DIGITAL SKYPAY LIMITED
AML/CTF POLICY

Table of Contents

1. Introduction

SkyPay Limited (hereinafter referred to as "SkyPay Limited", "SkyPay " or "Firm") provides Card Acquiring.

As a regulated entity, SkyPay Limited must implement and maintain robust and effective anti-money laundering (AML),counter terrorist financing (CTF) and sanctions / proliferation financing systems and controls. It is the policy of SkyPay to detect and actively pursue the prevention of money laundering and any activity that facilitates money laundering and other types of financial crime The Firm and its management is committed to AML and CTF compliance in accordance with applicable law and regulation.

Throughout this document, references to "employees" will include all employees (including temporary), consultants and directors of SkyPay , its agents and subsidiaries. Failure to follow this document by any employee may result in disciplinary action taken against the individual.

The Money Laundering Reporting Officer (MLRO) treats this manual as a live document which will be reviewed at least annually or sooner in the event of significant regulatory developments. All relevant employees are expected to familiarise themselves with this policy and all employees receive AML/CTF training appropriate to their role.

As employees in the regulated sector, all SKYPAY employees are responsible for ensuring the Firm meets our compliance obligations. Compliance is the responsibility of all employees and they MUST follow ALL policy, procedures and the training provided to operationalise these documents.

2. Objectives of this Policy

Through this Policy, the Senior Management of the Firm are committed to ensuring that SkyPay has in place adequate and proportional controls in relation to:

- Knowing clients (corporate or individual) appropriately at onboarding and on an ongoing business basis. SkyPay is committed to ensuring we do not engage in any business relationship without conducting the required due diligence;
- Taking appropriate steps to verify the client's identity and business along with the reason the client wishes to engage with us and what the client's activity is (e.g. what do they do for generating funds or financial activity e.g. salary and job, profit and business type etc); and

- Ensuring that all employees and third parties we rely upon are suitably trained and understand the law and their obligations, their importance that all employees know, and report suspect activity.

To achieve these objectives, the Firm must ensure:

- Deployment of adequate policies and procedures to ensure compliance with the requirements;
- Adequate 2nd and 3rd line monitoring is conducted to ensure policy is deployed effectively; and
- SkyPay adopts a culture of compliance when conducting business

3. The Regulatory Environment

The Firm is committed to maintaining the highest standards of financial crime compliance and adheres to all applicable laws, regulations, and guidance, including but not limited to:

- Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (as amended);
- Proceeds of Crime Act 2002;
- Terrorism Act 2000 (as amended by the Anti-Terrorism, Crime and Security Act 2001);
- Terrorist Asset-Freezing etc. Act 2010;
- Bribery Act 2010;
- Criminal Finances Act 2017;
- Anti-Terrorism, Crime and Security Act 2001;
- Counter-Terrorism Act 2008, Schedule 7;
- Applicable financial sanctions, in particular those administered by HM Treasury;
- The FCA Handbook and associated guidance, particularly its Financial Crime Guide; and
- The Joint Money Laundering Steering Group (JMLSG) Guidance.

Inherent to the business model of SkyPay is the provision of financial services to clients making international payments. SkyPay Limited will abide by all the relevant laws and regulations applicable in the jurisdictions in which it operates.

4. What is Money Laundering?

Money laundering (ML) is the process by which criminally obtained money or other assets (criminal property or the proceeds of crime) are exchanged for “clean” money or other

assets with no obvious link to their criminal origins. In this way, criminals aim to disguise the true

criminal nature of the assets to make it harder for police or investigatory authorities to seize these criminal assets.

Criminal property may take any form, including money or money's worth, securities, tangible property and intangible property. Money laundering activities include:

- Acquiring, using or possessing criminal property;
- Handling the proceeds of crimes such as theft, fraud and tax evasion;
- Being knowingly involved in any way with criminal or terrorist property;
- Entering into arrangements to facilitate laundering criminal or terrorist property;
- investing the proceeds of crimes in other financial products;
- Investing the proceeds of crimes through the acquisition of property/assets; and
- Transferring criminal property.

Money laundering is a distinctly different crime from the original underlying activity; however, SkyPay has chosen to put in place controls which make its services unattractive to criminals of all kinds, irrespective of whether the activity taking place is ML or other types of financial crime.

ML is not a single act but is in fact a process that is accomplished often in 3 basic steps/stages, placement, layering and integration. These stages are not distinct. They are very often overlapping with each other and repeated, making tracing of crime proceeds and their sources difficult.

5. What is Terrorist Financing?

Terrorism is the use or threat of action designed to influence government, or to intimidate any section of the public, or to advance a political, religious or ideological cause where the action would involve violence, threats to health and safety, damage to property or disruption of electronic systems.

Terrorist financing involves providing funds or financial support for terrorist activities. Funds used for terrorist financing can originate from both legitimate and illegitimate sources. Terrorists and terrorist organizations often use a combination of these sources, adapting their funding methods to exploit new technologies and financial systems. The diversity of funding sources makes it challenging for authorities to detect and prevent terrorist financing, as transactions may not always appear suspicious, especially when originating from legitimate sources.

The definition of "terrorist property" means that all dealings with funds or property which are likely to be used for the purposes of terrorism, even if the funds are "clean" in origin, is a terrorist financing offence.

6. What are Sanctions?

Sanctions are used by the international community, i.e. the UN, EU, US and UK:

- To encourage a change in behaviour of a target country or regime;
- To apply pressure on a target country to comply with set objectives;
- As an enforcement tool when international peace and security has been threatened and diplomatic efforts have failed; or
- To prevent and suppress the financing of terrorists and terrorist acts.

Financial sanctions are normally one element of a package of measures used to achieve one or more of the above. Financial sanctions measures can vary from the comprehensive – prohibiting the transfer of funds to a sanctioned country and freezing the assets of a government, the corporate entities and residents of the target country – to targeted asset freezes on individuals/entities.

SKYPAY predominantly uses four main administrators and enforcers of sanctions regimes.

- OFAC (US);
- HM Treasury;
- UN Sanctions; and
- EU Sanctions Lists.

For further guidance on SkyPay s' Sanctions processes refer to the separate document, "PEP/Sanctions Procedures".

7. What is Proliferation Financing?

Proliferation Financing is the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials. This includes technologies and dual-use goods intended for non-legitimate purposes. Proliferation financing can involve both legitimate and illegitimate sources of funds. It poses significant risks to the global

financial system and international security, requiring countries and financial institutions to implement measures to identify, assess, and mitigate these risks.

8. Risk Based Approach

The risk-based approach (RBA) is a strategic framework for identifying, assessing, and managing financial crime risks. It involves assessing financial crime risks and proportionate controls where risks are assessed to be greatest.

SkyPay Limited recognises the Firm's responsibility to apply a risk-based approach to AML/CTF as required by the relevant legislation.

The risk-based approach reduces the burdens imposed on some clients and allows the Firm to manage the risk that the services will be used to further money laundering or finance terrorism. The senior management at SkyPay Limited is aware that the risk-based approach cannot exist in isolation within the compliance function and its principles must be applied across the business.

Through training, procedures and cultivating a risk sensitive corporate culture, the senior management intends to infuse the Firm with an awareness of the risks that the Firm faces. The application of the risk-based approach is the responsibility of all Firm employees.

SkyPay deploys the following risk assessments in the application of the risk-based approach:

- AML- Whole Firm Financial Crime Risk Assessment ("WFRA");
- Industry risk assessment;
- Country risk assessment; and
- Customer Risk Assessment (refer to Business Assessment Policy).

These risk assessments are utilised to assess risk and deploy proportionate controls where the risks are assessed to be greatest.

9. AML- Whole-Firm Risk Assessment (WFRA)

The Whole-Firm Financial Crime Risk Assessment (WFRA) is the principal risk assessment in the firm's financial crime risk assessment and hence application of the risk-based approach. It acts as cornerstone of financial crime controls at the Firm.

SkyPay 's WFRA has been developed considering the following:

- National Risk Assessment, which is carried out and published yearly by the Interdepartmental Coordinating Group on Combating Money Laundering and the Financing of Terrorism ("CGMF");
- Mutual Evaluations conducted by FATF;
- Supranational Risk Assessment conducted and published by the European Commission;
- FCA Financial Crime Guide;
- EBA Risk Factor Guidelines (see Annex 4-II of JMLSG)1; and
- JMLSG (Part 2 Sectoral Guidance) for Firms2 .

SkyPay applied the high-level findings of these sources in order to determine risks that are specific to the SkyPay Limited business model.

The individual areas that must be risk assessed in order to better understand the Firm's vulnerabilities from an AML perspective include:

- Delivery channel;
- Products or services;
- Geographical areas of operation;
- Customers and where relevant ultimate beneficial owners;
- Operating environment; and
- Transactions.

The MLRO will ensure that SkyPay has a fully documented Risk Assessment methodology that is reviewed at least annually or on an event driven basis.

As the will enable senior management and the Firm to understand the risk profile of the Firm and the level of controls required based on our overall risk profile, the MLRO will also ensure that risk factors and considerations SkyPay needs to account for are incorporated into the risk assessment processes.

Upon completion of the periodic FWRA the MLRO will ensure that it is communicated to relevant employees within the Firm and coordinate follow-up actions according to the risks identified (e.g. updates to the Compliance Monitoring Plan).

For further guidance on the Firm's AML risk assessment please refer to the Whole Firm Risk Assessment.

10. Digital SkyPay Limited's Three Lines of Defence Model

SkyPay adopts the three lines of defence model. This ensures effective and independent oversight, and assurance that operations take place in line with policy set by the Board.

10.1 First Line (1LoD)

1LoD are responsible for deploying policy and procedure with due skill and care. At SkyPay , the first line is formed of Account Managers (AMs), Agents and/or Compliance Operations (which can be outsourced to assist agents). Collectively, they have the necessary knowledge, skills, information, and authority to apply their knowledge of the business and apply the relevant policies and procedures. This requires an understanding of the Firm, its objectives, the environment in which it operates, and the risks it faces.

The 1LoD are essentially the "risk-takers" in the Firm who will make measured risk decisions using risk assessments and advice provided by 2LoD.

Heads of Department and/or Managers on 1LoD have taken part in the development of the Firm's procedures, to ensure the operational procedures meet the policy requirements. Department leads will be responsible for reviewing and ensuring their processes meet the policy requirements, based on their technical expertise. They are also responsible for the adherence to policy within their teams.

10.2 Second Line (2LoD)

The 2LoD Compliance Team, acting in an advisory and monitoring capacity, as well as internal audit (outsourced to a third party), are the second line at SkyPay . Compliance will share policy and regulatory requirements and advise other departments on those requirements. This will feed into each departmental procedure document where necessary.

Each will share their operating procedures with the Management Committee for review and approval. Compliance will assess and challenge based on the regulatory requirements.

2LoD also provide 1LoD ad hoc advice and responses to escalations. This includes providing risk advice for consideration action by 1LoD.

Where required, legal will also advice, as part of the Management Committee review. Once a procedure has been reviewed and approved and meets the policy requirements it will be deployed. Compliance will then test the policy and procedures via a Compliance Monitoring Plan. Compliance will also deploy a Compliance Monitoring Plan for all agents. Where

regulatory or legislative guidance is unclear, legal will be asked to provide direction to compliance.

10.3 Third Line (3LoD)

SkyPay uses statutory auditors to perform the 3LoD function, rather than an internal audit function. The third line will independently test and monitor all policies and procedures and report to the management committee and board.

Sitting outside the risk management processes of the first two lines of defence, its main roles are to ensure that the first two lines are operating effectively and independently advise on improvements and enhancements Tasked by, and reporting to the Board, it provides an evaluation through a risk-based approach on the effectiveness of governance, risk management, and internal control to the organisation's governing body and senior management. It can also give assurance to sector regulators that appropriate controls and processes are in place and are operating effectively.

Additional guidance on SkyPay 's three lines of defence and the roles and responsibilities covered by the Firm, can be found in the Transaction Monitoring Procedure.

11. Money Laundering Reporting Officer ("MLRO")

SkyPay is required to appoint a MLRO.

The Money Laundering Reporting Officer, who has responsibility for overseeing the Firm's compliance with its regulatory obligations regarding AML systems and controls. If the MLRO is not available to carry out his duties a deputy MLRO acts on the MLRO's behalf, when necessary.

The MLRO has responsibility for the Firm's AML/CTF activities and must have sufficient experience, seniority, independence and resources to effectively oversee those activities within the Firm, therefore it will always be a senior employee or director who holds the MLRO position. The MLRO must also have access to all required information necessary to discharge the role.

Certain AML/CTF tasks may be delegated by the MLRO, but the ultimate managerial responsibility resides with the MLRO.

The MLRO, as with all EMD managers, must be screened each year and are required to notify the Firm of any issues that may affect their fit and proper status as they become aware of

them. Where any fitness or probity issues are identified these must be escalated to the board.

Where the MLRO is incapacitated no pre-approval of an interim MLRO (Deputy) is required for a period of 12 weeks, in any consecutive 12-month period. For any periods longer FCA approval is required.

Where the Firm has subsidiaries, the SkyPay MLRO will be appointed as group MLRO and the policy and all procedures that fall under this document will be regarded as group minimum standards that cannot be deviated from.

11.1 Responsibilities of the MLRO

- Acting as a focal point within the Firm for all matters relating to financial crime;
- Defining, developing, leading and embedding the Firm's framework relating to the management of financial crime risk;
- Understanding of relevant regulation as applicable to the Firm, including appropriate escalations;
- Ensuring AML/CTF, sanctions and fraud risk assessments are undertaken appropriate to the Firm's business, ensuring effective application of the risk-based approach;
- Ensuring relevant findings or guidance of HM Treasury, the Financial Action Task Force (FATF) are implemented;
- Development and maintenance of appropriate financial crime policies;
- Coordination of the Firm's strategy relating to financial crime guidance materials, training resources, ensuring alignment with the broader training strategy;
- Reviewing and decisioning of financial crime escalations and waivers as required by policy;
- Fulfilling the role of nominated officer for reporting to National Crime Agency, alongside responsibility for external fraud and sanctions reporting, including seeking licences from OFSI/OFAC and other jurisdictions (as appropriate);
- Leading and development of the AML and fraud team resource, working alongside management to ensure capacity and capability is appropriate for the Firm's business;
- Financial Crime regulatory reporting and compiling the annual MLRO report;
- Compilation and delivery of financial crime management information (MI) including resultant actions;
- Coordination with management to ensure financial crime risks remain top of mind and that controls are appropriate;
- Leading detailed ad-hoc investigations relating to non-compliance with AML/CTF, sanctions and fraud policies and procedures and reports; and

- Liaison with regulator(s), where necessary, including informing and/or corresponding with the regulators regarding any breaches of AML/CTF procedures and with the authorities on suspicious transaction disclosures.

11.2 Reporting MLRO Annual report

The MLRO annual report serves to evaluate the effectiveness of the Firm's financial crime controls, identify new risks, acknowledge weaknesses, and recommends improvements. The report typically includes an executive summary, overview of the MLRO's duties, assessment of policies and procedures, analysis of suspicious activity reports, review of training programs, and evaluation of high-risk clients and transactions. It also discusses breaches, areas for improvement, and action plans. The reporting period is each calendar year.

The basis of the report will be taken from the CMP, the annual financial crime report submitted to the FCA (REP CRIM - where applicable) and the overall testing of effectiveness outlined above, including any internal or external audit findings. The annual report will reflect the data captured in the quarterly board report.

Senior Management Review

The MLRO reports will be reviewed by senior management and the recommendations from the MLRO considered, along with any audit findings and recommendations. The MLRO should use the reports to make process improvement requests and proposals. Senior management should then consider the recommendations. Any significant remedial programmes will also be reported to senior management along with progress updates within the quarterly and annual reports.

Rep-Crim

Where required the MLRO will be responsible for the preparation and submission of the Annual Financial Crime Report (Rep-Crim) to the FCA. Regardless of the requirements to submit, the MLRO will use the Financial Crime Report as a basis for their internal reporting format, as outlined above.

12. Senior Management Responsibilities in Relation to ML/TF

Regulatory requirements stress the importance of Senior Management responsibility, and that Senior Managers are ultimately responsible for their Firm's risk management.

The MLRO is responsible for day-to-day management of Financial Crime risk (outlined above). AML and CTF are delegated to the MLRO, however the MLRO has a direct reporting line to the Board. The MLRO also reports and sits on the Risk and Compliance Committee and the Management Committee.

The Firm's Board is ultimately responsible for overseeing the institution's anti-financial crime efforts and ensuring compliance with relevant laws and regulations. Key responsibilities include:

1. Setting the "tone at the top" by fostering a strong culture of compliance throughout the Firm.
2. Approving and overseeing the implementation of anti-financial crime policies, procedures, and controls.
3. Ensuring adequate resources are allocated to financial crime prevention efforts, including staffing, training, and technology.
4. Regularly reviewing and approving the Firm's financial crime risk assessments.
5. Receiving and reviewing financial crime management information.
6. Overseeing the appointment and performance of the Money Laundering Reporting Officer (MLRO) or equivalent.
7. Ensuring proper governance structures are in place, such as a dedicated anti-financial crime committee.
8. Staying informed about financial crime risks, regulatory expectations, and industry best practices through regular training and briefings.
9. Promoting collaboration between different departments to enhance financial crime prevention efforts.
10. Demonstrating active engagement and scrutiny around the effectiveness of the Firm's financial crime controls.

This is actioned at SkyPay with the following specific actions:

1. Considering at Board / Risk Committee meetings the content of any reports (including the MLRO annual report) received in respect of matters relating to financial crime, including ML and TF, and taking the necessary action to remedy any deficiencies identified in a timely manner.
2. All PEP relationships will be reviewed by the MLRO, The Risk and Compliance Committee and Board. All PEP relationships need the approval of the MLRO, Director of Compliance and the board (refer to PEP policy for further guidance).
3. All new Agent relationships will be reviewed by the MLRO, The Risk and Compliance Committee and Board. All new Agent relationships will require the approval of the MLRO, Head of Compliance and the board (refer to Agent Onboarding Procedure for further guidance).

13. Policies and Procedures

The relevant legislation sets out requirements for SkyPay to establish and maintain appropriate and risk sensitive policies and procedures relating to:

- Customer due diligence;
- Reporting;
- Record keeping;
- Internal control;
- Risk assessment and management;
- Monitoring and management of compliance; and
- Internal communication of such policies and procedures with employees in relation to ML / TF prevention.

These requirements are met by the policy standards outlined in this document and procedures which operationalise these standards.

These policies and procedures ensure:

- Scrutiny of complex or unusually large transactions;
- Scrutiny of unusual patterns of transactions which have no apparent economic or visible lawful purpose;
- Identification of any other activity which may indicate related to money laundering or terrorist financing;
- The additional measures that will be taken to prevent the use of products and transactions that favour anonymity for money laundering or terrorist financing are specified;
- Appropriate measures are taken towards a client that is a politically exposed person
- (PEP), or a target of financial sanctions;
- An individual is nominated to receive suspicious activity reports;
- Employees understand their obligations to report suspicious activity and how to do this; and
- Ensure the Nominated Officer receives and considers such internal reports in the light of available information and determines whether there are grounds to file an external suspicious activity report.

14. Systems and Controls - Effectiveness Assessment Process

The effectiveness of the systems and controls is implemented by:

- Policies and procedures reflect current legal and regulatory developments and requirements;
- Compliance monitoring with a clear quality control/internal review process and timely follow up actions;
- Monitoring of outsourced compliance arrangements;
- Adequate resource is available to operate appropriate controls;
- Adequately trained employees, who are up to date with current developments;
- Management information made available to senior management and those with supervisory responsibilities (e.g. Management Committee); and
- Third party external audits (internal audit once appropriate and function is formed).

The MLRO coordinates the Financial Crime Compliance Monitoring Plan. This will generate critical management information and will be a key control in determining the effectiveness of the Firm's Compliance framework. The CMP will be reported to the Risk and Compliance Committee and Management Committee. Key aspects, where necessary will also be presented to the board, separately from the Annual MLRO report.

15. Customer Due Diligence (CDD)

The client onboarding and due diligence processes are key to the Firm's financial crime compliance programme. In all cases, SkyPay and its agents must apply CDD before establishing a business relationship, or prior to carrying out an occasional transaction. CDD is key to ensuring that the Firm:

- Can easily identify higher risk clients such as PEPs;
- Does not violate government sanctions by providing services or products to sanctioned individuals and entities, or those who are owned or controlled by them;
- Applies appropriate level of caution when dealing with PEPS or RCA.

15.1 Corporates

Where SkyPay or its agents on-board a legal entity, we must ensure we completely understand the full ownership and control structure of that legal person, trust, company, foundation or legal arrangement. Therefore, the key minimum elements to identify a corporate customer are as follows:

- Trading / registered name;
- Registration number;
- Address of its registered office and if different, its principal place of business;

- Full names of its board of directors or members of the equivalent management body, or any individual(s) who otherwise exercise control over the management of the company;
- Authorised signatories;
- The law to which it is subject to; and
- Its legal and ultimate beneficial owners (UBOs) – owning or controlling 25% or more (10% for high-risk customers).

The onboarding process is maintained in the Onboarding Procedure; this includes acceptable sources for the above data and should be reviewed by all relevant employees. In summary, prior to establishing a relationship, prospective clients are reviewed through an onboarding registration process. Client information collection and verification apply to the client, the client business itself, the beneficial owners and individuals who exercise control over the client business, including directors.

15.2 Nature and purpose

In addition to identifying and verifying a customer, SkyPay and its agents are required to understand the purpose and intended nature of the business relationship with our customers. This must be collected at the outset of the business relationship.

15.3 Simplified Due Diligence

SkyPay does not rely on simplified to onboard clients. However, it may leverage a client's listed or regulated status to apply a simplified process to verifying beneficial ownership data.

16. Enhanced Due Diligence (EDD)

At a minimum EDD must be applied to the following types of clients:

- PEP with high-risk characteristics (see the Sanctions / PEP procedure for more details);
- Client or director UBO is established in a high-risk third-country3;
- In the case where correspondent-like services are provided; and
- In cases where SkyPay doubts the veracity of the due diligence documents provided by the client.

In addition to this, clients indicated as high-risk by the SkyPay customer risk assessment (which considers customer, product, geography and delivery channel risk) must undergo EDD.

17. Politically Exposed Persons (PEPs), Relatives and Close Associates (RCA)

PEPs and RCAs may represent an increased risk to the Firm and enhanced measures must be deployed in if links to them are discovered during onboarding or during the course of the business relationship. The nature and intensity of these measures are determined by the nature of the PEP or RCA.

PEPs are persons that are entrusted with prominent public functions, whether in the UK or abroad. International standards recognise that a PEP may be in a position to abuse their public office for private gain, and a PEP may use the financial system to launder the proceeds of this abuse of office. Following the FCA PEP guidance, SkyPay will consider a PEP as any individual covered by any of the following definitions:

- Heads of state, heads of government, ministers and deputy or assistant ministers;
- Members of parliaments or similar legislative bodies; including regional governments in federalised systems and devolved administrations, including the Scottish Executive and Welsh Assembly, where such bodies have some form of executive decision-making powers. It does not include local government in the UK but it may, where higher risks are assessed, be appropriate to do so in other countries.
- Members of the governing bodies of political parties – the FCA has defined that this only applies to political parties who have some representation in a national or supranational Parliament or similar legislative body as defined above. The extent of who should be considered a member of a governing body of a political party will vary according to the constitution of the parties but will generally only apply to the national governing bodies where a member has significant executive power (e.g. over the selection of candidates or distribution of significant party funds).
- Members of supreme courts, of constitutional courts or other high-level judicial bodies whose decisions are not generally subject to appeal, except in exceptional circumstances; in the UK this means only judges of the Supreme Court; firms should not treat any other member of the judiciary as a PEP and only apply EDD measures where they have assessed additional risks
- Members of courts, of auditors or of the boards of central banks;
- Ambassadors, charges d'affaires and high-ranking officers in the armed forces (other than in respect of relevant positions at Community and international level such as Permanent Secretary/Deputy Permanent Secretary level, or hold the equivalent military rank (e.g. Vice Admiral, Lieutenant General, Air Marshal or senior);
- Members of administrative, management or supervisory boards of State-owned enterprises;

- Chief, directors, deputy directors and members of the board or equivalent function of an international organisation;
- Directors, deputy directors and members of the board or equivalent function of an international organisation; and
- Non-executive board members of central government boards in the UK should not be treated as PEPs unless they already meet the definition of a PEP in respect of another capacity (e.g. a Member of the House of Lords).

Relatives and close associates of PEPs carry the same risks as the PEPs themselves and accordingly are treated the same. The definition of relative or close associate includes:

- A spouse, or civil partner a partner (including a person who is considered by his national law as equivalent to a spouse);
- children and their spouses civil partners;
- Parents;
- Any individual who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with a person who is a PEP; and
- Any individual who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of a person who is a PEP.

Domestic PEPs should be treated as lower risk compared to non-domestic PEPs, as long as no other adverse risk factors are present. In general, a lower intensity level of enhanced due diligence is applied to domestic PEPs, their family members, and known close associates compared to their international equivalents.

All clients and linked persons (e.g. shareholders & directors) must be screened at onboarding. The screening process must be conducted again during periodic Know Your Customer (KYC) refreshes.

The lists the Firm uses for PEP Screening are aligned to the industry standards and are provided by Dow Jones, which is used as a feed for both our onboarding and Transaction monitoring platforms (Passfort and Napier). Accordingly, the Risk Rating for PEPs (or companies with PEP) links will be dependent on whether the PEP is a UK PEP (Domestic) and their RCAs if no enhanced risk factors are present a decrease in risk level will be considered but this will be at the discretion of the MLRO. Any measures deployed towards PEPs / RCAs must be done in a fair, proportional, objective and non-discriminatory manner.

SKYPAY is also required to apply the application level of CDD/EDD to a known PEP or RCA depending on the PEP risk-level. Calibration of the PEP risk level must consider the following factors:

- Product-Related Factors:
  - The product or relationship they are seeking is capable of being misused to launder the proceeds of large-scale corruption.

- Geographical Factors:
  - High levels of corruption;
  - Political instability;
  - Weak state institutions;
  - Weak anti-money laundering defenses;
  - Armed conflict;
  - Non-democratic forms of government:
  - Widespread organized criminality:
  - A political economy dominated by a small number of people/entities with close links to the state;
  - Lack of a free press and constraints on journalistic investigation:
  - A criminal justice system vulnerable to political interference;
  - Lack of expertise in book-keeping, accountancy, and audit, particularly in the public sector;
  - Laws and culture antagonistic to whistleblowers;
  - Weak transparency in ownership registries for companies, land, and equities; and
  - Human rights abuses.

- Personal and Professional Factors:
  - Personal wealth or lifestyle inconsistent with known legitimate sources of income or wealth;
  - Credible allegations of financial misconduct (e.g., facilitation, making, or accepting bribes);
  - Responsibility for, or ability to influence, large public procurement exercises, particularly where procurement is not subject to competitive tender or lacks transparency; and
  - Responsibility for, or ability to influence, allocation of scarce government licenses such as mineral extraction concessions or permission for significant construction projects.

Each parameter must be verified and considered carefully. SKYPAY is additionally required to follow a balanced approach with the need for good customer treatment starting at account

opening and throughout the relationship. Please refer to the Sanctions/PEPs & Onboarding procedures for the specific processes the Firm undertakes in relation to PEP relationships.

As per section 12, all PEP relationships will be reviewed by the MLRO, The Risk and Compliance Committee and Board. All PEP relationships need the approval of the MLRO, Director of Compliance and the board (refer to PEP policy for further guidance). All PEP relationships must be recorded on the Firm PEP register.

18. Agents / White label clients

SkyPay services agents. All agents must be registered with the FCA prior to going live. SkyPay is responsible for the actions or omissions of its agents, to the same extent as SkyPay or its own employees. Agents are not only customers but also form part of SkyPay 's business model; they carry out regulated activities on the firm's behalf.

The firm also has White Label clients, which need to be treated similarly to agents, however the key difference is that white label clients do not need to be registered as an agent or distributor with the FCA, or European Regulator. For white label partners SkyPay is required to ensure that the partner is regulated locally under equivalent requirements, where required in their domestic law, when providing regulated products or services.

Both agents and white label clients must undergo extensive and specialist onboarding and monitoring steps. Please see the agent and white-label Onboarding Procedure and Agent Oversight Procedure for more details.

19. Sanctions

The Firm must implement procedures to ensure that the prohibitions on dealing with sanctioned persons are adhered to. The prohibition applies to persons on the following sanctions lists:

- US Treasury Department's sanction lists issued through its Office of Foreign Assets Control (OFAC;
- HM Treasury Consolidated List of Designated Individuals;
- UN Security Council Committees lists of embargoes and asset freezes; and
- EU Consolidated lists of persons, groups and entities subject to EU financial sanctions.

SKYPAY is prohibited to:

- Deal with the frozen funds or economic resources, belonging to or owned, held or controlled by a designated person;
- Make funds or economic resources available, directly or indirectly, to, or for the benefit of, a designated person;
- Otherwise engaging in activities prohibited by applicable sanctions; and
- Engaging in actions that, directly or indirectly, circumvent the financial sanctions
- prohibitions.

19.1 Onboarding / ongoing screening

All clients and linked persons must be screened against relevant sanctions lists at onboarding and then screened on a daily basis. This check is conducted through our data provider Dow Jones, which is integrated with Passfort and screens against the relevant sanctions lists detailed above.

SkyPay Limited will not enter into a business relationship with any entity with which it is prohibited by applicable sanctions. If an investigation demonstrates the client is a true match for a sanctioned person or entity, then the match will be reported to the MLRO, who must then determine if any pending transactions should be frozen, whether further restrictions should be applied to prevent future transactions, and if the client should be off- boarded.

If any activity is identified that involves entities, or organisations listed on the UK Consolidated List of Financial Sanctions Targets, the Firm will promptly file a report with the Office of Financial Sanctions Implementation (OFSI) in accordance with its statutory reporting obligations. This ensures compliance with UK financial sanctions laws and supports the prevention of unlawful financial activities.

Please refer to the Sanctions/PEPs policy and procedures document for the specific processes the Firm undertakes with regard to sanctions.

19.2 Payment screening

All payments both inbound and outbound payments, are screened for Sanctions matches. This includes beneficiaries and senders of all payments, payment references. Prohibited or sanctioned countries as per the FATF list, OFAC/ US sanctions HM treasury, UN & EU must be detected in this screening. Hits are investigated in accordance with the process detailed in the PEP / Sanctions Procedures. True positives that involve individuals, entities, or organisations listed on the UK Consolidated List of Financial Sanctions Targets must be reported to OFSI.

19.3 System calibration

The MLRO/Deputy MLRO tests the existing sanctions screening system on its "fuzzy logic". If a close match known PEPs or sanctioned individuals and entities are undetected by the system during testing, then the MLRO will either secure documented improvements from the supplier or switch to another provider or arrange for internal provisions to verify the identity of the individual in question.

20. Suspicious Activity Reports (SARs)

SkyPay Limited will report to the relevant investigative authorities (this will be the National Crime Agency (NCA) in most cases) when it knows, suspects or has reasonable grounds for knowing or suspecting that a person (private or legal) is engaged in, or attempting money laundering or terrorist financing. The report is known as a Suspicious Activity Report (SAR).

The scope of what money laundering entails is wide, and any predicate offence (a crime) linked to a transaction or client is reportable. SkyPay and all employees are required to report any suspicious activity, which includes fraud, tax crime/evasion, Bribery and corruption, or any illegal activity to the MLRO.

SkyPay Limited will report to the relevant investigative authorities (this will be the Office of Foreign Asset Control in most cases) when it knows, suspects or has reasonable grounds for knowing or suspecting that a person (private or legal) is engaged is a designated person or has breached a prohibition or failed to comply with an obligation under specified provisions of the UK sanctions regulations.

It is a Policy of SkyPay Limited that all employees will remain alert signals of ML, TF, SE and PF and will immediately report if there are grounds to do so, using the channels described in the SAR Procedure.

The Nominated Officer will acknowledge receipt of the report and provide feedback, as is appropriate to do so. The Nominated Officer will review the SAR and If it is determined that there is knowledge, suspicion or reasonable belief that another person is engaged in money laundering or terrorist financing, an external SAR must be made to the NCA as soon as it is practicable to do so. This applies with retrospective suspicions (i.e. if the transaction has actually taken place).

A record of any employee exchanges around reporting suspicious activity will be kept as evidence of the decision-making process to report or not report based on their assessment of the information and if they determine it gives rise to knowledge or suspicion of Money Laundering or Terrorist Financing.

All SARs are required to be stored on the designated log, the compliance team of SKYPAY are required to keep the log update and include all information relating to the notification and investigation of disclosures. The log must also include all justification for reporting/non reporting of SARS. SKYPAY is required to adhere to data retention requirements, all data on the SAR Log will be required to be retained for a minimum period of 5 years. Please refer to the Data Retention Policy for full guidance.

20.1 Tipping off

It is a criminal offence for anyone in the regulated sector, following a disclosure to a nominated officer or to the appropriate agency, to do or say anything that might either "tip off" another person that a disclosure (i.e. internal / external SAR) has been made or prejudice an investigation.

SkyPay will, as part of its employee training, make certain all employees are aware of the requirement to submit suspicious activity reports where they have grounds to suspect money laundering and that they must not do or say anything to anyone about that report and its contents, without the consent of the Nominated Officer.

Care must be taken when speaking to a client whose account is so marked. Advice must be sought from the 2LoD prior to engaging with such a client.

20.2 Defence Against Money Laundering (DAML)

When suspicions relate to funds that are held at the Firm, the funds must remain on hold pending the submission of a DAML SAR. The funds must remain on hold until the Firm receives explicit or presumed consent from the NCA regarding the funds subject to suspicion. If such funds are transferred prior to receiving consent, the Firm risks committing a principal money laundering offences under the Proceeds of Crime Act 2002 (POCA). See section 9.4 of the SAR Procedure for more details.

20.3 Further Action

The MLRO will coordinate any further actions (e.g. restraint of funds, client offboarding) required as a result of the submission of a SAR.

For further guidance on SkyPay SARs processes, please refer to SARs Procedure.

21. Law Enforcement and Regulatory Requests

The Firm must promptly respond to law enforcement and other regulatory queries. The MLRO will coordinate the response to all such queries relating to financial crime and the Firm must provide all resources and assistance necessary to fulfil the request in timely and complete manner. For more details of the procedure around law enforcement request, refer to the DPA Procedure.

22. Transaction Monitoring

SkyPay has the regulatory obligation to mitigate the risk of financial crime to the business. In order to fulfil this requirement, the Firm must have in place a Transaction Monitoring framework that will allow all employees to ensure that they monitor client activity appropriately and report any suspicious activity they may come across. For more detailed guidance on the Firm's approach to Transaction Monitoring, refer to the Transaction Monitoring Procedure document.

The key requirements of SkyPay 's monitoring framework are that all relevant employees will ensure they monitor and flag activity that may indicate ML or TF. Specifically, the system must identify and flag:

- Complex or unusually large transactions;
- Any unusual, or unusual pattern, of transactions;
- Transactions which have no apparent economic or legal purpose; and
- Any activity which an employee believes is related to money laundering or terrorist financing (take into account known typologies and industry typologies shared at industry meetings e.g., Electronic Money Association typologies).

SkyPay Limited has determined that its business activities require an automated transaction monitoring system (Napier) to examine transaction patterns to detect suspicious activity.

The key requirements for such a monitoring system are as follows:

- It flags up transactions and/or activities for further examination.
- These transactions are reviewed promptly by the right person(s); and
- Appropriate action is taken on the findings of any review, including SAR filing if there are grounds to do so.

Automated transaction monitoring is conducted:

- In real time, if those transactions and/or activities can be reviewed as they take place or are about to take place; or
- Post the event, through independent review of the transactions and/or activities that a client has undertaken.

SkyPay employees are also required and trained to detect and report suspicious client activity that may not have been identified by the rules.

To manage the risk of this occurring, the SkyPay and its agents must subject all transactions for review on a regular basis to determine if these transactions are in keeping with a client's risk profile. The Napier system used by SkyPay will assign a risk score to each transaction, based on the following information:

- Higher than average Transaction Value;
- The total historical transactional average of a client will be assessed;
- Where a transaction exceeds the client's typical behaviours, these transactions will receive additional weighting;
- Frequency/Value;
- Unusual activities in the transfers between clients;
- Jurisdictions to which funds are sent to or being withdrawn from; and
- Sanctions, PEPs or Adverse media flags.

During the onboarding stage, information is collected from each corporate client regarding the estimated frequency and value of their transactions. This will be compared on a monthly basis to the number of transactions carried out by the client. An ongoing record of the number of transactions carried out by each client will also take place, with reviews being conducted on those accounts which exceed this average or have a substantial increase in the averages over time.

22.1 Monitoring Process

SkyPay Limited employees are trained to look for signs of out of the ordinary and/or suspicious transactions and if detected to immediately make an internal SAR to the Nominated Officer. Such reviews will take place by employees responsible for processing transactions and as such, where an outlier or unusual activity is found, this will be highlighted before the transaction is processed.

SkyPay has implemented a procedure which is commensurate with the size and complexity of the business and the volume of client transactions. The Firm has calibrated its transaction monitoring software, Napier, to pay particularly close attention activity that might indicate financial crime. The rules encompass many elements of data points and risk; rules can be

based on single-transactions or multi-transaction rule scenarios (a payment over a certain threshold has been breached) or (multiple transactions over a certain amount have been made in a specified time). Please see below some examples of data variables used assign an alert level (1-5):

- Volume /Value / Velocity
- Country of beneficiary
- Reference check of payment
- Beneficiary Bank Score.
- PEP Sanction Check
- Adverse Media

The alert level defines the level of intervention and overview require to investigate the alert.

For further guidance on the transaction monitoring framework, please refer to the SKYPAY Transaction Monitoring Procedure.

22.2 Client Profile

The Firm's business model enables employees to develop a detailed profile of each client, which directly feeds into type and frequency of transaction monitoring that the Firm undertakes. The client risk profile forms the basis for the level of ongoing monitoring that the Firm will carry out.

22.3 Effectiveness

The MLRO will ensure that any transaction monitoring system deployed is monitored for its effectiveness and calibrated accordingly based on that assessment. The effectiveness will be assessed and reported in the MLRO regular reporting (quarterly and annual MLRO report to the board).

The transaction monitoring system must be continuously calibrated to ensure it identifies and flags behaviour indicative of ML / TF. In order to ensure this outcome, the firm conducts an annual review of transaction monitoring systems to ensure that scenarios remain appropriate to the risks the firm faces and that thresholds remain effective for preventing and detecting financial crime. This process also includes a review to ensure that necessary payments data is being correctly transmitted and ingested by the transaction monitoring platform.

22.4 High-risk clients

All high-risk clients will undergo enhanced monitoring of transactions and enhanced monitoring at the onboarding stage and continued monitoring throughout the client relationship with SKYPAY .

TM Rules will trigger which encompass the client risk profile, high-risk clients will be subject to more scrutiny in respect of transaction if the client is classified as high-risk as they pose a greater risk of financial crime.

23. KYC refresh and Periodic Reviews

The Firm must conduct periodic reviews and refresh client KYC. The cadence of these reviews depends on the risk level of the client. These should serve to uncover risks and aspects with the relationship that were not present at onboarding review and have developed during the course of the business relationship.

Periods between periodic reviews occur according to risk level with higher risk clients being reviewed on a more regular basis:

- High risk customers: Annually;
- Medium risk customers: Two years; and
- Low risk customers: Three years.

In addition, SkyPay and its agents must review customer files upon the following trigger events:

- Confirmed adverse media hit;
- Confirmed PEP or sanctions list hit;
- Material changes in corporate structure;
- Sudden and unexplained change in jurisdiction, i.e., funds suddenly being sent to a high-risk jurisdiction; and
- Submission of an internal SAR, only once it has been confirmed by the MLRO to be suspicious.

At a minimum, the review will obtain up to date documents and risk indicator information as well as refreshing sanctions, PEP and adverse media screening. For more details refer to the Onboarding and Sanctions / PEP Procedures.

24. Training and Awareness

SkyPay considers learning and development in the field of anti-money laundering and anti-terrorist financing an important pillar for an adequate and effective transaction monitoring process. Therefore, SkyPay has established a training program for all levels of employees; from the board and senior management to junior employees.

SkyPay Limited is committed to ensuring that all relevant employees receive training for them to fulfil their roles. All employees are to be within one month of starting employment and then annually. Following training a test will be given of the material covered to ensure all employees are up to date with SkyPay AML/CTF processes. The content of the training will revolve around the Firm's AML and CTF obligations.

Records will be kept of attendance, test results and any remedial actions taken to ensure employees have the level of understanding required to fulfil their roles, in the form of a training log. SkyPay provides its training through the Talent MS platform. Training is delivered via a automated test with the pass mark required to pass the test being 80%, if a client fails the

test they are allowed to retake the test an additional two attempts before been given mandatory further training.

SkyPay Limited also engages an external training provider to train employees. The provider and training materials are reviewed annually by the MLRO for their effectiveness and appropriateness. Any issues or gaps that are identified with regards to the training regime are to be immediately brought to the attention of senior management for remediation.

Employees that fulfil specialised compliance functions as part of their day-to-day role are to be provided with targeted training from delivered by both internal and external trainers. Training is assigned using the risk-based approach with employees carrying AML operations and client- facing roles seen as highest priority recipients of targeted training.

Where appropriate, SkyPay may take steps to ensure that relevant contractors, subsidiaries, outsourced third parties and agents receive this targeted training. Compliance provide these employees with bespoke departmental workshops to provide specific guidance on areas relevant to employee's day to day operational activities.

All employees will be provided with all policy and procedures in relation to core compliance areas, which includes Financial Crime. The policy is readily available to each employee in the Bamboo HR (Employee Management), additionally the Policies & Procedures are available in

shared drive. Employees will be required to read and confirm they fully understand and accept the policy and processes they are subject to.

25. Record Keeping

All documents requested by the Firm to identify or verify individuals and entities are collected electronically. The digital CDD documentation is then stored for a period of at least five years from the end of the business relationship or occasional transaction.

The platform automatically saves records of transactions which are accessible only by authorised employees whose access of the records are in turn logged and kept on the system.

A periodic review of record keeping, and compliance procedures will be conducted by the MLRO, and the findings will be included within the MLRO annual report to the Board.

The MLRO will ensure that the following information is stored securely and electronically:

- Transaction data;
- CDD information;
- Internal and external suspicion reports;
- MLRO annual (and other) reports;
- Training records;
- Compliance monitoring records; and
- Information about the effectiveness of training.

All internal compliance records will be stored electronically for a period of at least 5 years. The MLRO has responsibility for ensuring that client records are then treated according to The Firm's data security policies.

The MLRO will ensure that a rationale is documented for any additional due diligence measures it has undertaken (or any it has waived) compared to its standard approach, in view of its risk assessment of a particular client.

For further guidance, please refer to the Record Keeping Policy and Procedures documents.

26. Horizon Scanning

The Compliance Team are responsible for ensuring the following:

- Adequate regulatory horizon scanning is conducted;
- Emerging risks and trends relevant to the business are monitored and reported and where required built into the Firm's risk profile and assessments. In addition, policy is adapted to manage those risks where needed; and
- Ensuring actions resulting from horizon scanning are appropriately actioned internally.

The compliance team maintains a horizon scanning tracker within internal management information to ensure these goals are achieved.

The MLRO must keep up to date with international findings in relation to countries, jurisdictions and risks that require policies and processes to be updated. This will be factored into the Horizon Scanning process. Specifically, the MLRO must:

- Must ensure the Firm obtains and utilises any information reported from a reputable body (e.g. HM Treasury, FATF, IMF, OECD. Transparency International) when updating policy and procedure related to financial crime compliance;
- Consider jurisdictional and country risk reports along with the national risk assessment in the UK;
- Ensure that the jurisdiction risk assessment accounts for the UK High Risk Third Country list4;
- Implement mechanisms to assess ML and TF risk of countries via a variety of sources. These sources may include a variety of the following:
    - HM Treasury Sanctions5
    - UN and EU Sanctions
    - FATF high-risk and non-cooperative jurisdictions6
    - FATF Mutual Evaluation Reports (see FATF website)
    - Transparency International Corruption Perceptions Index7
    - FCO Human Rights Report8
    - UK Trade and Investment overseas country risk pages9
    - Quality of regulation NCA Intelligence reports

- Consider reports relating to products and services, along with other sources outlining best practice such as the Wolfsberg Group.
- Ensure that business relations and transactions with individuals and Firms – whether direct or through correspondents - located in higher risk jurisdictions, or jurisdictions against which the UK has outstanding advisory notices, will be considered when assessing risk.

- Ensure that the Acceptance Policy is adopted and followed across the business, and where there are deviations from policy those must be clearly documented, reviewed and approved by SkyPay senior management and the board.

27. Business Model Alterations

Where there is a change to the business model (from SkyPay or an agent perspective) the change request process must be triggered (outlined in the management and board committee governance document and Terms of Reference). The request must also include a clear explanation of how the change meets the UK regulatory requirements for SkyPay , and where applicable further legal advice should be sought to confirm this.

Part of any new product, service, client and market that alters the business MUST be first reviewed by the Head of Regulatory Compliance and the MLRO. This is built into the management review process and requires a formal proposal to be reviewed and considered by all departments, including the MLRO.

The introduction of any new business offerings or products would need to be introduced in the BPOC (Business Proposal to add additional Products/Service) where all SMEs and stakeholders would sign off on product development before it goes in deployment. All new products are required to receive written sign off from the MLRO of the SKYPAY before the product goes live to ensure all oversight is in place.

29. Outsourcing and Third Parties

All activities performed on behalf of SkyPay must meet SkyPay policy requirements or an approved change alteration that meets UK standards. All outsourcing or use of third parties need to undergo an outsourcing assessment. This assessment is conducted by the Legal team and is captured by the Outsourcing Policy. In addition to this, the MLRO is accountable for ensuring all agents and third parties meet the required AML standards of the UK.

SkyPay policies and procedures are required to be adopted by any third party acting on our behalf. This is then monitored via the Compliance Monitoring Plan, testing and regular monitoring of the third parties.

All outsourcing must be reviewed and approved by the Firm's legal department and where it is determined that there is outsourcing (e.g. any aspect of the CDD or AML processes). Subsequently, this must be approved by management and a notification provided to Compliance to notify the FCA of such significant outsourcing. All outsourcing of compliance

related areas is subject to the Compliance Monitoring plan (CMP). Where the CMP reveals deficiencies or ongoing and repeated failures or issues on effectiveness the following action may be taken, depending on the severity of the issues identified:

- A third-party audit may be commissioned by the SkyPay Head of Regulatory Compliance and the MLRO, and a remediation exercise required (the agent or third party may temporarily be suspended until audit and/or remediation is complete);
- Termination of business relationship (based on CMP review or audit results);
- Suspension of business relationship (based on CMP review or audit results); or
- Continuance with conditions.

All agents and third parties MUST follow the SkyPay ’s onboarding policies and procedures. Where they wish to deviate then as per any policy change a change request would be required as set out above, and as per the governance process the Firm has deployed.

Where operational activities are outsourced to a third party or agent, they MUST have an appointed compliance officer and MLRO who is responsible for addressing compliance and financial crime risks in their business. This function must ensure SAR”s and other required regulatory reports are submitted, in collaboration with the SKYPAY MLRO who will also investigate and report accordingly as per their legal obligations.

Where a third party (e.g. a subsidiary) is required to comply with local legal or regulatory requirements that are different to the UK, the third party must meet the UK requirements as a minimum standard. Where the rules and requirements are stricter than UK requirements and are in essence stricter, then these must be adopted, however this must be made clear in any change request submitted to the SkyPay MLRO by the subsidiary or third party’s MLRO.

All outsourcing and change requests require the SkyPay MLRO to conduct a financial crime risk assessment. Where the risks (geographic, business, delivery etc) indicate a lower standard may be present, this must be documented and reviewed and approved by senior management.

28. Waiver (Change / Exception Request)

Where an agent or third party or SKYPAY itself wishes to deviate from the SKYPAY policy a change request (Wavier) needs to be submitted by the prospective risk owner to the Risk & Compliance Committee (if for an Agent by their MLRO). The change request must outline how the variation requested meets UK regulatory requirements (see Business Model Alterations). A SkyPay ’s Head of Regulatory Compliance and MLRO will review along with

the management committee. For the full policy and procedures on waivers please refer to the Exception Request Policy.

29. Employee Screening

SkyPay Limited requires that all key employees undergo screening. Those that are identified as key are as follows:

- Beneficial owners of the Firm;
- Directors of the Firm;
- Managers responsible for delivery of payment services(C - Level and Heads of Department); and
- 1LoD / 2LoD deploying AML controls (e.g. relationship managers on the 1st line, agents and their employees that deploy controls on our behalf etc.).

The screening conducted meets the FCA fit and proper test requirements and the JMLSG guidance on screening of AML employees. SkyPay has a specific screening policy and process that is managed by the Head of Compliance and HR. The checks are performed by a third party and HR receives reports and reviews. The reports ensure that key compliance and AML employees, as well as others, are checked with regards to their skills, knowledge and expertise and the integrity of the individual. SKYPAY has appointed screening partner CBS to conduct screening on its behalf.

Refer to the Recruitment Procedure document under Screening Applicants section for further guidance.

30. Vendor Configurations and Oversight

All AML software vendor system parameters and configurations and any changes must be reviewed and approved by the SkyPay MLRO prior to the relationship being commenced. This includes any changes requested by the agent or a subsidiary. No changes,

in relation to SkyPay regulated activity, or areas SkyPay is held responsible or accountable, can be changed or modified without review and approval by the SkyPay MLRO and Board of Directors, where the board are required to approve (e.g. substantial policy changes).

The Firm has established a procedure to conduct specialist annual checks and suitability reviews on AML software vendors which goes beyond those specified in the Outsourcing Policy. The following is checked:

- What databases does the system screens against? Down Jones Sanctions PEPS & Adverse Media checks;
- How up to date is the database that the provider uses;
- How often is the data refreshed and when it was last refreshed;
- Processes for updating the data (is it done internally or externally) from the service provider;
- How are updates recorded and what reports are produced on this;

The Firm must he software provider at the beginning of the relationship before it enters into an agreement with the vendor.

The SkyPay MLRO will be the main point of contact for all vendors and must be involved in any standard setting with vendors. These systems cannot be changed without consultation and approval by the SkyPay MLRO, and these must then be captured in policy and the context captured (emails, meetings and rationale supporting the settings/parameter change/modification or setup) and archived for audit purposes.

For change in vendors in relation to Financial Crime systems and controls that SKYPAY is responsible for (own activity, agents etc) this will need an assessment conducted and full review by the SKYPAY MLRO. This must then be reviewed and approved by the board, based on the MLRO's assessment and recommendations. Please see the SkyPay onboarding Manual and Appendix for more details.

30. Document Review and Version Control

This document is reviewed at least once every 12 months and this checked via the Compliance Monitoring Program. It will also be reviewed in the event that SkyPay Limited becomes aware of any significant or material changes to the regulatory environment that would call for additional review.

Version	Author	Issue Date	Version Details
1	Yerkebulan Torekhan	March 2025	Initial