Financial Institutions

BII invests in the financial Institutions – directly through debt and equity or indirectly through funds. Our investments bring affordable financial services to underserved segments. We target liquidity requirements through supply chain finance or risk-sharing facilities and pursue strategic objectives in gender, climate, and SME financing through our investments. BII caters to various types of FIs who offer various types of services and products and serve different customer profiles. Consequently, each FI present different financial crime risk and the approach organisations manage and control such risks. Therefore, a financial crime risk assessment should be performed to assess the financial crime risks presented by different FIs according to their customer profile and the way they serve customers, the products and services offered and the jurisdictions in which they operate. This risk assessment will then determine the nature and extent of financial crime controls required.

- Retail /SME Banking

  The European Supervisory Authorities define retail banking as "the provision of banking services to natural persons and small and medium-sized enterprises."

  Retail banking is susceptible to terrorist financing / money laundering due to the types of products and services offered, open access, as well as the high transaction volume and usually large number of customers. The transaction volume and large number of relationships makes it particularly hard to identify suspicious activity and money laundering / terrorist financing risks in relation to each person.

  Key product, service and transaction factors that could create additional risk include:

  - The product's anonymity features.
  - New products and or business practices that involve the use of novel technologies whose risk implications are not understood.
  - Loans where the collateral held in a different jurisdiction than that where the loan is made.
  - Loan repayments made in cash,

- Services to cash-generating businesses and failure to identify cash activity that is higher than the business activity justifies.

Key factors that can reduce risk of retail banking products include limiting features and use of the product capabilities, for example allowing access only to certain customers types, only allowing orders to be executed through an account in the customer's name at a credit or FI subject to AML/CFT rules. In restricting access to their products, FIs should be mindful of financial inclusion principles. Useful guidance on how to apply FCC controls in a manner that promotes financial inclusion can be found in the FATF's Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion.

Automated monitoring of customer transactions and activity is an important aspect of risk mitigation in retail banking, especially for high-risk customer and businesses operating in high risk jurisdictions. Automated systems used to spot ML/TF risks and suspicious activity should be checked to make sure they are fit for purpose. While useful, automated IT systems should not be used as a replacement of employee vigilance.

- Non-Banking Financial Company

A non-banking financial company (NBFC) is an institution offering various financial services and products to its customers but officially not recognised as a bank with a full banking license. Typically, an NBFC is not allowed to take traditional deposits and does not have access to funds from checking accounts from the public. All non-banking companies can be considered NBFC's such as, specialised lenders (real estate lenders, leasing companies); savings institutions (pension funds, mutual funds etc.); risk-pooling institutions (insurance, reinsurance or specialty insurance companies) and other general financial service providers.

Regulatory guidance on managing financial crime compliance risks for an NBFC may differ based on the exact nature of products and services provided by the company. However, as a regulated financial institution, an NBFC should be cognisant of exposure to financial crime risks and therefore should ideally have made an assessment on risks faced in its operations. The NBFC would be expected to have in place an appropriate risk-based approach for its compliance framework with clear

roles and responsibilities for the second line of defence employees and well-articulated operational procedures for financial crime risk management such as customer due diligence procedures, risk reporting, training and awareness, and record keeping and data protection.

- Microfinance Institutions

  The Basel Committee on Banking Supervision defines microfinance as "the provision of financial services in limited amounts to low-income persons and small, informal businesses." While abiding by regulatory and compliance requirements and having regard to the risks identified through their own risk assessment, MFIs should adapt their operational risk assessments and financial crime controls on a risk-based approach similar to banks. In this context, it is important that MFIs develop policies and procedures for the use of appropriate customer due diligence (simplified or enhanced) and ongoing monitoring. MFI's should also focus on other integrity risks such as frauds and misconduct risks within their business, especially internal fraud.

  Microfinance providers may consider placing restrictions on certain products and services to lower their risk and promote accessibility. These measures include low-value thresholds, geographical restrictions and restrictions on the type of customer who may use the product (for instance, only individuals). It is important to have a strong reporting mechanism within an MFI to identify actual suspicion of financial crime, and subsequent implementation of control activities such as enhanced due diligence, escalation, investigation and reporting procedures.

Insurance Companies

- General insurers

  Business Integrity risks in general insurance are focused towards misconduct risks that may be triggered by weak internal controls and poor quality of independent assurance. Financial crime risks in General insurance is perceived as a low risk especially for money laundering. The financial crime risks associated to general insurers are usually in relation to fraudulent claims.

General insurers should adopt a risk-based approach and design and implement policies and procedures to comply with applicable national laws and the insurer's own risk assessment. Generally, these policies and procedures should cover the processes to manage operational risks, report and investigate suspicious activity and compliance with financial sanctions lists.

- Life Insurance

Since life insurance products are mostly long term and will only pay out during a specified event like a death or retirement, it is not typically considered at high risk of misuse for money laundering. However, insurance does still run the risk of misuse, especially in customers purchasing the products using proceeds of crime.

There are numerous products, service and transaction risk factors that can contribute to added risk including flexibility of payments, accessibility to accrued funds, negotiability and anonymity. Factors that reduce risk include the product not having a surrender value or investment feature, and the product only paying out for a predefined event.

Customer and beneficiary risk factors can be affected by the nature of the customer, the customer's behaviour and the relation to the beneficiary. Distribution channel risk factors can be affected by sales not carried out in person or a lengthy series of intermediaries.

FI's should apply customer due diligence (CDD) measures for all life insurance business to the customer, the beneficial owner and to beneficiaries as soon as they are established. In high risk situations, enhanced customer due diligence should be used. This can mean taking additional steps to supplement the firm's knowledge of the customer, the beneficial owner, the beneficiary or the beneficial owner of the beneficiary, the third-party payers and payees.

Useful guidance on different risk factors to consider can be found in Title III, Chapter 7 of the ESA's Risk Factors Guidelines and Part II of The Joint Money Laundering Steering Group (JMLSG) Guidance on Prevention of Money Laundering/Combating Terrorist Financing.

- Fintechs and Money Service Businesses

The term Fintech refers to technology-enabled innovation that is used to support the production of and delivery of financial services, which includes mobile-enabled services. Fintech is generally viewed as a vehicle for financial inclusion and innovation and its development is supported by national government and intergovernmental organisations alike. At the moment, there's no real agreement about what standards should apply to FinTechs and a number of regulators have been devising specific regulatory guidelines for operations. It is considered that they should apply the same controls as banks, but it is important to balance these requirements with financial inclusion and customer experience. For instance, while supporting financial innovation, the FATF requires that new technologies abide by the organisations AML and CTF standards. FinTechs will need to undertake KYC and transaction monitoring, but *how* exactly they conduct these activities depends on the scale & size of the company, the business model, and importantly the key risks identified. At a minimum, any FinTech that needs a correspondent relationship with a regulated bank will have to demonstrate to the bank that it has these controls in place.

Fintechs can expect an increased amount of regulation and compliance requirements across the world. For instance, in the European Union, the 5th Anti-Money Laundering Directive tackles Fintechs as the Directives' scope has been widened and applies to certain fintech providers, which will be subject to the same requirements as any other financial service providers.

The JMSLG defines electronic money as "a prepaid means of payment that can be used to make payments to multiple persons, where the persons are distinct legal or natural entities." AML & CTF risks associated with electronic money issuers are determined by the specific features of the e-money products and the extent to which e-money issuers use other persons to distribute and receive e-money on the issuers' behalf.

Electronic money issuers should have in place arrangements to periodically monitor transactions and customer relationships. Enhanced customer due diligence should be given to high risk situations and simplified customer due diligence to reduced risk situations, to the extent to which it is allowed by national legislation and international best practice.

Firms issuing e-money should take into consideration risks factors and appropriate measures. Useful guidance on different risk factors to consider can be found in Title III, Chapter 3 of the ESA's Risk Factors Guidelines and Part II of The Joint Money

Laundering Steering Group (JMLSG) Guidance on Prevention of Money Laundering/Combating Terrorist Financing.

- Trade & Supply Chain Finance

Trade Finance: Trade Finance is described as the various operations, including the financing, usually but not exclusively by FIs, undertaken to facilitate trade or commerce, which generally involves the movement of goods and services between two points. Trade transactions can represent high inherent risks of money laundering because money launderers can exploit the complexities associated with trade financing arrangements to evade detection.

In managing the inherent risks associated with this product, best practice suggests that a risk-based approach. FIs should complete a documented financial crime risk assessment for trade finance business that gives appropriate weight to money laundering, fraud and sanctions risk associated with trade transactions. The key risks to be assessed will include the product type, distribution channel, jurisdiction, customer type, volume and size of transactions. Once these risks have been assessed, financial crime controls should be designed and implemented to mitigate risk trade-based money laundering risk.

FIs should carry out enhanced customer due diligence (CDD) on the instructing party, to establish visibility on the customer's business when providing trade finance services. This could include information detailing which trade routes are used or the goods traded to help better understand the customer and in turn help better determine suspicious transactions.

Monitoring procedures for trade transactions should be well-documented and comprehensive to ensure that financial crime risks specific to trade finance transactions are considered. Screening should be conducted on all relevant parties to a transaction with procedures in place for screening against sanctions and the identification of trade-based money laundering typologies; for example; ghost shipments, over or under-invoicing and dual-use goods.

Supply Chain Finance: Corporates involved in international trade will often leverage their financial institutions to optimise their supply chains through technological solutions, payment systems and payables or receivable financing options. The

sophistication of these systems make it difficult for money launderers to infiltrate, however it remains important that financial institutions to risk assess their corporate customers who are managing large global supply chain networks as significant financial crime risks can be prevalent in complex, multijurisdictional business models.