FINANCIAL CRIME STATEMENT

AIB Group plc

August 2023

INTRODUCTION

Financial Crime is any kind of criminal conduct relating to money or to financial services or markets, including any act involving:

- money laundering;
- handling the proceeds of crime; or
- the financing of terrorism; or
- fraud/dishonesty; or
- anti-bribery and breaching any relevant corruption legislation; or
- breaching of any law/regulation relating to sanctions, Financial Crime or tax evasion (including facilitation thereof) in all jurisdictions in which the Group operates.

AIB Group plc ("AIB") recognises that Financial Crime poses economic and social problems for business and consumers throughout the world, including the jurisdictions in which the Group operates. Financial Crime undermines the integrity of markets, diverts resources away from productive uses, erodes public trust in financial institutions, and can be used to fund further illegal activities. Additionally, it often disproportionately harms low-income communities, as well as small and medium sized businesses. This has a devastating impact on both individuals and society as a whole.

We are committed to doing business responsibly and sustainably, and to live by our economic, social, ethical and environmental values. Practically, this means that from a Financial Crime perspective, AIB is committed to:

- Safeguarding our customers, the Group, community and the wider financial system through the detection, prevention and deterrence of Financial Crime across the Group;
- Supporting law enforcement in the investigation and prevention of Financial Crime, in all jurisdictions in which the Group operates;
- Complying with not only the letter, but also the spirit, of all laws, codes and regulations applying to our businesses in all jurisdictions in which the Group operates;
- Acting with honesty and integrity in relation to all business activities and customer engagements that we undertake;
- Effectively implementing and executing the requirements of applicable sanctions programmes.

Framework & Policy

Our robust Financial Crime Framework, approved by our Board Risk Committee, includes our Financial Crime Policy and Standards on Anti-Money Laundering ("AML")/Countering the Financing of Terrorism ("CFT"), Fraud, Anti-Bribery and Corruption ("ABC") and Sanctions. The Policy and Standards are embedded within business operating procedures, and subject to at least an annual content verification to ensure they are kept up to date.

The Policy and Standards are applicable to all staff including contractors and consultants working in or for the Group (including all business functions, relevant subsidiaries and branches of Allied Irish Banks, plc) across all jurisdictions in which the Group operates.

Training & Awareness

All employees and the Directors of AIB Group plc receive communications about, and training on, our Financial Crime Policy and Standards and on their responsibilities in relation to them.

All employees are required to complete three mandatory e-learning courses annually that cover (i) Anti-Money Laundering and Countering Terrorism Financing, (ii) Conflicts of Interest and (iii) the Code of Conduct (our anti-bribery and corruption training is covered in ii) and iii). This intranet-based training includes case studies and self-assessment checks to help build and reinforce awareness.
Our Money Laundering Reporting Officer (MLRO) provides comprehensive annual training to the Board on Financial Crime matters, including Anti-Bribery and Corruption. Bespoke, face-to-face training tailored to consider the Financial Crime risks relevant to specific roles is also provided to key employees by Group Financial Crime Compliance.

To further enhance awareness, Financial Crime Bulletins are issued periodically to our employees, outlining key trends and other topical items relating to Financial Crime.

Accountability

The Group Board is ultimately responsible and accountable for management of Financial Crime risks within the Bank. Group Financial Crime Compliance, led by the MLRO, perform ongoing monitoring and oversight of Financial Crime controls across the Group.

ANTI-MONEY LAUNDERING (AML) / COUNTERING THE FINANCING OF TERRORISM (CFT)

Money laundering is any act or attempted act to conceal or disguise the identity of illegally obtained proceeds so that they appear to have originated from legitimate sources. Terrorist Financing is the processing of funds to sponsor or facilitate terrorist activity. This may include funds raised by legitimate businesses and charitable organisations, as well as from criminal activities, such as the drug trade, the smuggling of weapons and other contraband, human trafficking, fraud, cybercrime, kidnapping and extortion. It is different from Money Laundering in that the funds involved do not have to come from illegal sources and it is the destination of the funds and not the origin that is the focus of terrorist financing.

AIB is committed to the fight against money laundering and the funding of terrorist and criminal activities. The Bank operates a comprehensive AML/CFT Programme to:

- comply with all applicable legal and regulatory requirements in relation to AML/CFT; mitigate identified AML/CFT risks; and
- protect its customers, the Bank and wider society from the harm of financial crime.

In AIB, we manage Financial Crime matters through the Three Lines of Defence ("3LOD") model. Through the deployment of a 3LOD framework, the operation of each line of defence is assessed by the next line. Assurance teams operate throughout each of the Three Lines, and regularly report to Senior Management and the Board on the efficacy of Financial Crime controls. AIB's Group Money Laundering Reporting Officer (MLRO) is responsible for oversight of the AIB Group compliance with applicable AML laws, regulations and codes. The MLRO is also the PCF-52 (Head of Anti-Money Laundering and Counter Terrorist Financing Compliance) which is a Pre-Approved Control Function under the supervision of the Central Bank of Ireland. A local MLRO (in the UK) and BSA/AML/OFAC Officer (in the US) have a statutory control function responsibility within their jurisdictions. AIB is externally supervised, in the jurisdictions in which it operates, by the Central Bank of Ireland (ROI), the Financial Conduct Authority and the Prudential Regulation Authority (UK) and the New York Department of Financial Services and Federal Reserve Board of New York (USA).

Our customers go through Customer Due Diligence process at the onboarding stage and on an ongoing basis, which is driven by the risk assessment of the customer. Within the due diligence process, we screen customers against various criteria including national/international sanctions lists. Additional measures are applied where a higher risk is presented (e.g. business relationship is conducted on a non-face to face basis). Some customers and beneficial owners present an inherently higher risk (e.g. politically exposed persons ("PEPs") and/or customers established/residing in a 'high-risk third country'). For these customers we apply enhanced due diligence and require senior management approval.

AIB has appropriate monitoring processes in place to identify and investigate unusual patterns of customer activity which may give rise to suspicions of money laundering or terrorist financing. Where suspicious activity is identified, it is reported to the relevant authorities in accordance with operating guidelines for reporting.

AIB, in compliance with the relevant regulatory requirements, retains specific records, e.g. concerning the Business Risk Assessment, customer identification and transactions, for at least seven years after the cessation of the business relationship.

SANCTIONS

Sanctions are restrictive/coercive measures against targeted individuals, entities, countries, governments and industries. They are a key element of AIB's Financial Crime Framework and are heavily influenced by geopolitical considerations. Sanctions regulations applicable to the Bank are derived from the foreign and security policies of the United Nations, the European Union, the United Kingdom, and the United States, amongst others. They are an essential tool of international foreign and security policy, through which groups of nations work together to prevent conflict, deter aggression, or respond to emerging or current international crises. In spite of the implications within the name, "sanctions" measures are not intended to be punitive. They are rather intended to deter serious illegal activity such as terrorism, corruption, armed aggression, and human rights abuses, and to bring about a change in policy or activity through targeting the entities and individuals responsible for such malignant behaviour.

Sanctions may be aimed at members of government bodies within specified target countries, as well as companies, groups, organisations, or individuals, through the following measures:

- arms embargoes
- restrictions on admission (travel bans)
- asset freezes
- other economic measures such as restrictions on imports or exports.

Sanctions are carefully directed and designed to be proportionate to the objectives they seek to achieve. As such, they target those responsible for malign policies or actions, while reducing as much as possible any unintended consequences. The success of sanctions programmes depends on their enforcement and their effective execution by institutions. AIB undertakes customer and transactional due diligence to manage its adherence to these requirements and sanctions risk. It is wholly committed to the effective implementation of applicable sanctions programmes and shall not tolerate compliance failures in respect of its business activities in this regard. This means that at times our sanctions risk appetite may be more conservative than the letter of the prevailing regulations, and we may resolve not to support particular business activities even where we are legally permitted to do so.

FRAUD

AIB defines fraud as "acts of deception or omission intended for personal gain or to cause loss to another party by customers, suppliers, third parties or colleagues. This includes acts of theft". Actions which constitute fraud include external fraud (fraud perpetrated against the Bank and/or its customers which does not involve the participation or involvement of Bank staff) and internal fraud (fraud involving the participation or involvement of staff).

In line with our Strategy, 'Customer First' is a primary ethos of AIB and all staff. To safeguard our customers, we apply detection, prevention and deterrence measures against Financial Crime, including Fraud. We comply with the spirit and the letter of all applicable laws, codes and regulations, including the Consumer Protection Code, ensuring that we act honestly, fairly and professionally in the best interests of customers and with necessary due skill, care and diligence. We have a set of

Fraud Standards, supporting the Financial Crime Policy, which set out the overall approach to managing external and internal fraud. Underpinning our Policy and Standards are various operational processes and procedures carried out by teams within the wider Financial Crime team.

At AIB we are committed to protecting customers against the threats associated with fraud, and we have a strong record in this regard. We have implemented an ongoing fraud education programme for customers via online messaging, emails and issue-targeted social media alerts. In addition, our Online Banking Security Centre web page has details of specific current fraud threats that are targeting our customers, and alerts that they should be aware of.

We have multiple layers of two factor payment authentication and fraud monitoring in place for online and card payments. The bank deploys a suite of anti-fraud controls which include (but are not limited to) sending texts and mobile banking in-app messages to customers to confirm some transaction types and also reviewing transactions in real time. We work closely with the Gardaí to prevent fraud and support their investigation of cases.

The bank is fully engaged at industry level, including participating in the FraudSmart education agenda and limiting the opportunities for telephone networks to be misused by fraudsters. The bank presents a comprehensive fraud training course to all staff members on a yearly basis. This course is designed to ensure that staff members are aware of current trends on the fraud landscape.

ANTI-BRIBERY AND CORRUPTION ("ABC")

Bribery is an inducement or reward offered, promised or provided in order to gain any commercial, contractual, regulatory or personal advantage, whether received intentionally or unintentionally. Corruption is the abuse of entrusted power for the private gain of the individual or company. Corrupt business practices put the interests of an individual or company before the interests of the environment, customers, societies, communities and other key stakeholders. Corrupt behaviours / practices include, but at are not limited to, acting with an improper purpose personally or by influencing another person, by:

- making a false or misleading statement;
- withholding, concealing, altering or destroying a document or other information; or
- any other means.

AIB prohibits bribery and corruption. Our ABC programme seeks to address the following risks:

- Employees offering, giving, promising, providing, soliciting, requesting, accepting or agreeing to receive anything of value, whether cash or in any other form (directly or indirectly), intentionally or otherwise, to or from any person or entity (wherever located) for the purpose of (i) Gaining any commercial, contractual, or regulatory advantage for AIB in any way which is unfair or unethical (ii) Gaining, or engaging in conduct that could be viewed as gaining, any personal advantage, financial or otherwise, for themselves;
- Employees improperly offering, promising or transferring anything of value (directly or indirectly) to a public official wherever located in order to (i) Influence the public official in the

exercise of their public functions, or (ii) Obtain or retain business for AIB, or (iii) Secure advantage for AIB, its employees or any other entity or person;

- Employees failing to adhere to the requirements of our Conflicts of Interest Policy or Code of Conduct.

Corruption undermines stakeholder legitimacy and trust, and regular communications and training on Conflicts of Interest and ABC helps to build our organisational resilience to it. AIB's approach is set out in the ABC section of our Financial Crime Policy (supported by a set of ABC Standards), and in our Conflicts of Interests Policy - two of the policies that underpin our Code of Conduct for employees. These policies cover how actual, potential or perceived conflicts of interest are to be evaluated, reported and managed to ensure that employees, including our Directors, act at all times in the best interests of the Group and its stakeholders.

All business areas are responsible for completing a four-monthly risk assessment of all registered activities to ensure they are in keeping with our ABC obligations and identify those which might give rise to a potential or perceived conflict situations or corruption. Material matters relating to ABC will be escalated to the Board by management on a case-by-case basis through Executive Management Reporting.

We will run due diligence checks on all potential suppliers to ensure they comply with our policies and to minimise risk. Depending on the potential risk, some suppliers will be subject to our risk assessment process. This risk assessment will be reviewed annually in line with our third party management policy.

Any member of staff who has concerns or suspicions regarding suspected instances of bribery and/or corrupt behaviours or practices is obliged to report the matter. There are three channels open to staff to do this:

(i) Their supervisor or line manager (where appropriate);
(ii) Head of Special Investigations Unit, Group Internal Audit;
(iii) Internal Speak Up Channel.

ABOUT THIS DOCUMENT

This document synopsises the key aspects of our internal Financial Crime Policy, a detailed policy which is part of the Regulatory Compliance Risk Management Framework. The policy defines AIB Group plc's approach to managing Financial Crime Risk and covers Anti-money laundering, Countering the financing of terrorism, Sanctions, Fraud and Anti-bribery & corruption. The policy was approved by our Board Risk Committee in Sept 2022.

The policy and supporting standards are embedded within business operating procedures, and subject to at least an annual content verification to ensure they are kept up to date. The employees of AIB Group and our 100% owned subsidiaries AIB Mortgage Bank, EBS dac (incl. Haven), AIB UK and Goodbody are required to comply with our Financial Crime Policy.

This document is owned by the Group Chief Compliance Officer.