Information Security, Cyber Security and Fraud Controls

Information has emerged as a valuable asset in this technological age, necessitating robust control over information security, cyber security and fraud. Our Information Technology (IT) framework provides for controls to overcome the various challenges and threats that can disrupt our business operations and endanger customer data.

We overcome these threats and challenges through the IT framework, which inter-alia covers governance, policy, operations, security, audit and Business Continuity Plan (BCP).

The IT framework of each of the Group companies is designed to establish, implement, monitor and constantly improve its information security posture.

- The focus of the IT framework is on the privacy of customer information and data security
- The material subsidiaries of the Company are compliant with ISO 27001:2013 Information security management system and ISO 22301:2012 Business Continuity Management
- The subsidiaries also comply with the applicable regulatory framework and guidelines (viz. RBI's Master Direction – Information Technology Framework for the NBFC Sector, IRDAI's Guidelines on Information and Cyber Security for Insurers, etc.)
- The Group companies have implemented Data Loss Prevention (DLP) solutions, such as:
  - Endpoint DLP
  - Email DLP
  - Conditional access to Office 365
  - VPN access on corporate laptops
  - Mobile Device Management for corporate mobile apps, etc.
- All data protection controls are enhanced periodically and evaluated at least once a year.

IT Framework and Policies

The material subsidiaries have defined and implemented policies / frameworks / practices on cyber security and risks related to data privacy. The policies cover and communicate the respective company's:

- Commitment to obtain user data through lawful and transparent means, with explicit consent of the data subject where required
- Clear terms involving the collection, use, sharing and retention of user data, including data transferred to third parties
- Commitment to notify data subjects in a timely manner in case of policy changes or data breaches
- Commitment to collect and process user data that is limited to the stated purpose

The Group companies clearly disclose the mechanisms for data subjects to raise concerns about data privacy through dedicated cyber cell units / email IDs on their respective websites.

Cyber Security

Cyber security policies and practices have been institutionalised with the aim to protect information infrastructure on the internet; prevent and respond to cyber threats; reduce vulnerabilities, and minimise damage from cyber incidents. A combination of dedicated teams, processes and technology enable the successful realisation of these objectives. Some of the operational measures to monitor and respond to data breaches and cyber-attacks are:

- Security operations centre: managed by reputed cyber security service providers,
- Surface Web and Dark Web monitoring: carried out through service providers, and
- Customer related fraud events: detected, managed and mitigated through risk control unit along with cyber risk team.

Privacy of Personal Information

Led by a commitment to protecting the privacy of personal data, we have put well-structured privacy policies in place. Our privacy policies apply to our entire operations, including the suppliers. The privacy policy system is embedded in risk/compliance management across the material subsidiaries.

The material subsidiaries of the Company are compliant with ISO 27001:2013 Information security management system and ISO 22301:2012 Business Continuity Management.

Ensuring personal information privacy

- The Customers' Personally Identifiable Information (PII) is masked in the core systems and customer-facing systems through data encryption
- Access to customer PII is restricted, and access is granted based on consent on a need-to-know basis with due approval
- Data uploaded on dialler is stored in an encrypted format, and no access to customer's PII is granted to the calling agent
- Privacy terms are displayed on the website of the respective Group company; it covers the details regarding consent, collection, use, sharing, processing and retention of customer data. Any changes to the Privacy Terms are updated on the respective company's website, where the customers can also raise their concerns

The BFS Group has zero-tolerance for breaches confidentiality and privacy. Further, the Group companies have defined actions, ranging from suspension to termination, penalty, legal action, etc., for noted instances of data breach. During the year, there were no instances of data breaches involving PII of customers across any of the Group companies.

Audits and Assessments

We undertake regular audits and assessments of the security threats through a comprehensive strategy comprising:

- Regular internal security audits, vulnerability assessments and penetration testing of systems, products and practices affecting user data
- Periodic application security assessment, like pre-production, six-monthly application security assessment and yearly structured exercise at various stages of business enhancements, APIs, Bots etc.
- At least annual audit assessments, by external experts, of systems, products and practices affecting user data
  - ISO 27001 Surveillance Audit
  - ISO 22301 Surveillance Audit
  - Audits required as per the applicable regulatory requirements
  - Red Team exercise for internet-facing customer systems and IT Infrastructure

Governance structure

In case of material subsidiaries, the IT security-related projects and operations are reviewed by a committee, under the oversight of the respective company's Board. The committees meet at least on a half-yearly basis. Dedicated teams manage the cyber security programme and operations for digital initiatives.

Awareness and Training

The BFS Group deploys multiple channels, such as class-rooms training, mails, posters, chronicles, brochures, etc., to create cyber security awareness across stakeholder communities, including employees, value-channel partners, business partners, etc.

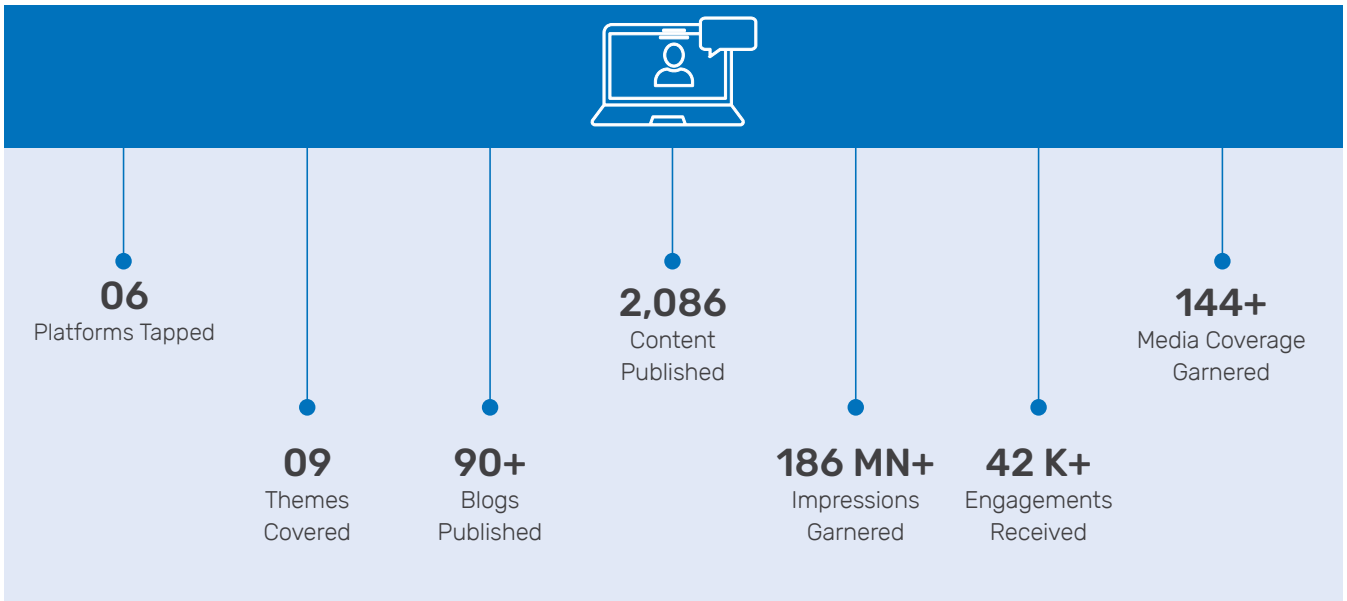
- Trainings are conducted for employees and vendors who use customer-facing application and assets
- To educate customers / users on privacy, security awareness and confidentiality aspects, the Group companies run campaigns on NOT sharing OTP, Fraud alerts, no asking/ sharing of personal details on calls, etc.

Led by a commitment to protecting the privacy of personal data, we have put well-structured privacy policies in place.

- "Fraud Awareness Week" is celebrated during November across insurance companies, with the active participation of Mancom members
- Training for law enforcement agencies, such as Police, on Insurance Frauds, creating awareness among them and an environment of deterrence among fraudsters
- Cautionary Note for customers on being ' Beware of spurious calls', and Fraud Prevention Tips on the website for all stakeholders
- In addition, awareness campaigns were conducted during the year for fraud prevention, cyber security and data privacy by the Group companies, more than 63,000 hours of training were provided to permanent employees

'Be Cyber Safe' Campaign

Deployed a 360-degree customer awareness campaign for RBI's cyber security awareness drive throughout October 2021.



Fraud Awareness Campaigns

Group companies conduct various campaigns to create awareness amongst its employees, customers and value chain partners. Insurance Subsidiaries celebrated International Fraud Awareness Week from 14th to 20th November, 2021 with the intention of creating an anti-fraud awareness among our distributors and customers alike. Key highlights of some of the campaigns have been presented below:

'Savdhaan Rahein. Safe Rahein'

Our fraud awareness focus encompasses targeted initiatives and programmes covering customers and employees. It covered fraud themes of loans, fake profiles, ads on social media, UPI, vishing, phishing, SMS, lottery/ offers, job and insurance frauds. The Group's Fraud prevention awareness campaign was recognised with Gold at Adgully's Digixx 2022- BFSI services sector.

Fraud Prevention | Savdhaan Rahein Safe Rahein - Key Highlights

Input

10+ Platforms Tapped	**10+** Themes Covered
130+ Blogs Published	**10,000** Content Published

Output

343MN Impressions Garnered	**15MN** Engagements Received
167MN+ Video Views Achieved	**500** Media Coverage Garnered

Click images to watch the video

Business Continuity Management

All Group companies have in place a business continuity strategy and framework, which is also compliant with applicable regulatory requirements. BCP envisages the likely disruptive events, as well as their probability and impact on business operations. The impact is assessed through business impact analysis. The process is aimed at eliminating or minimising any potential disruption to critical business operations.

The BCP includes Disaster Recovery procedures to quickly recover from an emergency. Annual BCP drills and reviews are conducted to ensure that the BCP is effective given the current nature of business processes, infrastructure, personnel, etc.

Fraud Risk Management

To check any fraudulent activities across our business operations, we closely assess the various fraud risks to which we are exposed. Our anti-fraud programme is crafted to prevent such risks. Fraud risk audits are conducted at least annually. Fraud risk policies and frameworks are also reviewed annually. Fraud risks are monitored at least quarterly and have Board oversight through Audit Committee, Risk Committee and Whistle Blower Committee.

Insurance Subsidiaries celebrated International Fraud Awareness Week from 14th to 20th November, 2021 with the intention of creating an anti-fraud awareness among our distributors and customers alike.