RISK MANAGEMENT

As part of our risk strategy, we have a comprehensive Enterprise-wide Risk and Compliance Framework aligned with our vision to drive consistent value for stakeholders through the optimisation of risk and reward. Within this framework, we have established robust controls and tools that include the following:

- A "three lines of defence" model is central to our risk management framework, helping us to identify potential risks and gauge the effectiveness of related functions and policies.
- FAB has a 'New Product Approval Policy' that provides guidelines on developing new products, and our Risk Management team reviews and approves all new products before launch.
- Our Risk Appetite Framework includes metrics and thresholds, which form part of the balanced scorecard and performance appraisals of senior executives.
- We provide risk-related training to relevant employees that cover Basel guidelines, credit risk and modelling, and financial statement analysis. We also provide mandatory training to all employees on general risks, such as data security and money laundering, discussed in other sections of this report.
- We conduct internal surveys annually to get employee feedback on managing risks, which help us continuously improve our practices.
- To sustain our operations in the event of major events and crises, FAB has a Business Continuity Policy along with plans and incident response procedures that are tested regularly and at a minimum on an annual basis.

Oversight

Overall accountability for risk governance lies with the Board Risk and Compliance Committee (BRCC), which develops and oversees the Group risk strategy, risk appetite and policy guidelines, and monitors adherence to these.

Assisting the BRCC in carrying out these functions are the Group Risk Committee and the Compliance Committee, as well as several sub-committees such as the Operational Risk Committee and the Information Technology/ Information Security Risk Committee that oversee specific risk responsibilities.

Managing Risk

Three Lines of Defence

Board group CEO Executive management

Provides Oversight of Three Lines of Defence

First Line of Defence

- Execute processes & Controls
- Business & Enabling Functions
- Own, Supplement & Operate within the Risk Appetite, Limits and Framework

Second Line of Defence

- Design & Facilitate Pro-active Risk Management
- Group Risk & Compliance
- Design & Monitor Risk Appetite, Limits and Framework Based on Group's Strategy

Third Line of Defence

- Independent Assurance
- Group Internal Audit
- Provide independent assurance on the Adequacy &Effectiveness of the Internal Control, Risk Management, Governance, System and Processes

Data Privacy & Security

The very nature of our business is based on safeguarding customers and their assets, and personal information is an integral component of those assets.

That's why protecting the privacy of our clients and handling sensitive information they entrust to us with the utmost care will always be a top priority at FAB.

A Layered Approach

We have a multi-layered program in place to protect and use personal data in a responsible manner. Aligned with information security standards such as PCI-DSS and NESA, the program includes security and privacy policies, procedures and protocols, such as strong customer authentication methods; secure data storage areas with employee clearance requirements to minimise the risk of unauthorised data access; and a comprehensive data leakage prevention strategy.

We build robust data encryption techniques, network security (e.g., firewalls) and other tools into our products, services and technologies. Sophisticated systems are inplace to continuously monitor suspicious activity and thwart cyber attacks in an evolving threat landscape, and FAB works closely with government agencies and other financial institutions to share security intelligence and analytics. We perform periodic testing and security assessments and our 24/7 security monitoring team reviews security events and incidents.

Employee and Customer Education

Employee education is a key cornerstone of our data governance program. We provide compulsory training (e-learning and classroom based), promote good privacy and security practices among our employees and contractors, and test compliance with these practices through periodic "phishing" simulations. In addition, we have a customer awareness program in which we communicate the importance of customer vigilance regarding online safety and protection of their accounts, financial information and devices.

Oversight

FAB's Group Security Office (GSO) provides direction and oversight of the bank's data privacy and security programme including employee training and awareness.All related policies and procedures are periodically reviewed by the GSO and approved by FAB's executive team. Our EVP & Chief Information Security Officer and Head of Business Continuity Management is responsible for the bank's data security and privacy program.

FAB's information security/cyber security risk, challenges, regulatory requirements and the bank's security initiatives are discussed and reviewed by the Group Security Committee (GSC) and Group Risk on a monthly basis, the Compliance Committee (GRCC) on a quarterly basis, and the Board Risk and Compliance Committee (BRCC) on a quarterly basis. FAB's Information Security Strategy is formulated on the basis of such discussions and reviews in GSC, GRCC, BRCC meetings which are delegated committees from Board of Directors and includes FAB Executive Management.

Fighting financial crime

We invest heavily in crime prevention strategies and maintain robust controls to combat various types of criminal activities – including fraud, corruption, bribery, money laundering, terrorist financing, and breaching of international sanctions.

Anti-Fraud

Our global financial crime unit includes dedicated experts who specialise in crime prevention and managing threats posed to FAB. They undertake activities like fraud risk assessments, review new products before roll-out from a fraud risk perspective, conduct mystery shopping and spot checks to proactively test fraud controls, and update staff and customers about the latest trends in financial crime.

The financial crime unit also works together with law enforcement agencies and industry peers to share intelligence, coordinate efforts and help fight financial crime in the wider community.

We have a Group Vulnerability Assessment and Penetration Testing Policy and Procedures and perform routine assessments to identify possible vulnerabilities on all bank assets and infrastructure including payment card systems. We use advanced analytics that give us better insights and real-time data to uncover and act on potential threats.

Employee Screening and Training

Our approach to fraud prevention includes an employee background check process, mandatory fraud awareness training as part of staff induction and an annual mandatory Anti-Money Laundering (AML), Anti-Bribery and Corruption (ABC) and Sanctions e-learning programme, which requires a minimum pass rate of 80%.

We train our people on how to identify, prevent and deal with financial crime and provide risk-assessment tools and models.

Various polices are in place to guide employees and articulate our commitments, including Anti-Corruption and Anti-Bribery Policy and the Prevention of Money Laundering and Counter Financing of Terrorism and Sanction Compliance Policy.

Screening Customers and Transactions

To verify and onboard legitimate customers, our due diligence process reflects international best practices and complies with relevant laws and regulations with respect to Know Your Customer (KYC) and other client identification requirements.

We continuously update our deterrence and detection infrastructure, which includes sophisticated tools to monitor, track and report criminals and any suspicious transaction activity across channels. Customers and counterparties are regularly screened against listed terrorist organisations and sanctioned names issued by the UN, US, EU, UK and UAE.