Information Security, Cyber Security and Fraud Controls

Information has emerged as an asset in this technological age regardless of its source and nature. A robust control over information security, cyber security and fraud is a requisite part of operational risk management framework to be able to continuously manage risk to systems, networks and databases from cyber-attacks and threats. The Information Technology (IT) system controls and processes established assist to obviate any disruptions and security threats which might endanger customer data and lead to disruption in business operations.

Information Security

Bajaj Finserv companies have a comprehensive IT framework which inter alia covers governance, policy, operations, security, audit, outsourcing and Business Continuity Plan (BCP) to overcome the threats and challenges pertaining to information security, cyber security, and fraud.

The Group companies have adopted information security frameworks to establish, implement, monitor, and constantly improve its information security posture. Bajaj Finserv and its material subsidiaries wherever applicable are compliant with:

- ISO 27001:2013 Information security management system
- ISO 22301:2012 Business Continuity Management system
- RBI's[1] Master Direction on Information Technology Framework
- NHB's[2] Policy circular on Information Technology Framework
- IRDAI's[3] Guidelines on Information and Cyber Security
- SEBI[4] compliant Cyber Security and Resilience Framework

To protect systems and data against the threats in "remote work environment" Bajaj Finserv Group has also implemented Data Loss Prevention (DLP) solutions such as:

- Endpoint & Email DLP
- Conditional access to Office 365
- Global protect (VPN) access on Business Applications
- Mobile Device Management (MDM) for corporate mobile apps

All data protection controls are improved, enhanced periodically, and evaluated at least once a year.

Cyber Security

Cyber security policies and practices have been institutionalized with the aim to protect information infrastructure on the internet; prevent and respond to cyber threats, reduce vulnerability, and minimize damage from cyber incidents. A combination of resolute teams, processes and technology enables the successful realization of these objectives. Few examples of the operational measures to monitor and respond to data breaches and cyber-attacks are:

- Security operations center: managed by reputed cyber security service providers
- Threat hunting: managed by reputed cyber security service providers and by in-house team.
- Surface Web and Dark Web monitoring: conducted through service providers, and
- Customer related fraud events: detected, managed, and mitigated through risk control unit along with cyber risk team

> “In today's interconnected world, cybersecurity is the foundation for building trust and confidence in the digital age. It requires collaboration and cooperation from all stakeholders. Investing in cybersecurity is not just a cost, it's an investment in the future resilience and sustainability of our organization. A strong cybersecurity posture is not only a defensive measure; it's a competitive advantage that instils trust and confidence in customers and partners.”
>
> **Anurag Chottani**
> Chief Technology Officer,
> Bajaj Finance Ltd.

Data Privacy

Led by a commitment to protect the privacy of personal data, we have formulated a well-structured Data Privacy Policy which incorporates:

- 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.
- Collection and processing of user data that is limited to the stated purpose.
- Commitment to notify data subjects in a timely manner in case of policy changes or data breach.
- If any employee discovers data breach incidents, they can be reported on resolute email id.

Ensuring Personal Information Privacy

- The Customers' Personally Identifiable Information (PII) is masked in the core systems and customer facing systems.
- Access to customer PII is restricted and access is granted on a need-to-know basis with due approval.
- Privacy terms are displayed on the website of the Company. It covers details regarding consent, collection, use, sharing, processing, and retention of customer data. Any changes to the Privacy Terms are updated on the Company's website, where the customers can also raise their concerns.

The Company has zero tolerance for breach of data confidentiality and privacy. The Company has defined actions, ranging from suspension, to termination, penalty, legal action, etc. for noted instances of data breach.

[1] RBI - Reserve Bank of India

[2] NHB - National Housing Bank

[3] IRDAI- Insurance Regulatory and Development Authority

[4] SEBI - Securities Exchange Board of India

Audits and Assessments

Bajaj Finserv companies undertake regular audit and assessment 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.
- The system and process audits conducted at the company, but not limited to are as below:
    i. ISO 27001:2013 Information security management system
    ii. ISO 22301:2012 Business Continuity Management system
    iii. Red Team exercise for internet facing systems and IT Infrastructure
    iv. Audits required as per the applicable regulatory requirements

Business Continuity Management

Bajaj Finserv's material subsidiaries have a robust and resilient business continuity strategy and framework which is also compliant with regulatory requirements. BCP envisages disruptive events, their probability and impact on business operations which is assessed through business impact analysis. It aims to eliminate or minimize potential disruption to critical business operations.

BCP includes Disaster Recovery (DR) procedures to quickly recover from an emergency. DR plan includes planning, developing, and implementing disaster recovery management for IT services. Annual BCP drills ensure that it is effective given the current nature of business processes, infrastructure, personnel, etc.

Governance Structure

In the case of material subsidiaries, a committee reviews the IT security-related projects and operations, under the oversight of the respective company's Board. The committees meet at least on a half-yearly basis and the functions of such committee is to formulate an IT strategy and related policy documents, to ensure that the IT strategy is aligned with business strategy, review IT risks, etc. Resolute teams manage the cyber security programme and operations for digital initiatives.

> “We have been assumptively working on fraud management using various aspect of digital technology and ecosystem integration to enhance customer experience and at the same time protect customer's long-term benefits. Fraud management is part of our sustainable business processes and starts at initial phase of customer onboarding process through digital integrations with various internal databases as well as external / third-party services. These arrangements ensure pre-emptive check and balance around insurable interests, financial viability and other early detectors. Capturing live photo of customer during onboarding journey and providing digital platform to independently validate customer's chosen Life Goals solution – ensures trust and transparency during the whole process.”
>
> **Goutam Dutta**
> Chief Technology Officer,
> Bajaj Allianz Life Insurance Company Limited

Awareness and Training

Bajaj Finserv companies use multiple channels, such as classrooms, mails, posters, chronicles, brochures, etc. to create cyber security awareness across stakeholder communities, including employees, value-channel partners, business partners, etc.

- Training is conducted for employees and vendors who use customer facing application and assets.
- To educate customers / users on privacy, security awareness and confidentiality aspects, we run campaigns on fraud alerts, no asking / sharing of personal details on calls, etc.
- Training for law enforcement agencies, such as Police, on Insurance Frauds, creating an awareness among them and an environment of deterrence among fraudsters

For example, “Information Security Awareness | Know the infosec guidelines” by Bajaj Finance created awareness amongst its employees on importance of information security on following topics:

- Password security
- Phishing attack
- Mobile security
- Prevent Malware
- Beware of social engineering
- Clear desk and clear screen
- Printouts
- Data security
- End user security
- Internet usage – controlling access for safety and security
- Email security

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 policies and frameworks are reviewed annually. Fraud risks are monitored at least quarterly and have Board oversight through Audit Committee and Risk Management Committee of the Board of Bajaj Finserv and material subsidiaries.

Our four pillars of Fraud Risk Strategy are:

- Prediction & Prevention: Financial controls for areas with a potentially higher risk (e.g., estimates, revenue recognition, non-standard journal entries and manual journal entries), as well as controls over the financial reporting process, and the possibility of management override
- Detection: Predictive - Preventive Analysis, Early Warning Signals Default Investigation
- Response: Investigations and Strict Consequence Management, FIRs, and Police Complaints
- Collaboration: Industry Collaboration, Regulatory collaboration – black listers the fraudsters and misinformation spreaders

Campaigns and Awareness

Bajaj Finserv companies conduct various campaigns to create awareness amongst their employees, customers, and value chain partners. Some of the campaigns and awareness programs run during were:

Gupta ji ki Path Shala

This was an employee awareness campaign which highlighted the importance of using official lines to make promotional calls as well as raising service requests and the consequences of not doing so. Gupta Ji, our mascot, came to the rescue and through various offline and online media did an education series where a step-by-step process video on how to raise a service request was also displayed.

Savdhaan Rahein Safe Rahein

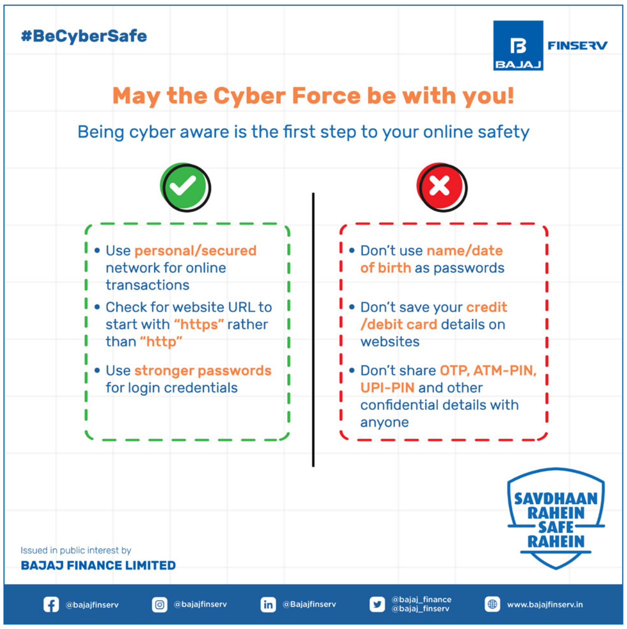
The public awareness campaign 'Savdhaan Rahein Safe Rahein,' was launched across digital and social media platforms. It not only made customers aware of financial fraud risks and how to stay protected but also empowered them with simple tips to differentiate between a genuine Bajaj executive and an unauthorized agent.

BALIC celebrated Fraud Awareness Week

The Company celebrated International Fraud Awareness Week from 14th to 18th Nov 2022 with the intention of creating an anti-fraud awareness among our distributors and customers alike.

Cyber Jagrookta

To caution people against the modus operandi of financial fraudsters and the kinds of prevalent cyber frauds, BFL, under the initiative of MHA, launched a social media awareness campaign called "Cyber Jagrookta Diwas". The campaign focuses on sharing tips on safe digital actions and staying alert. It aims to train the public to adopt cyber hygiene habits and become empowered to responsibly manage situations involving potential cyber-crimes.



#BeCyberSafe

BAJAJ FINSERV

May the Cyber Force be with you!

Being cyber aware is the first step to your online safety

✓

- Use personal/secured network for online transactions
- Check for website URL to start with "https" rather than "http"
- Use stronger passwords for login credentials

✗

- Don't use name/date of birth as passwords
- Don't save your credit /debit card details on websites
- Don't share OTP, ATM-PIN, UPI-PIN and other confidential details with anyone

SAVDHAAN RAHEIN SAFE RAHEIN

Issued in public interest by
BAJAJ FINANCE LIMITED

@bajajfinserv @bajajfinserv @Bajajfinserv @bajaj_finance @bajaj_finserv www.bajajfinserv.in

Bajaj Allianz Life Insurance Company Launched a Fraud Awareness Booklet

This handbook, which is available on the website, communicated through social media and circulated within our sales team is to create awareness and keep forewarned, our valued customers, distributors, and internal teams, against possible fraudulent activity and modus operandi suggesting ways to mitigate such actions and practices.

#BeCyberSafe G20

BAJAJ FINSERV

http://paisakarodoublefatafat.com
iss link par click kariye aur
25 din mein
aapka paisa double

Aise messages dein sakte hai aapko trouble!

SAVDHAAN RAHEIN SAFE RAHEIN

Issued in public interest by
BAJAJ FINANCE LIMITED

@bajajfinserv @bajajfinserv @Bajajfinserv @bajaj_finance @bajaj_finserv www.bajajfinserv.in