Manufactured and Intellectual Capital

Cyber Security, Data Privacy and Information Security

As custodians of customer information, protecting data is a fundamental responsibility. Our security architecture and data protection practices are built around confidentiality, consent and compliance. In an increasingly digital economy, we remain committed to ensuring that every interaction with Bajaj Finserv meets the highest standards of privacy and protection.

Anurag Chottani,
Group Head—AI,
Bajaj Finserv

At Bajaj Markets, we build trust in a financial marketplace through simpler product discovery, intuitive digital journeys, and stronger fraud awareness. This helps millions of consumers compare options, make informed, confident choices, and select solutions that best meet their needs.

Ashish Panchal,
MD and CEO, Bajaj Finserv Direct Ltd.
(Bajaj Markets)

The BFS group is known for actively adopting new technologies to enhance its operations and services. At the BFS group, digital resilience is a strategic imperative. While the Group is focused on taking lead in new technology adoption, we are equally committed to data privacy and cybersecurity, ensuring full compliance with regulatory frameworks. Through robust policies, regular audits and employee training, we proactively safeguard customer data and ensure uninterrupted business continuity.

UN SDGs Aligned

Material Topics Impacted

- Data Privacy and Security
- Innovation, Digitisation and Responsible Use of Technology (AI Governance)
- Risk Management
- Marketing and Selling Practices

Building Digital Resilience

We have created layered technical controls and a workforce trained to treat security as a personal responsibility as we constantly work to stay ahead of threats that grow more sophisticated each year. Suppliers and service providers who handle customer or sensitive data are required to meet our data protection standards. Their compliance is verified and monitored through structured vendor assessments, in addition to contractual safeguards.

Key Highlights for FY2026

Zero

Cyber security and Customer data breaches recorded in FY2026

300+

Total AI projects conceived, with more than 100 fully deployed

250+

Data and technology professionals driving the FinAI and InsurAI agenda across the Group

₹60+ crore

Insurance revenue generated through AI-driven propensity scoring and behavioural insights

₹1,500–2,000 crore

Planned investment over five years in AI innovation startups under Finserv Intelligence

₹5,520 crore

Loan disbursements directly catalysed by advanced AI models in FY2026

Cyber Security Measures

A dedicated Cyber Security Operations Centre (CSOC) provides 24x7 real-time monitoring of threats and security events across the Group.

Comprehensive internet surveillance, including dark web monitoring, to identify data breaches and emerging threats.

- Proactive alerts for anomalous email activity and unauthorised sensitive data sharing, enabling rapid containment.
- Mobile Device Management (MDM) ensuring consistent security policies across all endpoints: laptops, desktops, tablets, and mobile applications.
- Internet access to business applications is secured through Proxy-based access controls and Virtual Private Network (VPN) solutions. Regular internal audits to periodically evaluate and strengthen data protection practices.
- BFL conducts periodic cyber drills as a preparedness for all relevant stakeholders towards cyber resilient environment.
- Board Risk Committee oversight encompassing the review of controls, threats, and breach response preparedness ensuring accountability at the highest level.

No cyber security breaches were recorded in FY2026.

Cyber Security Governance and Audits

At Bajaj Finserv group, cyber security is embedded across our business units and subsidiaries. Cyber security and information security risk updates are reported to the Board through the IT Strategy Committee and Risk Management Committee on a periodic basis, covering the threat landscape, control effectiveness, material incidents and regulatory readiness.

The Group conducts comprehensive internal and external assessments on a regular basis to prevent, detect and mitigate cybersecurity risks. These include:

- Internal audits, vulnerability scans and penetration tests across both network and application layers.
- Annual third-party audits conducted across entities to assess maturity across all companies.
- ISO surveillance audits and adversarial Red Team exercises on critical digital assets.
- All assessment findings are systematically used to strengthen threat detection and response capabilities.
- Audit observations from internal and third-party reviews are tracked through defined remediation processes with clear ownership and timelines to ensure continuous improvement in controls and governance.

Business Continuity and Operational Resilience

Financial services are essential services. Our customers depend on us being available, reliable and secure all the time. Our Business Continuity Management Strategy framework is built around that expectation.

The Group maintains a robust, regularly tested, Business Continuity Management (BCM) strategy encompassing:

Disaster Recovery (DR) procedures with defined Recovery Time Objective (RTO) and Recovery Point Objectives (RPO) designed to minimise customer-facing disruptions in all scenarios.

- Periodic DR drills with formal documentation of outcomes, findings and corrective actions.
- DR infrastructure integrated with Security Information and Event Management (SIEM) platforms enabling real-time threat monitoring and event correlation across environments.
- Business Continuity Plan (BCP) drills with findings incorporated regularly for continuous improvement actions each year.

Governance and Oversight

- Board Risk Committees of material subsidiaries maintain active oversight of cyber security posture, IT risk and incident response readiness.
- Dedicated in-house teams and specialist partners partner provide continuous 24x7 monitoring of cyber operations with defined escalation protocols.
- Group-level accountability for data privacy governance is vested with a designated senior official.
- All subsidiaries follow ISO-aligned frameworks to implement, monitor and improve cyber security practices.

Advanced Security Systems

Across the Group, subsidiaries deploy a layered set of advanced security capabilities:

- Security Operations Centres (SOC) managed by third party security experts, providing continuous monitoring and rapid incident response.
- Continuous surface and dark web monitoring to identify data exposure, credential leaks and threat intelligence relevant to the Group.
- Dedicated Risk Containment Units (RCUs) leveraging advanced analytics and investigative capabilities for real-time fraud detection and prevention.

Internal Protections

- Continuous vulnerability management through regular threat scanning, structured tracking of remediation, and verified closure by a dedicated team.

Periodic independent audits of IT infrastructure and the information security management system by external auditors.

- Event-driven penetration testing across critical networks, systems, and applications following major releases, updates or enhancements.

Simulated cyberattack exercises (Red Team assessments) conducted by external agencies to validate the effectiveness of security controls.

Data Privacy Framework

We uphold a zero-tolerance policy for breaches of data confidentiality and privacy. Each Group Company enforces stringent data privacy controls with well-defined accountability frameworks and with consequences for non-compliance. Privacy is treated as a shared responsibility across functions.

Key Data Privacy Practices

+ All customer data is collected lawfully, with full transparency and explicit user consent, in line with applicable regulations. Clear disclosures are showcased to customers on how their data is used, shared and retained as part of our privacy policy and consent framework.
+ Defined policies and procedures for limited-purpose data processing. Mandatory breach reporting protocols and stakeholder notification procedures are maintained across entities.
+ A Group-wide privacy policy governed by dedicated privacy teams and integrated with our compliance management systems.

No customer data breaches were recorded in FY2026.

Customer Data Rights

+ The Company safeguards customer personal data by ensuring its collection, use, storage, and sharing are conducted transparently, securely, and lawfully through robust technological, administrative and organisational controls, protecting against unauthorised access, misuse and loss.
+ Customer information is collected solely to deliver products and services and to fulfil legal obligations, in accordance with policies ensuring confidentiality and integrity.
+ Purposeful customer consent is obtained prior to the collection and use of personal data, with a separate mechanism available for consent modification, and an opt-out option provided specifically for non-essential communications, along with defined processes for consent withdrawal. Customers may request deletion of personal data through the Company's Digital Platforms and service channels, addressed in accordance with applicable regulatory obligations and defined timelines.
+ Customer data is retained for defined periods across categories, including KYC documents, loan files, and transaction records, governed by retention schedules aligned with legal and regulatory requirements, with subject to secure disposal upon expiry.
+ Data sharing is limited to lawful and regulated third-party disclosures and is protected in accordance with applicable privacy laws and Group-level regulations. Any secondary use of customer data requires formal approvals, defined controls, and monitoring through established tracking mechanisms.

Preparing for the DPDP Act 2023

The Group is evaluating the requirements of the Digital Personal Data Protection Act, 2023 and its impact on existing policies and processes, and is proactively preparing for compliance through a structured cross-functional programme that includes:

+ Establishment of cross-functional working groups across IT, Legal and Compliance functions of all Group entities.
+ Development of SOPs and detailed process maps covering data discovery, access management and privacy governance.
+ All material subsidiaries have published Board-approved privacy policies on their respective websites.

Customer Data Retention and Access

To ensure trust and compliance, the Group has implemented the following practices:

+ Data retention periods are determined based on legal, regulatory and business requirements, with secure disposal upon expiry of defined retention timelines.
+ Regular compliance audits to assess adherence to data retention and policy standards.
+ Strictly enforced, role-based access protocols for all sensitive customer information.
+ Industry-leading practices across Group Companies for secure storage, retrieval and disposal of customer data.

Our Commitment to Consumer Financial Protection

At the BFS group, consumer financial protection is a foundational commitment. We deliver prompt, efficient and personalised services with strict adherence to compliance, fairness and transparency.

During the year, over 2.3 lakh employees—98%* of our workforce—were trained in FY2026 on data privacy, cybersecurity, and consumer protection.

*Both permanent employees and other-than-permanent employees are included in the reporting. While other Group companies cover consumer finance under broader training modules, BFL has implemented a specialised and focused Consumer Finance training programme for the entire workforce, resulting in approximately 98% compliance of the workforce

We are guided by the following principles:

Customer Rights

Customers may access and rectify their personal information through our digital platforms (App and Web) or via our contact centres with robust authentication safeguards in place.

Data Usage

Our Data Privacy Policy, available at all material subsidiaries on their respective websites outlines that, customer data is used for legitimate purposes and is not sold or shared with third parties, except for completing transactions/services.

Retention Policies

Data retention policies and durations are clearly defined in Board-approved policy, accessible on the public domain.

Information Security and Policies

The BFS group operates under a comprehensive IT governance framework to secure customer data and ensure operational continuity.

The Group maintains a unified security framework through its Group Information Security and Group Cyber Security policies, applicable to all group entities. This framework governs all business information, IT infrastructure, and data processing facilities, extending to customers, employees, and third parties to ensure standardised security protocols across all digital and physical touchpoints.

All material subsidiaries are aligned with regulatory requirements and certified under:

+ ISO 27001:2022 – Information Security Management System.
+ ISO 22301:2019 – Business Continuity Management System.
+ Payment Card Industry Data Security Standard v4.0.1 – For Wallet Environments.

Additional frameworks followed (as applicable) include:

+ RBI's Master Direction on Information Technology Governance, Risk, Controls and Assurance Practices.
+ The National Housing Bank's IT guidelines for HFCs.
+ IRDAI's cybersecurity guidelines and Insurance Self-Network Platform (ISNP) framework.
+ SEBI's Cybersecurity and Resilience Framework.
+ National Payments Corporation of India.

Remote Work and Data Security Controls

+ To protect the security of remote and hybrid work environments, the Group has developed and implemented a comprehensive suite of advanced controls.
+ Remote access to corporate infrastructure is controlled via secured VPN.
+ Endpoint, Network and Email Data Loss Prevention (DLP) tools to prevent unauthorised data exfiltration.
+ Endpoint Detection and Response (EDR) providing real-time protection against malware.

+ Conditional access controls governing authentication and authorisation for Office 365 and all corporate digital assets.
+ Formally documented and Board-approved Cyber security, IT and Data Privacy policies in all subsidiaries.

Data Privacy and Personal Information Protection

+ The Group enforces a zero-tolerance policy on data breaches and maintains structured, auditable processes to ensure compliance:
+ Lawful, consent-based collection and limited processing of user data.
+ Transparent privacy policies and timely user notifications.
+ Customer privacy concerns addressed through cyber cell units.
+ Strictly restricted and encrypted access to Personally Identifiable Information (PII).
+ Continuous employee training programmes and proactive customer education on data rights and digital safety.
+ Zero data breaches reported in FY2026.

Awareness, Training and Culture Building

Recognising that people are both the greatest vulnerability and strongest line of defence in cyber security, the Group fosters a culture of awareness and vigilance through:

+ Employee and vendor training on key systems and risks
+ Targeted customer awareness campaigns on digital hygiene, safe financial behaviour and fraud prevention
+ Collaborative sessions with law enforcement agencies on emerging fraud patterns (e.g. insurance frauds)
+ Our specialised IT awareness programmes cover essential topics such as:
  - Password and email security
  - Phishing
  - Malware prevention
  - Mobile safety
  - Social engineering
  - Clean desk practices

Cyber Security Awareness Campaigns

Our subsidiary, Bajaj Finance Ltd. (BFL), executed a structured, multi-vertical customer awareness programme in line with the Reserve Bank of India's (RBI) customer awareness guidelines. The campaigns focused on promoting cyber safety, responsible financial behaviour, and informed decision-making across seven key themes:

+ Account Operations
+ Avenues of Redress
+ Charter of Customer Rights
+ Digital Banking
+ Digital Frauds
+ Facilities for Senior Citizens
+ Loans

The awareness programme was delivered through targeted digital campaigns spanning six customer-facing verticals, with content customised to address the specific needs of each business function.

Campaign Themes Across Business Verticals

Risk Containment Unit (RCU)

Focused on strengthening customer awareness around account security, cyber fraud prevention, safe digital banking practices, grievance redressal mechanisms, senior citizen protection, and responsible loan-related transactions. Campaigns addressed emerging frauds such as fake APKs, upfront fee scams, Insta EMI Card fraud, investment scams, impersonation fraud, and phishing.

Debt Management Services (DMS)

Promoted responsible borrowing and repayment behaviour by educating customers on repayment discipline, EMI management, credit scores, credit reports, loan tenure, Days Past Due (DPD), proof of payment, and maintaining healthy credit practices.

Service

Enhanced customer awareness around account servicing, KYC updates, digital servicing channels, transparent fees and charges, secure digital banking, document access, grievance redressal, financial literacy, credit awareness, and digital inclusion for senior citizens.

Fixed Deposits (FD)

Focused on helping customers manage deposits efficiently through awareness on TDS, nominee updates, maturity processes, renewals, digital document access, unclaimed deposits, premature withdrawals, and dedicated benefits and support for senior citizens.

Insurance

Educated customers across the insurance lifecycle, including policy renewal, claims processes, policy conditions, nominee updates, premium payments, and digital access to policy documents, enabling informed insurance decisions.

Payments

Promoted secure digital payment practices through awareness on cyber frauds, fake advertisements, identity theft, unauthorised transactions, safe UPI usage, two-factor authentication (2FA), third-party app fraud, online shopping scams, and cybercrime reporting.

Targeted hyperlocal campaigns were delivered across Meta (Facebook and Instagram) and YouTube in multiple regional languages, including Gujarati, Tamil, Telugu, Kannada, Marathi, and Bengali, improving accessibility and customer outreach. During the year, Fixed Deposits and Payments were introduced as dedicated focus areas under Operational Risk Management (ORM), further expanding the programme's customer awareness initiatives.

Visual Messaging (Poster Campaigns and Creatives)

The following creatives were deployed across social media and digital platforms as part of Bajaj Finance Ltd.'s customer awareness programme. Designed in simple, relatable language, these campaigns translated complex financial concepts and cyber security risks into easy-to-understand messages that encouraged customers to make informed and secure financial decisions.

Keep Your Account Active, Keep It Secure

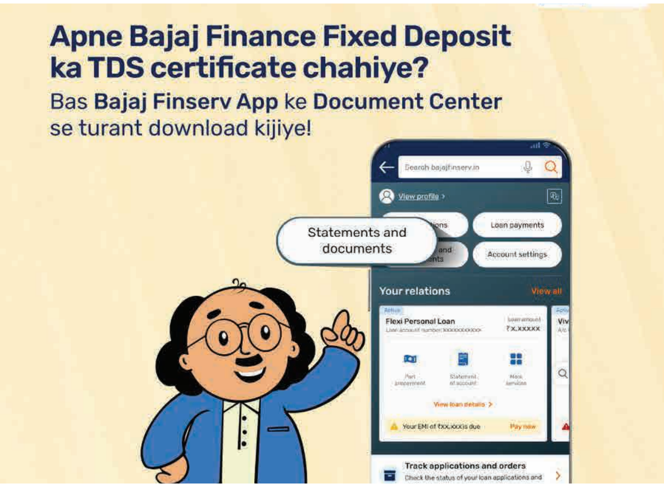
This campaign highlighted the risks associated with inoperative accounts and encouraged customers to stay vigilant by regularly monitoring account activity and protecting sensitive credentials.

Know Your Credit Report. Decoding Days Past Due (DPD)

This campaign educated customers on the importance of Days Past Due (DPD) as a key indicator of repayment behaviour in credit reports. By simplifying financial concepts, it encouraged timely repayments and empowered customers to build and maintain a healthy credit profile.

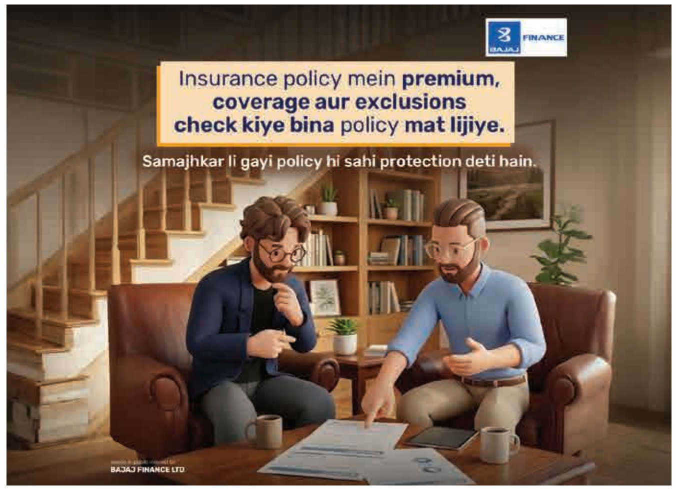
Smart Banking Starts Here

This campaign encouraged customers to securely access important financial documents, including TDS certificates, through Bajaj Finance's digital channels, making account management faster, simpler, and more convenient.



Know Your Insurance Policy

This campaign encouraged customers to understand key policy features, including coverage, exclusions, and premium terms, empowering them to make informed insurance decisions and avoid surprises during claims.



Transforming Financial Ecosystems through Advanced AI Capabilities

As a Core Investment Company, Bajaj Finserv Ltd. drives long-term value creation across its subsidiaries by fostering a robust, future-ready digital ecosystem. In FY2026, our technology framework evolved significantly through the deployment of specialised FinAI and InsurAI platforms across the Group. FinAI and InsurAI remain central to our long-term vision. The phase-wise implementation across businesses and functions has begun to show early signs of costs and productivity benefits. We are on track to become a future-ready financial services company.

Managed as a horizontal capability across the BFS group, we now deploy a dedicated team of over 250 data and technology professionals to drive FinAI and InsurAI agenda across the Group. This next-generation architecture spans Enterprise AI (Voice, Text, Vision, and Business Intelligence), Consumer AI, Agentic AI and Data AI.

With over 300 total projects conceived and more than 100 fully deployed, this technological transition from process-centric automation to goal-oriented autonomy has realised material economic and operational impacts. In FY2026 alone, these advanced AI models directly catalysed over approx. ₹5,520 crore in loan disbursements and generated more than ₹60 crore in insurance revenue through highly personalised propensity scoring, behavioural insights and optimised credit-risk profiling.

Bajaj Finserv Intelligence

The Company has launched 'Finserv Intelligence', a Group-wide initiative focused on applied research and innovation in areas such as AI, cyber security, quantum technologies and digital financial services. This initiative aims to invest ₹1,500-2,000 crore over five years in AI innovation startups, from seed to Series B, and is partnered with IIT Bombay to establish a joint research centre. The initiative is structured with a five-to-ten-year horizon and focuses on building scalable technology solutions for India and the world.

Bajaj Finserv's commitment to technology adoption is reflected in its strategic focus on foundational digital public infrastructure and AI capabilities in India. The Company aims to leverage these technologies to create a set of high technology, scalable, secure, and low-cost solutions for India and the world.

The initiative is structured with a five-to-ten-year horizon and will operate through a mix of research labs, centres of excellence, venture-led models and academic collaborations. It aims to bridge the gap between academia, industry and national priorities by bringing together research institutions, startups, and in-house specialists under a single innovation ecosystem.

Bajaj Finserv's technology adoption strategy is a strategic bet on in-house technology development and aims to create a deployment platform on a national scale. The initiative is designed to support high-tech, low-unit-cost, highly scalable solutions developed in India for both the domestic and global markets.