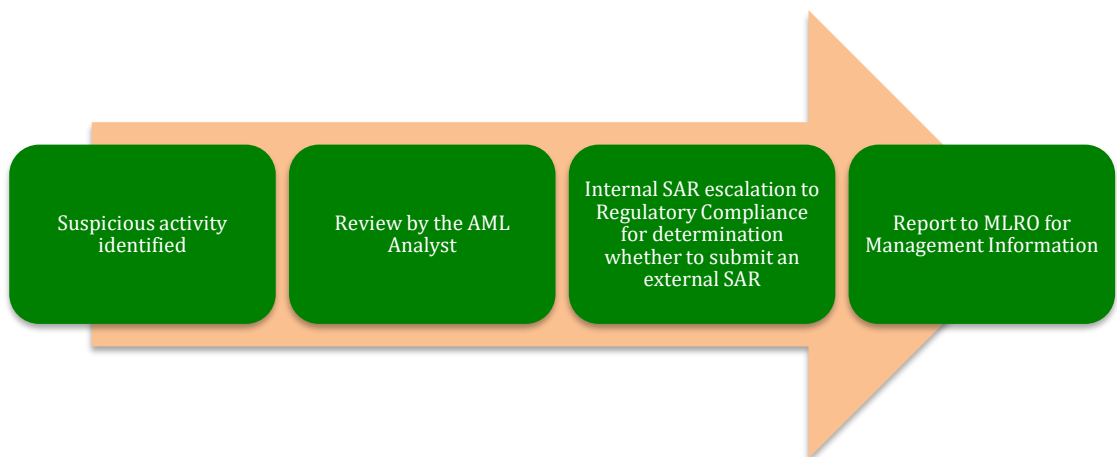
NOTE: All printed copies of this document are NOT COPY CONTROLLED and are to be used for INFORMATION ONLY as printed copies will not be automatically updated. Not to be shown outside Paysafe. This document may not be disclosed to any external party without the permission of the document owner.

INTERNAL

laundering or terrorist financing.

On escalation, the Regulatory Compliance Department **must** decide what further verification steps are to be taken or if the case needs to be reported to law enforcement agencies. A record of all internal money laundering reports **must** be kept to ensure proper record keeping and must be sent to the MLRO for Management Information.

Our Internal Reporting Process can be summarized as follows (**Figure 1**):



5.1. Suspicious activity identified

All employees are responsible for identifying suspicious transactions, activity or content.

- Suspicious activity must be reported as an Internal SAR to sar@paysafe.com.
- The AML Investigation Team must review the internal suspicious activity following the steps below to confirm the suspicion and then prepare the SAR report

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

for the National Crime Agency (NCA)¹ (as well as any other applicable Financial Intelligence Unit (FIU)). Regulatory Compliance reviews and submits the report to the NCA/applicable FIU on behalf of the MLRO.

5.2. Who is the responsible MLRO?

The responsible MLRO with Paysafe are:

- The Group MLRO of Paysafe Group or in his/her absence his/her deputy;
- Germany MLRO for business of “paysafecard.com Deutschland, Zweigniederlassung der Prepaid Services Company Limited”;
- Swiss MLRO for business of “paysafecard.com Schweiz GmbH” and MENA DMCC;

5.3. Investigative steps to be considered

The exact steps to be followed when investigating potential suspicious activity will depend on the circumstances and nature of the suspicion. In particular, when determining the appropriate level of investigation, you **must** take into account the nature of:

- the initial referral;
- the suspicion itself;

¹ NCA is the FIU for the UK.

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

- the degree of clarity around the suspicious activity;
- the number of accounts/products concerned;
- contact from the customer;
- the products being used; and
- the extent of knowledge about the account/products(s) concerned.

The goal of all investigations and Internal SARs review process is to fully understand the activity a customer is using our products and services for, establish the customer's profile, define the suspicious behaviour or activity, investigate and document all relevant data and then provide a reasonable conclusion to aid the responsible MLRO (or duly authorised delegate) to determine if escalation to the authorities is appropriate.

The following steps **should** be followed when compiling an Internal SAR. These steps **must** be considered in light of the Recommended Content of an Internal SAR (see paragraph 5.4 below):

- an initial review is carried out of the relevant account(s)/product customer info section, transaction history, financial details, comments section, duplicates info, log-in information, KYC on file.
- Member accounts linked by account information, behaviours and/or member to member relationships are thoroughly reviewed following a risk-based approach.

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

- Transaction details are analysed to establish transactional behaviours or patterns, or changes in them, to identify possible suspicious transactions; often the entire account history may look suspicious. When looking at transaction history, a number of criteria may need to be reviewed including: products being used, risks associated to those products; and any subsequent associated source of funds information.
- Sources of such information may include, inquiries with the payment processing teams, the business units, merchant enquiries, peer mates, and/or account review with the member.
- The comments section of a member's account is an ongoing archive of the member's data. The investigator can observe previously documented links, previously listed personal and financial information which has been changed, documentation collected/KYC notes, recorded email and live person exchanges, etc., all of which contribute to understanding the member's profile.
- Bank information or credit/debit card associated to the account should be observed.
- Searching a member's login IPs can be useful in establishing common IP users. For the purpose of a review, it is generally beneficial to set the date range for one year.
- Any known business relationships associated to the account (may be determined in the account review phase, noted in comments, flagged as an affiliate, business name in email domain, etc.) should be taken into consideration.

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

- Web search should be used to search for any possible adverse information.
- Review of the Responses of the member.
- If KYC documents are relevant to the investigation, they should be reviewed for authenticity and the conclusion clearly noted in the Internal SAR. If they are deemed in some way to be fraudulent or questionable, copies will be placed into the SAR folder.
- The SARs register must be completed with all pertinent information. An Internal SAR form must be populated, including a free form narrative summary of findings, and any conclusion (or lack thereof) about the activity that was reported as suspicious. Should the responsible MLRO (or duly authorised delegate) decide to escalate the case, the escalation would take place as soon as practicable.

5.4. Content of an Internal SAR

You **must** follow the recommended content checklist set out in Appendix 1 (Internal SAR checklist).

5.5. Failure to make an Internal SAR

A failure to make, without reasonable excuse, a report about a suspicious transaction is a breach of an employee's employment contract and may have disciplinary consequences. It may also constitute a criminal offence².

² Under the Proceeds of Crime Act 2002 (POCA 2002), it is a criminal offence for a person working in the regulated financial sector, if they fail to report where they have knowledge, suspicion or reasonable grounds for knowledge or suspicion that another person is laundering the proceeds of any criminal conduct.

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

5.6. Tipping off

It is a criminal offence for anyone to take any action to prejudice an investigation by informing the person who is or might be the subject of a suspicion report, or anybody else, that a disclosure has been made, or that the police or customs authorities are carrying out or intending to carry out a money laundering investigation³.

This means that you **must not** make any disclosure or do anything that you suspect might prejudice any investigation the police or other authorities may be undertaking

The responsible MLRO (or duly authorised delegate) **must** decide (on a case-by-case basis) how best to communicate with a suspicious customer/merchant (or distributor) to ensure compliance with these tipping off rules but at the same time avoid complaints to escalate (e.g. blocked accounts).

6. Our external reporting process

We are required to report promptly to the National Crime Agency (NCA) (as well as any other applicable financial intelligence unit (FIU)) any suspicious transactions and to maintain our internal control system so that suspicious transactions can be verified.

6.1. Who is responsible for external reporting?

The responsible MLRO (or duly authorised delegate) is responsible for submitting Suspicious Activity Reports (SARs) to the NCA and Paysafe's other external money laundering

³ Section 333 POCA 2002.

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

reporting duties (although any employee remains responsible to report any suspicious activity internally).

The MLRO **must** keep proper records of any decision not to make a report to the NCA.

6.2. MLRO review

The responsible MLRO (or duly authorised delegate) must review the Internal SAR without undue delay. All internal reports received by the responsible MLRO **must** be recorded on the internal "MLRO dashboard".

The MLRO **may** then require further investigation (e.g. to contact the customer, merchant or distributor involved asking for further information). The MLRO **may** also ask for additional blocking/unblocking actions to be taken in connection with the Internal SAR, and **must** record in writing the reasons for such requests.

The responsible MLRO **must** decide, in a timely manner, whether the available information provides sufficient grounds for reasonable suspicion to meet the standard required for filing a SAR with the financial intelligence unit (FIU) in the appropriate country. If that standard is met, the responsible MLRO **must** file an accurate, thorough, informative and timely SAR with the relevant FIU in accordance with regulatory guidelines and to complete any other notifications required to relevant regulatory bodies in the MLRO's area of responsibility.

The responsible MLRO must ensure that these actions are

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

carried out in a timely and competent manner.

If the responsible MLRO decides that the available information does not provide sufficient grounds for filing a SAR with the relevant FIU, the MLRO **must** document in writing the reasons for that decision.

7. Communication and disclosure of information

Once it has been decided that reasonable grounds for suspicion exist:

- you **must not** give any further information to external parties (other than law enforcement and authorised regulatory entities);
- the customer, merchant or distributor **may** be notified that the account is still under account review, but **must not** be told that suspicious activity is suspected or is being reviewed.

All information connected with Internal SARs and the detection of suspicious activity **must** be kept confidential within Paysafe and **must not** be shared with other employees unless necessary for them to carry out their job.

8. Ongoing monitoring of SAR escalations and decisions

The Compliance Department seeks to ensure that timely, accurate, risk sensitive decisions are being made about how best to comply with our obligations and ensure that appropriate activity is identified and, as necessary reported.

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

Periodic spot checks are made of accounts where potentially suspicious activity has been identified and the process and decisions taken are reviewed by the Compliance Department. This includes cases in which the decision has been taken not to file a SAR with external bodies, to ensure that such decisions are being taken and documented appropriately.

The results of these reviews are reported to the responsible MLROs, the Group MLRO and the Paysafe Audit Committee.

9. Glossary

Customer means any non-commercial user of the system, who has opened an account through the Paysafe websites and has signified their willingness to start using our products.

Device ID means a unique device identifier assigned by our monitoring system to the computing device used to make a transaction or to register for a new account.

EU means European Union.

FIU means Financial Intelligence Unit.

Internal SAR means a suspicious activity report made by an employee to following the checklist at Appendix 1.

KYC means Know-your-customer, the process, which begins at the time of signup, through which the business verifies the identity (name & date of birth) as well as the residence (address) of the customer, in accordance with the guidelines, provided by the UK Financial Conduct Authority (FCA).

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

Member means any user of our services.

MLRO means money laundering reporting officer.

NCA means National Crime Agency. NCA is the FIU for the UK.

PEP means Politically Exposed Person.

SAR means Suspicious Activity Report.

Verification means the act of verifying that the provided details and/or documentation are valid, truthful and correspond to the customer's details that the business has on file.

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

APPENDIX 1**INTERNAL SAR CHECKLIST**

- What is the concrete suspicious activity (detailed description of the suspicious activity)?
- Where and when has the suspicious activity taken place?
- How did we become aware of the suspicious activity?
- Why is the activity suspicious (i.e. suspicious in such a way that we are obliged to report it)? Include a detailed description of the facts that indicate a suspicion of money laundering/terrorist financing.
- Who are the suspected persons (real individuals⁴ who have been identified in the course of the investigations)? Is it a PEP or a sanctioned person? Add all the information you have about these persons to the Internal SAR (personal data and information about their transaction behaviour).
- How did we gather information about the suspected persons? If you have contacted a merchant, briefly describe what the merchant has been asked, what his answer was and how this information has been used in this Internal SAR.
- For real persons identified as suspects, why do we believe that these persons played an active role in the suspicious activity?
- Are there any patterns and similarities that form links between suspects or activities that might otherwise appear unrelated? Include

⁴ Real individuals are persons whose identity was verified with the help of an official identification document (e.g. ID card, driver licence, passport).

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

detailed descriptions of these patterns and similarities (e.g. when you have information that a group of suspects work together, describe how you have this information and how the individuals are linked).

- Have any Device IDs, accounts and/or cards (e.g. MasterCard, paysafecard voucher) been blocked? Add information about the blocked Device ID, account and/or card, date of block, reason for block, who blocked it.
- Have any accounts of the suspected person been identified? If so, name the account number and describe the transaction behaviour of the account holder. Describe any abnormalities identified on the account.
- Is there a link to an Internal SAR that has already been filed with the responsible MLRO? Include the Internal SAR number and describe the connection.
- What are the sources of information and is there any other information available that could be useful to the authorities?
- Describe what steps you have taken to investigate the suspicious activity, name the documents (e.g. excel files) where the results of the relevant analyses can be found and set out where any supplementary information can be found.

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

APPENDIX 2**KEY TRAITS OF AN E-MONEY LAUNDERER**

- Cross border transactions (IP Mismatches, Company Structure, Multiple Bank Accounts)
- Layering of casino winnings won by multiple accounts connected to a master account controlling the scheme
- Irregular or Short Term Account Usage. E.g. High value deposit, stays dormant for 6 months then withdrawn
- U Turn Transactions – Money Passes from one person or company to another, and back to the original person or company
- High Value One-off Transactions with no real explanation
- Member is defensive when requested ID documents
- Merchant activities are suspect based on URL check (in breach of the Paysafe Group Terms and Conditions, the website does not contain privacy statement, no legal documents supplied, missing Terms and Conditions, not registered with other regulated e-money payment options)
- Comments on account from the Fraud Department
- Multiple accounts with no identity documents, false identity documents or spurious registration details. E.g. incomplete telephone numbers, irregular postal codes, nonsensical first and last names.

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

- Suspect Country Traits – e.g. IP's registered from countries such as considered high risk (e.g. see *Merchant and Distributor Due Diligence Policy*).

Please take note that the above criteria are a strong indicator, but it is also limited in its application and none of the above have to be present in order to identify an E- money launderer.

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

APPENDIX 3
FURTHER GUIDANCE ON SUSPICIOUS ACTIVITY

TABLE 1: FURTHER GUIDANCE ON SUSPICIOUS ACTIVITY		
Suspicious Activity	Description	Trait
Non-delivery (confirmed)	Suspect ecommerce URL or auction merchant selling goods that are subsequently not delivered. The sellers usually sell their products and services by advertising them in social media and forums. The merchant withdraws profits or sends to another account to start up a similar operation. The sellers are usually unable to provide with delivery proof if such is requested for justifying the receipt of a particular payment. In confirmed non-delivery cases the money launderer creates the URL or auction site to defraud multiple buyers (> 5 complaints received). In a different variation of the scam the fraudster takes over a genuine auction site to process orders without delivering. Take over cases are achieved using phishing attacks, when the fraudster has gained access to an auction seller ID and password.	Non-response to ID request, multiple complaints as goods never dispatched, and the merchant has gone out of business, withdraws the profits of latest orders (previous good history), transactions serve a short-term purpose.
Fraud Proceeds laundered	In these cases, the money launderer creates a set of multiple accounts using stolen identities to fraudulently obtain funds. A stolen identity (also known as “ID Fraud” or “ID Theft”) is when a fraudster has accessed a name, address and the financial details of a victim he intends to defraud. How the fraudster collects and uses this information depends on his own creativity. In the section “Phishing Attacks” the most common method of identity theft is discussed. Once the fraudster has control of the victim’s account he sends stolen funds to connected accounts. To disguise the	Western European name and address, address verification fails by name and/or post code, IP mismatch with country of registration, Occasionally Mr. <female>, connected to other accounts by: similar emails, ‘passmates’, IP Mates, date of birth, time of registration, transaction pattern and ZIP code. When dialing telephone number person unknown by recipient.

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

	<p>fraud, he splits the payments, and then skims under transaction verification limits to avoid detection. Commonly, stolen identities are Western European or US profiles, with a transaction limit of 1000 EUR. Eventually, the money launderer will collect the funds, and then withdraw to his own bank account. Or, he will use a stolen identity to buy resalable goods such as Voice-Over IP credits, lottery tickets, virtual game credits and web design templates.</p>	
Betting fraud controller (BFC)	<p>A betting fraud controller is the main suspect account who collects the pay-outs generated by fraudulent activity at a betting firm. Paysafe ensures confirmation that pay-outs are generated by fraudulent activity is received from the casino. This means the casino will confirm either that a chargeback is received that confirms fraud; or that forensic evidence proves multiple accounts are connected (Forensic evidence includes password mates, IP mates and time of registration).</p>	<p>Winnings paid out simultaneously in similar values to a set of multiple accounts created using stolen Western European identities. The stolen identities are connected by IP or 'passmates' and have no prior funding via the Paysafe account. Fraudulent pay-outs are then collected by a main account or group with high-risk country traits.</p>
Credit card fraud laundered (CC/ML)	<p>A credit card fraud controller is similar to Betting Fraud, except that the main suspect collects the credit card fraud proceeds directly from the victim's accounts.</p>	<p>In a related scheme, CC payments are often from a set of cards with a similar BIN range (banking identification number is the first six digits of the card number). This type of CC fraud is known as 'Credit Master Fraud', which means a series of valid CC numbers are generated using a program that predicts card numbers, by analysing the algorithms of previously issued cards. Alternatively, CC/ML activity is a result of a Phishing Attack.</p> <p>Fraudulent Credit Card uploads will eventually</p>

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

		result in chargeback. A chargeback is when the genuine card holder contacts the card issuer (e.g. Visa, Amex, MasterCard) to dispute a card transaction.
Bank wire fraud laundered	<p>A bank wire fraud controller is the main suspect account, who collects the proceeds of bank wire fraud deposits, into an account held with Paysafe.</p> <p>Bank wire fraud payments are usually connected to an auction platform. In these cases, the fraudster tricks the victim into sending money via bank transfer to pay for non-existent goods. The fraudster will provide the customer with a reference to initiate the bank transfer. The reference is the customer account ID of Paysafe, created by the seller (fraudster) using the delivery address provided by the auction buyer (victim).</p> <p>The victim enters the exchange in good faith, under the impression that wire transfer funds will be received by the fraudster. Concern arises when the victim receives his bank statement which displays the Paysafe debit. Bank wire fraud cases are reported either by the victim, bank or the police investigating the case. Any available balances are refunded to the victim.</p>	Suspect connected to associate victim by password, similar emails, registered IP Address, time of registration, similar customer ID range, and transaction pattern. Bank Wire uploads of similar value in all associate victim accounts; then sent to main suspect account simultaneously.
False ID	Suspicion of False ID sent in to verify an account held with Paysafe e.g. Passport, driver's license or identity card - blurred ID, low resolution copy, coat of arms omitted; signature or font appears in a courier typographic, photos are not aligned, MRZ (Machine Readable Zone) does not	Linked by device, IP, password, time of registration, transaction pattern and address – city, zip code, street.

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

	<p>match the data in the document, the document template does not exist, details such as photograph, colouring, stamps look out of place. Depending on the quality of the false document it can be hard to spot.</p> <p>Employees authorised to complete document verifications undergo document verification training. According to the UK Fraud Act 2006, an offence is committed once false identity documents are submitted (Fraud Act 2006 (2) Fraud by false representation).</p> <p>Most common cases of false identification are related the verification of groups of fake accounts created for the purpose of promotion abuse. To receive more bonuses, a bonus abuser must create a large number of accounts that will be funded from one master account where the real details of the abuser will be registered. The other accounts will attempt verification with fake documents. When asked for explanation of activity, the customer provides unclear information that does not explain the transaction history.</p>	
Phishing Attacks	<p>Phishing attacks are predominantly designed by the fraudster to facilitate identity theft in order to 'hack' member accounts and defraud them. The Account Take Over (Controller) uses spoof emails to trick the member into disclosing their login details. The fraudster has altered the sender field of the e mail to make the victim think that the Paysafe Group customer services is requesting further information. Once the victim clicks on the Link to "update" information a fake website is displayed. The fake website will replicate the home page of the Paysafe Group. Except the URL supplied is not ww.paysafe.com.</p> <p>Often the Account Take Over (Controller) never reveals their</p>	<p>Merchant or customer complains account is "hacked" or lost balance. IP address reveals suspect last login not consistent with usual pattern of activity. Primary email address changed by fraudster. Series of false identities used to receive unauthorised payments, then subsequently sent to sports books/casinos or VOIP. Alternatively, fraudster receives payments then withdraws to his bank account.</p> <p>We use two sub-categories to analyse phishing cases:</p> <p>Account Take Over (Victim): Genuine member</p>

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

	<p>true identity and uses a number of stolen identities to collect the Account Take Over (Victim) funds, then redeems via another merchant, e.g. Casino or a Voice Over IP service provider. In other cases, the Account Take Over (Controller) reveals their identity by withdrawing Account Take Over (Victim) funds to their verified bank account.</p>	<p>whose funds are withdrawn</p> <p>Account Take Over (Controller): Stolen identity or main suspect who redeems the funds via another merchant using their own bank account.</p>
Cheque fraud	<p>Stolen Cheques used to deposit funds at the Paysafe Group. Finance receives notification from the bank, or an instant payment method such as Bibit, that cheques are stolen and subsequently charged back.</p>	
Child exploitation (CE)	<p>Indecent images of young children under the age of 18. Images hosted anywhere in the world. It is “an offence in the UK “to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children. Indecent should be taken as its dictionary meaning; as a guide it means any images of children, apparently under 18 years of age, involved in sexual activity or posed to be sexually provocative”.</p> <p>It is illegal both to distribute and to purchase indecent images of children. In particular, merchants offering a child modeling service must be automatically referred to the Compliance Department. Child modeling services can host private member pages with a pay per view opportunity. We report indecent images to both the Internet Watch Foundation and to NCA.</p>	<p>Child Modelling Agencies, private member pages, currency US dollars, slip ID reveals “model”, “girl”, private member purchasing images of children</p>
Infringement	<p>Unauthorised attempts to make, use, sell or have made a</p>	<p>Price substantially lower than expected (e.g.</p>

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

Intellectual Property Rights (confirmed)	property right owned by another. Merchant uses URL or auction platform to sell goods. This includes illegal downloads and pirated music, films, software, games etc.	Designer handbags sold for £50). Key words found in slip IDs (Hand bags, Region 0, Region All, Replica, Louis Vuitton, DVDs, etc.). Latest movie and music releases for sale or download, software at greatly reduced prices, hardware that allows pirated games to be played on console.
Money Exchange (Illegal)	<p>Suspect transactions sent with a payment reference of “e ac num xxx” or “exchange” to another, which are then forwarded on by the exchanger to a company based off shore with little or no CDD (Know Your Customer) requirements.</p> <p>Although Money Exchange can be a genuine activity, unregulated money exchange is regarded as unacceptable at Paysafe. An exchanger is reported when associate activity is predominantly related to any other high risk suspect. E.g. Pyramid Seller, Account Take Over (Victim) money, Credit Card or Bank Wire fraud.</p>	Payment instruction indicates “exchange”, account serves short term use, email address contains key words such as “forex” or “trader”.
<u>Illegal</u> breach of Paysafe’s Acceptable Business Policy (see Global Compliance Policy para 7)	For example: Firearms, hard-core pornographic content, Sale of Illegal Drugs.	

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

Pyramid selling	Pyramid selling is illegal in the UK. A Pyramid seller will promote rewards or bonus pay-outs to subscribers using multi-level marketing, get rich schemes, auto surf or high yield investment programs (HYIP). Legal low risk customer referral schemes can involve multi levels and are free to join.	To be confirmed as a pyramid seller, the scheme will involve more than two “levels” in the commission structure, paid membership and recruitment of new members.
High risk transactions	<p>When a new member deposits \geq EUR 10,000 we will request ID plus Postal Address Verification and an explanation.</p> <p>We request ID, address verification documents and a reason for the deposit for any first time high value deposit (\geq EUR 10,000). The deposit can only be processed upon approval from the MLRO or Compliance Department.</p>	
Terrorism	<p>Paysafe pays special attention to vulnerable industries such as charities, to prevent terrorist funding opportunities. On the surface terrorist funding will usually appear genuine, so it is therefore essential that effective Know Your Customer / Customer Due Diligence (CDD) checks are completed for all members. Additionally, for charities we collect the government registered charity number. For example: www.charity-commission.gov.uk. By collecting CDD documents, we can respond appropriately to any potential police investigations.</p>	

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

APPENDIX 4**FURTHER GUIDANCE ON SUSPICIOUS ACTIVITY**

Below are examples of patterns of behaviour which would be regarded as unusual activity and that may form the basis for investigation and ultimately a SAR.

It should be noted that these patterns do not always indicate that suspicious activity is taking place. As such, when one of these suspicious patterns appears, further investigative steps must be taken to determine what the causes of the pattern are likely to be.

a) Combination of multiple means of payment issued by Paysafe Group entities

Several means of payment issued by Paysafe Group offer financial services that can be combined or used to top up respective balances:

- paysafecard vouchers can be used to top up mypaysafecard accounts
- mypaysafecard accounts can be used to top up Skrill wallets, Neteller wallets as well as paysafecard prepaid MasterCards
- credit cards can be used to cashout funds from Skrill and Neteller wallets

The review of money laundering patterns and the review of involved individuals has shown that often a variety of means of payment is utilized for layering purposes when laundering money. Bearing in mind that each money transfer adds costs for the end-user (fees deducted from the balance for every money transfer), questions arise related to the benefit of customers. Furthermore, knowing that the mentioned accounts and wallets offer almost the same access to webshops, checking for the add-on value the customer aims for by transferring money is advisable.

There is behavior that can indicate possible money laundering intention:

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

- Newly registered mypaysafecard account customers who transfer money from their account to a Skrill or Neteller wallet as a first activity (instead of using any mypaysafecard account services or frequenting any webshops directly with their mypaysafecard account).
- Transfer of payouts from a mypaysafecard account to a Skrill or Neteller wallet, instead of using the cashout functionality or credit card with the mypaysafecard account directly.

Logins to the mypaysafecard accounts or the registration itself showing different geo location details than the payment or money transfer activities themselves.

b) Clustering of residential addresses (account registrations)

We have found that, when application fraud occurs, there will often be an unusually high number of payment accounts registered using the same or similar residential addresses. When multiple applications are registered in this way, there are typically a very small number of individuals actually controlling the accounts. As a result, they normally use a relatively small number of computing devices when setting up the accounts.

Residential addresses are also available with point of sales (POS). When analyzing patterns the review of POS locations can provide further evidence of linked individuals.

c) Clustering of similar registration data (account registrations)

Just as with clustering of residential addresses, we have found that groups of fraudulent account registrations often show clusters of similar usernames, email addresses and security questions and answers provided at registration. As with clusters of similar residential addresses, we find that clustering of usernames, email addresses and security questions and answers is highly associated with fraudulent activity.

d) Large transactions at a small set of merchants from a single device

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

or IP address, where IP address and/or browser language do not match issuing country

Whenever a large transaction volume at a single merchant, or at a small set of merchants, coming from a single device or single IP address is observed, there is a heightened risk that the transaction volume may represent suspicious activity.

However, in the absence of additional factors, such increased volume may simply represent a "high roller". One factor which increases the index of suspicion is a mismatch between the country of the IP address, and/or the language used in the browser settings, and the country where the account was set-up from.

Mismatches between the IP address country and the country of account registration is more significant than "mismatch" between country of account registration and browser language, as in every country there will be substantial minorities who are most comfortable using a language other than an official language of the country in which they live. However, when this type of suspicious behavior occurs, often there will be a very specific set of characteristics which recur across all transactions in the pattern, and consistent use of a specific browser language which is not an official language of the country where the account was opened is often a consistent characteristic across all transactions in a suspicious group.

Often, a highly specific pattern will be identified upon analysis, that will have a large enough number of distinctive features (which, in normal transaction activity, do not all typically appear together), and which is found to occur across more than one device and/or IP address.

e) Spike in transaction volumes at a specific merchant

A large spike in transaction volumes at a merchant is a high-risk pattern which is cause for concern, even when other known indicators of suspicious activity are not present. Whenever such a spike is detected,

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

enquiries must be made with the merchant concerning any knowledge they have about the abnormal transaction volumes, and investigation must be made to determine whether the transactions can be linked to other known suspicious activity.

There can be many reasons why this type of spike may occur, and not all of them are suspicious. As with the pattern described in the preceding section, this type of activity can result from a legitimate high roller who was not previously using our payment method or was using a different merchant. A spike could also occur as the result of a promotion that drives additional traffic. It is important to understand all of the known factors which may account for a spike before making a determination that the transaction activity is suspicious and, therefore, reportable.

f) High volumes of ATM withdrawals on a single payment account

An ATM facility is available only for accounts which have an associated physical MasterCard. Our experience with legitimate customers shows that it is very uncommon for them to make large or frequent ATM withdrawals. In cases involving suspicious ATM withdrawals, the pattern usually involves loading the account and then withdrawing the cash via ATM as soon as possible.

Often, the ATM withdrawals take place in a city located at a considerable distance from the residential address provided at registration for the account, and sometimes several such accounts (i.e. showing high ATM withdrawals and possible application fraud) can be linked together due to the presence of ATM withdrawals at ATMs located within the same small geographic area. The index of suspicion is also raised if the ATM withdrawals take place in a different country from the one in which the payment account was issued, as this can indicate use of the payment account to transfer funds cross-border.

-

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