# Prevention of Financial Crime Policy

## 1. Aim of policy

We are committed to preventing, detecting and guarding against the impacts of financial crimes and reporting about these appropriately. This policy outlines how we do this and applies to the whole VIVID group.

We have a zero-tolerance approach to all forms of financial crime committed by staff, board members, formally involved customers, volunteers and other organisations or individuals we work with or who act on our behalf. We expect all these individuals and organisations to follow this policy.

We aim to uphold legislation and regulation relating to financial crime, including:

- Bribery Act 2010;
- Computer Misuse Act 1990;
- Criminal Finances Act 2017;
- The Money Laundering, Terrorist Financing & Transfer of Funds (Information on the Payer) Regulations 2017 (MLR);
- Fraud Act 2006;
- Prevention of Social Housing Fraud Act 2013;
- Proceeds of Crime Act 2002 (PoCA);
- Serious Crime Act 2015;
- Terrorism Act 2000.

## 2. Definitions of financial crimes

**Bribery** is offering, giving or accepting money or something of value for influence or action in return.

**Corruption** is dishonesty or fraud by people in authority, typically involving bribery.

**Financial cybercrime** is a criminal activity carried out by means of computers and/or internet. It includes unauthorised access, sabotage or use of computer systems with the intention to cause financial gain to the perpetrator or financial loss to the victim.

**Fraud** is wrongful or criminal deception for personal or financial gain.

**Money laundering** is the process by which money or other assets obtained through crime is exchanged for clean money or assets without an obvious link to the money's criminal origins.

**Tax evasion** is the offence of cheating the public revenue (e.g. HM Revenue & Customs (HMRC) and other taxation authorities) or fraudulently evading tax.

**Tax evasion facilitation** is where an individual or entity deliberately and dishonestly facilitates tax evasion.

**Terrorist financing** is the provision of funds or financial support to terrorists, usually associated with money laundering.

**Theft** is dishonestly appropriating property belonging to another person with the intention of permanently depriving them of it.

## 3. Policy

We prevent and mitigate **Financial Crime** through:

- our Rules which provide a governance framework; we make charitable donations in accordance with our Rules;
- maintaining annually reviewed:
    - standing orders which set out how our Board will work and what authority they have delegated to sub-committees or the Executive team;
    - financial regulations including delegated authority limits;
    - intra-group agreements which set out agreed terms, roles and responsibilities between VIVID and our subsidiaries
    - internal financial processes and controls for income, purchases, payments, property and investments and monitoring these for compliance;
    - compliance with our code of governance;
    - procurement procedures and an approved list of contractors and consultants. We conduct due diligence on suppliers at tender stage and throughout our relationship. Suppliers are required to put in place appropriate measures to prevent financial crimes occurring. We provide clear statements of the services and relevant payments to be made in the contracts. We make a provision for termination where any such crime has been committed;
    - code of conduct, conflict of interest procedure and gifts and hospitality procedure and register;
    - speak up policy and procedure to facilitate whistleblowing and provide guidance on investigating;
- reviewing management accounts at Executive team monthly and Board a minimum of six times a year;
- keeping quarterly reviewed and assessed operational and strategic risk registers where risks relating to financial crime are recorded and kept up to date, as determined in our risk management policy which is annually reviewed by Audit and Risk Committee (ARC);
- consideration of risks as part of every new project, business activity, business processes change or new technology through capital proposals to the Project Approvals Committee (PAC) and project risk registers;
- undertaking a schedule of internal audits to ensure operational risk controls are functioning on a quarterly basis and specialist deep dive audits to examine effectiveness of specific areas of the business. Agreed by ARC annually and reviewed at every ARC meeting;
- maintaining crime insurance;
- Heads of Service and the Executive team reviewing a six-monthly legal update report to help identify any threats of financial crime in the social housing sector and wider business community;
- keeping a Fraud Register which is a standing item at every ARC meeting, providing our regulator with an annual fraud losses report through the NROSH+ portal within 6 months of the end of the financial year and reporting material fraud at the earliest opportunity to the regulator;
- ensuring that any Joint Ventures we enter are managed through a written contract;
- mandating staff to read and comply with this policy.

We specifically prevent and mitigate against **Bribery, Corruption and Theft** informed by principles of the Bribery Act:

- Proportionality – our prevention of financial crime policy considers bribery and our activities are proportionate to our size and sector risk. Our policies are approved by the appropriate level of authority annually as specified by our policy framework.

- Top level commitment – our Board is committed to preventing bribery associated with VIVID. They foster a culture within VIVID in which bribery is unacceptable. We publicise our approach to preventing financial crime on our intranet and website.

- Risk assessment – we understand and keep up to date with bribery risks through quarterly risk assessments.

- Due diligence – we take steps to understand those who perform services on our behalf in order to mitigate bribery risks through our procurement procedures.

- Communication – we publish our prevention of financial crime policy on our intranet and website.

- Monitoring and review – we monitor and review our prevention of financial crime policy annually and make improvements where necessary.

We specifically prevent and mitigate against **Money laundering (including terrorist financing)**:

- Registration – we are registered with the HMRC for our estate agency work and the Financial Conduct Authority (FCA) for our consumer credit activities.

- Money Laundering Reporting Officer (MLRO) - We've appointed the Company Secretary as our MLRO (deputised by the CEO). This is who we report concerns of money laundering to.

- Training is available for specific roles whose work is relevant to compliance with AML and/ or whose work may contribute to the identification, mitigation, prevention or detection of money laundering such as staff involved in consumer credit, sales and lettings, rent collection.

  We can arrange enhanced training for those staff in higher risk areas of the business if required.

- Staff screening - 'Screening' is an assessment of skills, knowledge, and competence to carry out the role and conduct and integrity. We carry out screening of relevant employees before and during employment. This may include undertaking DBS checks. These checks are recorded on their personnel records.

- Due diligence – we conduct due diligence on our transactions as detailed in Appendix 1

- Reporting of suspicious activity - Where we know or suspect money laundering, we make a disclosure to the MLRO as soon as possible and treat the reporting of such suspicions confidential and securely because we are conscious that failing to disclose knowledge or suspicion of money laundering or tipping off can result in serious criminal penalties for both individual members of staff and for VIVID.

- Record-keeping – we keep documents demonstrating compliance with the regulations in line with our document retention schedule, which is guided by the National Housing Federation document retention schedule.

- Risk assessments and risk management - we conduct quarterly assessments of our exposure to risks, including money laundering risks, and the controls we have in place. We report risks to the ARC at every meeting and the Board every six-months as detailed in our risk management policy.

- Transactions - We risk assess individual transactions and conduct ongoing checks according to the assessment of that risk as detailed in Appendix 2.

- Internal controls – we maintain adequate and appropriate controls to forestall and prevent money laundering. These controls take account of the risk factors which we face, and where activities are outsourced our contracts set out minimum 'standards' suppliers must adhere to.

- Independent audit – we have independent external and internal audit functions which examine and evaluate our compliance with the regulations. Board appoints the external auditors annually and ARC appoints, or renews, the internal auditors annually with a full internal audit tender at least every ten years. The assurance plan for internal audits is set annually by ARC then reviewed and updated at every meeting to ensure these audits match our current risk environment as detailed in our risk management policy.

**Prevention of facilitation of tax evasion**
We publish an annual statement of our position to prevent tax evasion and the measures we take.

## 4. Responsibilities

**The Board**
- review our policy annually;
- appoint an MLRO who makes sure we work within money laundering law.

**The Audit and Risk Committee**
- review reports about financial crime and recommend or approve action;
- ensure adequate systems of internal control are in place to manage and report financial crime.

**The Money Laundering Reporting Officer (MLRO)**
- ensure that we do background checks on staff who could uncover identify, mitigate, prevent or detect money laundering within their role;
- make sure staff, agents and consultants are appropriately trained in money laundering;
- receive and investigate reports of suspicious activity;
- make quarterly reports to ARC;
- where there are reasonable grounds that there was actual or suspected money laundering, make a Suspicious Activity Report to the National Crime Agency (NCA) as soon as reasonably practicable;
- inform staff who have made a disclosure how to proceed, including when the informant can continue with activity that would be prohibited under PoCA or the MLR;
- suspend activities giving rise to actual or suspected money laundering pending a response from the NCA;
- document the decision taken and any outcomes from the NCA.

**Managers**
- implement policy in their processes and procedures;
- make sure staff know what's expected of them and are properly trained.

**Staff, board members, formally involved residents, volunteers, and others acting on our behalf**
- read and comply with this policy and related documents;
- undertake training as necessitated by role;
- report any suspected incidents of financial crime directly to the MLRO.

| Author | Owner | Date approved | Review date |
|---|---|---|---|
| Head of Governance | Chief Finance Officer | November 2022 | November 2023 |

## Appendix 1

**What is due diligence**
Due diligence involves identifying and verifying identity based on documents, data or information obtained from a reliable and independent source.

**When do we conduct due diligence?**
The situations in which we would conduct due diligence include but are not limited to:

- tenancy sign up for lettings, successions, and mutual exchanges;
- sale of a property - right to buy, right to acquire and shared ownership;
- when changes to tenancy are requested;
- at a tenancy audit - we conduct tenancy audits on either an annual, risk-based or rolling basis to check that the authorised tenant is living at the property;
- when providing consumer credit services;
- when we suspect money laundering or terrorist financing activities are being carried on;
- when we have doubts if a document or information provided is genuine or adequate.

**Enhanced due diligence for high risk situations**
We would also consult money laundering legislation regarding undertaking enhanced due diligence if:

- we identify a situation in which there is a high risk of money laundering or terrorist financing;
- we undertake a business relationship or transaction with a person established in a high-risk third country;
- the customer or one of their close family members or associates is a Politically Exposed Person (PEP) e.g. member of parliament, member of supreme courts/ courts of auditors or central banks; ambassadors, high-ranking officer in the armed forces, etc.;
- the customer has provided false or stolen identification documentation or information and we propose to continue to deal with that customer;
- a transaction is complex and unusually large, there is an unusual pattern of transactions, and the transaction has no apparent financial or legal purpose.

**How do we conduct due diligence?**
We verify the individuals full name(s), residential address(es) and date of birth using government-issued documents which must include the customer's full name and a photograph with either the customer's date of birth or residential address such as a full driving licence, passport, or identity card.

Where the customer does not have such documentation, we accept a government-issued document (without a photograph) which includes the customer's full name and is supported by secondary evidence of the customer's address such as evidence of entitlement to state or local authority-funded benefit, a council tax statement, utility bill, or bank statement which are not more than 3 months old.

We conduct checks to ensure we are satisfied that the evidence presented is genuine. These checks may include checking spelling of names, validity, photo likeness, whether addresses match, a visit to the customer at their home address, corroborating checks from separate sources, etc. and we will only accept this evidence when we are satisfied it is genuine.

We proceed with transactions with the customer present in person, digitally or where we have had contact with them digitally or by phone. We explain to the customer that failure to disclose information or false claims on an application may lead to housing being denied and/ or legal action taken.

## Appendix 2

**Business transaction payments**
We do not accept cash payments (notes, coins or travellers' cheques) to any value.

**Ongoing tenancy management**
Lettings Officers make financial checks when a nomination is received. Income officers monitor the accounts and weekly rent sense monitoring raises unusual payment patterns.

At tenancy audits Neighbourhood Officers review any red flags of potential fraud that may warrant further examination. These include:

- no repairs raised for a prolonged period;
- high arrears on rent;
- high number of antisocial behaviour reports;
- high number of complaints.

We respond to claims of tenancy fraud and investigate each allegation.

Actions taken due to any further examination depend upon the outcome.