Anti-Money Laundering, Counter Terrorist Financing, Counter-Proliferation Financing and Sanctions Policy

Tier 1 Policy

- Version: 3.1
- Updated: December 2025
- This is a Conduct and Regulatory Risk policy

Policy Governance	
Policy Owner	Compliance Director and MLRO
Executive Owner	Chief Risk Officer
Approver	Board
Date of Approval	December 2025
Version	3.1
Date Effective	December 2025
Related Policies and Procedures	**Associated Policies and Frameworks:** • Anti-bribery and Corruption Policy • Fraud Policy • Failure to Prevent Facilitation of Tax Evasion Policy • Procurement Policy • Third Party Risk Management Policy • People Policy • Senior Managers & Certification Regime Policy • Data Protection Policy • CEL AML Policy • Risk Management and Internal Control Framework • Policy Governance Framework • Moneybarn Broker Oversight Framework **Associated Standards and Procedures:** • Customer Due Diligence Manual • Surveillance Manual • Regulatory Obligations Register • Colleague Background Checking Procedure
Accessibility	If you have a disability, require additional support, if English is not your first language or you need help to understand this policy, you should speak with your line manager or People team who will make appropriate arrangements to support you through the process.

Contents

Purpose

This Policy sets out Vanquis Banking Group's ("Vanquis" or the "Group") approach, risk appetite and standards for managing money laundering, terrorist financing, proliferation financing and financial sanctions risk ("Financial Crime risk)". It sets out how the Group will meet their legal and regulatory obligations and to manage and mitigate their Financial Crime risks within risk appetite. These risks may arise from:

- Customer relationships, including all parties associated to the relationship such as authorised users, secondary card holders, nominated users, guarantors and power of attorneys;
- Colleagues;
- Arrangements with parties acting on behalf of the Group in the delivery of their products and services, such as outsourcing partners;
- Other third parties with whom the Group engages for its general commercial operations, such as affiliates, brokers, dealers, and suppliers; and
- Cheque cashing agents or retailers who may be a sole trader, company or partnership firm as set out in the CEL AML Policy separately.

Scope

This Policy applies to Vanquis Banking Group and the legal entities listed below.

1. Vanquis Bank Limited, including the cards and deposits products ("VBL")
2. Moneybarn Limited
3. Moneybarn No.1 Limited
4. Vanquis Banking Group Plc
5. PFG Corporate Services Ltd
6. Cheque exchange Limited ("CEL")
7. Snoop Limited

Cheque Exchange Limited, being a money service business (MSB) is regulated by HMRC and has an independent Money Laundering Reporting Officer ("MLRO"). CEL is governed by its own AML policy, which has been set considering their business model and risk appetite. The CEL MLRO is responsible for ensuring this business complies with the regulatory requirements and industry/government guidance applicable to their business. CEL has its own board and governance framework.

Any reference to Vanquis in this policy would mean reference to all legal entities listed above included in the scope of this policy, except for CEL, unless it has been distinctly mentioned.

Where the term MLRO or Money Laundering Nominated Officer ("MLNO") is used in this Policy, it means the individual(s) registered with the FCA as the SMF17 role holder for each regulated entity.

Legal and Regulatory Requirements

Vanquis has a legal, regulatory, moral and social responsibility to detect and disrupt activities of those who would seek to use Vanquis to facilitate any form of financial crime, including money laundering, terrorist financing, proliferation finance or activities in breach of sanctions. In whatever form it occurs, financial crime influences all parts of the economy. It undermines Vanquis' purpose, principles and objectives and causes harm to our customers and to the wider society. Vanquis requires all colleagues to always act with integrity and within the law. The Group must comply with the Applicable Sanctions as outlined in this Policy (and any applicable in their overseas operations) and must not knowingly establish or maintain a relationship with any individual or entity subject to sanctions.

The regulated entities must ensure that any party acting on their behalf meets all requirements in this Policy. Relevant legislation and regulatory requirements for the purposes of this Policy are encapsulated in:

- The Terrorism Act 2000 (as amended by the Anti-Terrorism Crime and Security Act 2001)
- The Proceeds of Crime Act 2002
- Counter Terrorism Act 2008
- Bribery Act 2010
- Criminal Finances Act 2017
- Sanctions and Anti-Money Laundering Act 2018
- The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017) amended 2019 and 2022.
- Data Protection Act
- EU Regulation 2016/1675
- Scrap Metal Dealers Act 2013

Regulatory expectations and industry standards are contained in:

- FCA SYSC Handbook
- FCA Financial Crime Guide
- FCA Politically Exposed Persons ("PEPs") Guidance
- Joint Money Laundering Steering Group (JMLSG) Guidance
- ESA Guidance
- HMRC Money Service Business guidance (for CEL only)

Key Policy Principles

1. Governance:

Financial Crime Risk Appetite

- Vanquis will operate a strong and risk-proportionate set of systems and controls to detect and prevent financial crime breaches. If they do occur, we will investigate them promptly and learn from control failings, gaps or issues. We will maintain oversight of our business through robust and clearly documented governance and delegation arrangements.
- To monitor financial crime risk against appetite, the Vanquis MLRO must set a range of risk appetite metrics. These must be reported to the Executive and Board Risk Committees where appropriate. The Vanquis MLRO will escalate any other metrics or management information as deemed necessary to ensure management are aware of material risks.
- The Vanquis policy requirement and risk appetite are based on the products and services offered; therefore, the first line of defence is responsible for assessing whether any business change increases or changes financial crime risk and the MLRO must be consulted for advice and guidance at each instance.
- Customers who fall outside of the regulated entity's risk appetite (Appendix 3 and 4) will not be accepted or maintained.

Business-wide financial crime risk assessment

- A business wide financial crime risk assessment ("BWFCRA") must be completed for all entities/products offered by the Group in line with the Money Laundering Regulations (this is in exception to CEL who will need to complete the assessment separately) in line with a documented assessment methodology.
- The BWFCRA must be updated at least annually and presented to the senior management forum having financial crime representation each time there is a material change, or annual review completed and also track any actions identified within the assessment.

MLRO Oversight and Reporting

- The MLRO must submit a formal report to senior management and the Board Risk Committee at least once annually.
- The report must evaluate the effectiveness of Vanquis' AML systems and controls, and include:
  - Recommendations for risk mitigation and control enhancements
  - Prioritisation of key risks and resource requirements

2. Due Diligence: Identification of the customer, colleague or any third party they are dealing with and verify their identity and also screen them against PEPs, Sanctions and Adverse Media. Vanquis has set strict requirements to do this prior to establishing a business relationship.

Customer Due Diligence

- Vanquis must complete due diligence checks prior to entering a business relationship. All CDD process, settings and thresholds set must meet legal and regulatory requirements including Anti-Impersonation Checks in case of non-face to face engagements. CDD requirements must be documented in the Due Diligence manual approved by the MLRO and must comprise of:
  - Identification and verification of the customer and any associated third parties;
  - Obtaining any other information as necessary as set out in the Customer Due Diligence Manual; and
  - Screening: PEPs, Sanctions and Adverse Media.

Identity and Verification

- At onboarding, Vanquis must identify the individual subject to due diligence by obtaining their full name (including middle name where possible), date of birth, and current residential address and verifying the applicant is a true person and they the individual they purporting to be.

PEPs, Sanctions and Adverse Media Screening

- Identifying whether the customer is subject to sanctions, politically exposed or adverse media.
- Where a PEP is identified including their relatives and close associates ("RCA"), they must be subject to enhanced due diligence, including checks on source of wealth, source of funds, and MLRO approval.
- Vanquis is not permitted to enter a relationship with any sanctioned individual who is included on the consolidated list issued by His Majesty's Treasury in the UK ("HMT"), or who are subject to sanctions issued by the Office of Foreign Assets Control ("OFAC") in the USA. Any application considered to be a likely match against an individual on these lists is to be escalated to the MLRO using business procedures, for consideration for reporting to OFSI, and for the application to be declined.
- If a customer matches applicable sanctions at any point, their account must be immediately blocked and terminated once OFSI confirms the match. Additional actions must follow the relevant sanctions regime, as advised by the MLRO. Suspected sanctions breaches must be escalated to the MLRO immediately. If confirmed, the MLRO must notify the Board Risk Committee and report to OFSI.
- It is prohibited to enter business relationships who meet the criteria of a Special Interest Person ("SIPs"); individuals who, due to their previous criminal conduct, may be outside of the VBL or Moneybarn risk appetite (refer Appendix 4 for the risk appetite relating to adverse media/SIP customers). Applicants outside the regulated entity's risk appetite must be declined unless an exception is approved by the MLRO. Financial Crime Operations (or the first line of defence, where applicable) must implement processes to assess applicants and existing customers with adverse media. The regulated entity's MLRO should establish a second-line escalation and decision-making process to determine the appropriate course of action

Third Party Due Diligence and Reliance

- All new third parties with whom Vanquis is to establish a business relationship are required to be subject to due diligence prior to the commencement of any contractual agreement, as set out in the second line supplier due diligence procedure and the Procurement Policy, including any other additional checks that the regulated entity may deem as necessary depending upon the type of relationship, such as brokers or dealers in case of Moneybarn (refer VF Broker Oversight Framework) and agents in case of CEL (refer CEL AML Policy).
- For any entity operating overseas, Vanquis must ensure they are compliant with the local regulations of that country.
- If Vanquis relies on a third party to carry out the customer due diligence, the Group MLRO must implement appropriate oversight measures to satisfy themselves the third party are operating in line with these Policy requirements.

Colleague Due Diligence

- All colleagues should be subject to identification and verification checks before on board and granted access to company systems. This includes screening for PEPs and Sanctions and completing this periodically, on a risk-based approach. Where reliance is placed on third parties to complete these checks on behalf of Vanquis, the owner of the relevant policy/procedure must implement an oversight mechanism to ensure the nature and scope of checks performed are in line with the requirements of this Policy
- The Group must maintain recruitment processes that assess conduct, integrity, competency, skills, knowledge and expertise of candidates prior to employment. A risk-based approach is required for senior roles (e.g. SMF, MRT, SIF under SMCR), with enhanced vetting checks.
- Prior to entering into any contractual relationship, all new third parties must undergo due diligence in line with the Anti-Bribery and Corruption Policy. This includes additional checks based on the nature of the relationship, brokers/dealers (e.g. Moneybarn – refer to VF Broker Oversight Framework), agents (e.g. CEL – refer to CEL AML Policy) and for overseas entities, Vanquis must ensure compliance with local regulations.

3. High Risk Customers and Enhanced Due Diligence: Identifying high-risk customers and applying enhanced due diligence measures.

- Vanquis will use a two-pronged customer risk assessment where customers will be assessed as STANDARD or HIGH.
- A customer relationship will be assessed as STANDARD risk where the customer (and any individual forming part of the customer relationship) has successfully completed identification and verification processes in accordance with this Policy, and no high-risk factors have been identified.
- A customer relationship must be designated as HIGH risk where the customer is a PEP or an RCA of a PEP (as defined in Appendix 3). The MLRO can mandate that any customer is designated as high risk due to the presence of one or more high-risk factors. These high-risk factors may include:

- Conviction of a criminal offence or subject to adverse media, which may not mean the relationship is outside of risk appetite but may warrant enhanced due diligence measures. This may include offences or media, which present a reputational risk to Vanquis.
- Subject to a criminal law enforcement enquiry, which may indicate the customer is involved in illicit activities.
- Links (transactional or otherwise) to jurisdictions outside the UK, which might indicate a permanent or temporary connection to a jurisdiction, which is considered a High-Risk Country, as outlined in Schedule 3ZA of the MLRs.
- Customers residing outside of UK are outside risk appetite and therefore will be exited upon being notified or identified.
- Transactional activity is considered unusual or presents heightened financial crime risk.

- The MLRO of the regulated entity has the authority to:
  - Determine whether a customer should be assessed as HIGH risk.
  - Change a customer's risk rating, including lowering from HIGH to STANDARD or vice versa.
  - Block a customer account to mitigate risk due to suspicious activity being identified or CDD requirements not being completed.
  - Exit a customer relationship should they be deemed outside of risk appetite in line with the risk appetite statement at Appendix 3 and 4.
- Where a customer is assessed as high risk, their details must be added to a register of high-risk customers, alongside the reason for their high-risk designation. This list is maintained by the regulated entity MLRO. The MLRO will determine whether any additional controls, enhanced due diligence or actions are required on a case-by-case basis.
- Enhanced Due Diligence ("EDD") measures must be documented in procedures and processes and should include more frequent and targeted surveillance, with specific requirements to be completed for PEPs and RCAs.
- All high-risk customer relationship must be subject to annual review, approved from the MLRO and documented in line with the procedures set by the MLRO.

4. **Ongoing Monitoring and Transaction Monitoring:** Applying ongoing due diligence measures, including monitoring of their transactions to detect potential suspicious activity.

- Following a business relationship being entered, Vanquis must:
  - Customers must be screened for PEPs and sanctions on a regular basis, with screening conducted at least monthly. Where applicable, EDD measures or exit procedures must be applied in accordance with the requirements set out in the Due Diligence Manual.
  - On a risk-based approach, regularly screen their customers for adverse media. This is not a requirement for customers who only operate Vehicle Finance products.
  - Monitor transactions for identifying potentially suspicious activity.
  - Source of funds or wealth checks where a high-risk customer is identified, transaction is complex, or unusually large, or there is an unusual pattern of transactions, and the transaction or transactions have no apparent economic or legal purpose.

Ongoing Monitoring

- Ongoing monitoring may lead to various outcomes. Customers outside risk appetite must be exited. Additional or updated information, such as income details, activity rationale, or third-party connections, may be requested. Refusal to provide required due diligence information, or submission of false or misleading data, will result in application or relationship termination.
- Financial Crime Operations must maintain processes to collect and assess relevant information as part of their ongoing monitoring obligations. The Group's surveillance approach must be formally documented in a Level 2 Surveillance Manual, outlining both the overarching methodology and the calibration of surveillance tools. The Group MLRO will issue guidance specifying when sources of funds and wealth checks are required, including mandatory and discretionary scenarios for verification.

Transaction Monitoring

- Vanquis must operate transaction monitoring which is designed to identify potentially suspicious activity that is indicative of possible money laundering and / or terrorist financing, for investigation. The following requirements apply to transaction monitoring:
  - The monitoring must be conducted through an automated transaction monitoring system where applicable.
  - The monitoring approach must use rules, which are established based on the risks and threats identified within the BWFCRA for that regulated entity.
  - All rules, thresholds and settings used to monitor transactions must be documented alongside the rationale as to why they are appropriate for managing the risk. This must be approved by the Group MLRO.
  - Rules, thresholds and settings must be reviewed at least annually to ensure ongoing appropriateness. This review must be documented and follow the updating of the BWFCRA for that regulated entity.

Suspicious Activity Reports (SARs)

- All colleagues must report any suspicion or knowledge of money laundering or terrorist financing to the Money Laundering Nominated Officer (MLNO). The Group MLRO acts as MLNO for all Regulated Entities except CEL. Failure to report is a criminal offence, punishable by up to five years' imprisonment and/or an unlimited fine.
- MLNOs must ensure systems are in place so that colleagues:
  - Recognise indicators of suspicious activity.
  - Know who the MLNO and MLRO are.
  - Can report suspicions promptly.
  - Understand how to report in line with requirements.
- Upon receiving an internal suspicious activity report (ISAR), the MLNO decides whether to submit a suspicious activity report (SAR) to the National Crime Agency (NCA), including any Defense Against Money Laundering (DAML) SARs.
- MLNOs may delegate ISAR receipt to a competent individual/team, with formal documentation, oversight, and annual review. Accountability remains with the MLNO.

5. **Training:** Vanquis provides training on the money laundering, sanctions, proliferation and terrorist financing regulatory requirements and their personal obligation to identify and report suspicious activities.
• All Applicable Colleagues must complete annual Financial Crime training in line with the Training Policy. Training may be required more frequently if there are significant changes to risk profile, operations, products, or regulations. New joiners must complete the training as part of their onboarding. • The MLRO is responsible for the training content, which must cover relevant laws and regulations, personal obligations and consequences of non-compliance, identity and contact details of the MLRO and MLNO, red flags and suspicious activity indicators and reporting procedures for suspicious activity. • The MLRO monitors the completion of the training and event of delay could lead to colleague's system access removal leading to further actions following the Group's disciplinary procedures. • The MLRO may also determine specific roles or individuals who have heightened financial crime risk exposure and require more tailored training. MLRO to decide when such assessments are to be undertaken.
6. Record Keeping: Vanquis are required to retain customer and transactions data in order to meet the money laundering regulations.

• All Financial Crime-related records must be retained for at least five years after the end of a customer relationship, in line with this Policy and the Data Retention Policy.
• All customer and transactions records must be:
  ○ Legible, high-quality, and readily retrievable
  ○ Capable of reconstruction (for digital/electronic formats)
  ○ Include audit trails to evidence compliance with policy requirements
• ISARs and NCA submissions must be stored securely with restricted access to prevent unauthorised disclosure or tipping off.
• The MLRO must have unrestricted access to all records to fulfil regulatory duties under the Money Laundering Regulations (MLRs).

Monitoring

The following monitoring controls are in place to support the effectiveness of the policy:

- Identified money laundering and sanctions risks are documented on Riskonnect and assessed and monitored in line with the **Risk Management and Internal Control Framework**. Risks outside of tolerance are escalated to the CRO and Collections, Recoveries and Fraud Committee and monitored until risk exposure is back within appetite.
- Risk events, policy breaches and control ineffectiveness are escalated to the CRO and Collections, Recoveries and Fraud Committee and tracked to resolution in a timely manner.
- Performance against financial crime risk appetite metrics and supporting key risk indicators are monitored with breaches or trends toward breaches escalated to the CRO and Collections, Recoveries and Fraud Committee to monitor.

- Second and Third Lines of Defence provide independent and risk-based oversight and assurance, in line with the **Integrated Assurance Framework**.

Policy Governance

This policy is governed as per the requirements set out in the Policy Governance Framework, which provides a structured process with clear roles and responsibilities for the development, review and oversight of policies within Vanquis' Policy Hierarchy to support policy embedding and ongoing management.

Roles and Responsibilities

The RACI matrix below details the AML, CTF, CPF and Sanctions Policy roles and responsibilities:

	Roles						
	1LoD	2LoD			3LoD	Governing body	
Task/Activity	Financial Crime Operations	MLRO	2nd Line FC Risk Team	CRO	Internal Audit	Collections, Recoveries & Fraud Committee	Board Risk Committee
Policy development & review	C	A	C	I	I	C	C
Policy approval	I	R	R	C	I	C	A
Policy communication & implementation	C	A	R	I	I	C	I
Policy monitoring	C	A	R	I	I	I	I
Policy attestation	I	A	R	I	I	C	C
AML framework development & implementation	C	A	R	C	I	I	I
Business-wide financial crime risk assessment	C	A	R	C	I	C	I
MLRO annual report	I	A	R	C	I	C	C
AML risks identification & management	C	A	R	I	I	C	I
Oversight of governance, risk management & controls	C	C	R	A	I	C	I
Risk-based independent assurance	C	C	C	C	A	I	I

RACI key:

R: Responsible	Assigned to complete the task/activity.
A: Accountable	Has final decision-making authority for task/activity completion. Only one per task.
C: Consulted	An adviser, stakeholder or SME who is consulted prior to a decision/action.
I: Informed	Must be informed post decision/action.

Policy Non-Compliance

This is a mandatory policy for Vanquis; however, it is recognised that waivers and exceptions are sometimes necessary. Where a policy user is unable or potentially unable to comply with a particular element of the policy, a breach, waiver or exception must be raised in accordance with the Policy Governance Framework. Unreported breaches or policy non-adherence may result in disciplinary action.

Policy Attestation

Policy owners must conduct an annual policy attestation of adherence and effectiveness at the point of policy reapproval.

Version Control

Version No.	Reason for Change	Approved by	Date Approved
1.0	New Group-wide policy	Group Risk Committee	May-23
2.0	Annual refresh, incorporating CEL	Board Risk Committee	May-24
3.0	Annual refresh	Board Risk Committee	May-25
3.1	Change of policy template	Compliance Director & MLRO	Dec-25

Appendix 1 Key Definitions

1. **Money Laundering**: Money laundering risk is defined as the risk that VBG's goods and services are used to launder criminal property. This definition is based on the three principal money laundering offences under the Proceeds of Crime Act 2022 ("POCA"):
    - Concealing, disguising, converting, transferring criminal property, or removes criminal property from the UK.
    - Entering into or to become concerned in an arrangement which facilitates the acquisition, retention, use or control of criminal property.
    - Acquisition, use, and possession acquire, uses, or possesses criminal property.

    Money laundering requires the offender to suspect or know that property is criminal such as those derived from fraud, tax evasion, or offences involving illegal drugs. Criminal property is defined as a person's benefit from criminal conduct including cash, cheques, and other possessions such as vehicles, jewelry, and electronics.

2. **Terrorist Financing:** Terrorist financing risk is defined as the risk that VBGs products and services are used to finance or facilitate terrorist acts. This definition is based on the principal terrorist financing offences under the Terrorism Act 2000 ("TACT"). These are:
    - Fund-raising for the purposes of terrorism.
    - Use and possession of money or other property for the purposes of terrorism.
    - Making money or other property available for the purposes of terrorism.
    - Insurers making payments in connection with terrorist demands.
    - Facilitating the retention or control of terrorist property, by or on behalf of another person.

    Terrorist property is money or other property which is likely to be used for the purposes of terrorism. It also includes the proceeds of the commission of acts of terrorism, and the proceeds of acts carried out for the purposes of terrorism.

3. **Proliferation Financing:** Proliferation financing risk is defined as the risk that VBG's products and services 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 (including both technologies and dual-use goods used for non-legitimate purposes), is in contravention of national laws, or where applicable, international obligations.

4. **Sanctions:** Financial sanctions are restrictive measures implemented by individual countries and supranational groups typically to try and achieve a foreign policy or national security objective. They tend to target specific states, entities, organizations, or individuals and can limit the provision of certain financial services and restrict access to financial markets, funds, and economic resources. Sanctions risk is defined as the risk that VBG onboards or maintains a relationship with an individual or entity in contravention of applicable sanctions laws.

5. **Customer:** A customer is defined as any direct individual with which a business relationship is established, but also includes any third party who has control, and / or access to a

customer's account. This includes any Power of Attorney, secondary card holder, joint holder, authorized user, or any other third party meeting the definition above.

6. **Tipping Off:** Where a customer is the subject of an ISAR to the MLNO or a SAR to the NCA, under no circumstances can that customer be informed they are the subject of such a report. This is called Tipping Off and is a criminal offence under POCA, with further offences in place where this information may prejudice an investigation. Tipping off offences have a maximum sentence of 2 years imprisonment and / or an unlimited fine. Further actions may be taken in line with the Group's disciplinary procedures which can lead to outcomes up to, and including, dismissal. Care must also be taken to ensure that accessing public information online does not leave an electronic footprint attributable to the Group which could infer an ongoing investigation into money laundering or terrorist financing. Colleagues should refrain from discussing reports they have made with other colleagues unless there is a business need to do so. Tipping off does not typically occur where enquiries are made to the customer in the investigation of whether activity is suspicious. This includes proportionate questions, and evidence requests as to the nature and purpose of transactions, source of funds, and the customer's identification. However, note that customers must not be informed these enquiries are being made for the purpose of satisfying an investigation into possible suspicious activity.

7. The MLRO and the MLNO have distinct responsibilities within the financial crime governance framework. The MLRO is the senior individual accountable for overseeing the firm's compliance with anti-money laundering (AML) and counter-terrorist financing (CTF) obligations, ensuring robust systems and controls are in place, and reporting directly to the board and regulators. In contrast, the MLNO acts as the designated point of contact for receiving internal suspicious activity reports (SARs) and determining whether these should be escalated to the MLRO for onward reporting to the authorities. While the MLRO provides strategic oversight and regulatory engagement, the MLNO focuses on operational handling of disclosures and ensuring timely, accurate escalation in line with legal requirements.

Appendix 2 MLRO Contact details of Vanquis

Vanquis Bank Limited and Moneybarn 1 Limited

Name: Chris Pawson

Title: Compliance Director and MLRO

Email: Chris.Pawson@Vanquis.com and AMLReporting@vanquis.com, MLRO@vanquis.com

Cheque Exchange Limited

Name: Kathryn Thompson

Title: MLRO

Email: kathryn.thompson@cheque-exchange.co.uk

Appendix 3: PEPs and RCAs

Under the MLRs and FCA guidance, a person is considered a PEP if they hold any of the following positions:

- Heads of state, heads of government, ministers and deputy or assistant ministers
- Members of parliament or of similar legislative bodies – similar legislative bodies include regional governments in federalized 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 considers 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 of any judicial body the decisions of which are not subject to further 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 – where those holding these offices on behalf of the UK government are at Permanent Secretary/Deputy Permanent Secretary level, or hold the equivalent military rank (e.g., Vice Admiral, Lieutenant General, Air Marshal or senior).
- Members of the administrative, management or supervisory bodies of State-owned enterprises – this only applies to for profit enterprises where the state has ownership of greater than 50% or where information reasonably available points to the state having control over the activities of such enterprises; and
- Directors, deputy directors and members of the board or equivalent function of an international organization –this only includes international public organizations such as the UN and NATO.

Relatives are determined under MLRs to include: a spouse or civil partner of the PEP, children of the PEP, spouses or civil partners of the PEP's children, the parents and siblings of the PEP.

Known Close Associates include:

- An individual known to have joint beneficial ownership of a legal entity or a legal arrangement or other close business relations with a PEP.
- An individual who has sole beneficial ownership of a legal entity or a legal arrangement which is known to have been set up for the benefit of a PEP.

Appendix 4: Vanquis Risk Appetite Statement

The Board of VBG has determined that it will not establish or maintain relationships with customers or other parties which fall outside of its defined financial crime risk appetite, or which are prohibited by law.

Specifically, VBL will not provide or maintain Customer Relationships with the following individuals:

- Any person (or entity with which that person is associated) is prohibited under applicable sanctions laws or regulations, being those issued by OFSI, OFAC, or the UN.
- Any person linked to proliferation financing activities which comes to the attention of VBG.
- Any individual who has been convicted of a criminal offence (anywhere in the world) which is a predicate offence to money laundering and has led to the individual being given a custodial sentence of 6-months or more, and such custodial term was not concluded within the previous 5 years.
- An individual who has been convicted of any fraud, money laundering (including drug related offences) or terrorism offence of any nature, regardless of the length of custodial sentence or when it was concluded, unless approval is given by the MLRO where for the need for the implementation of additional controls can be considered.
- An individual who has been convicted of a criminal offence or the subject of adverse media that due to its nature may present a material reputational risk to VBL.
- Any individual who refuses to provide information requested by VBG for the purposes of implementing this Policy or provides information, which is determined to be fake, forged, or fraudulent.
- Any individual whom VBG suspects is in breach of the Terms and Conditions applicable to the Product or Service being used which could increase the risk of Financial Crime to a level outside of risk appetite.
- Any individual who is known to be involved in ML/TF or sanctions circumvention or where VBG has reasonable grounds to suspect the customer is/has been involved in ML/TF or sanctions circumvention.

Vanquis will not maintain relationships with Outsourcing Parties where:

- The Outsourcing Party (or person with which that entity is associated) is prohibited under applicable sanctions laws or regulations.
- Vanquis is aware of significant adverse media on the Outsourcing Party, which gives rise to increased financial crime risks or the potential for negative reputational concerns for the Group.
- Vanquis suspects that the Outsourcing Party may be involved in ML/TF or have reasonable grounds to suspect the customer is involved in ML/TF.
- Any entity or person with which that Outsourcing Party is associated refuses to provide Due Diligence information requested by Vanquis as part of the Procurement Policy.

Vanquis will not employ any individuals as Applicable Colleagues nor will they permit any Outsourcing Party to allow any individual to act on behalf of VBG where such individual:

- Is listed on the OFSI, OFAC, or UN Sanctions Lists;
- Has a criminal record involving any crime involving financial matters; or
- If holding a position under the FCA's SMCR regime, it does not meet the requirements applicable to their role.