EXTERNAL-FACING PQC READINESS VALIDATION

Practical first phase for Bajaj Finance Limited

Prepared by QuReady
The specialist post-quantum cybersecurity practice of Quant Dev Pte. Ltd.
August 2026

Objective

Validate and operationalise post-quantum protection across selected internet-facing traffic paths, using Bajaj's existing Cloudflare and Akamai architecture wherever practical.

Vendor-neutral	Low disruption	Measurable
Independent validation across CDN, origin, certificate and client layers.	Start with selected domains and application paths; no estate-wide replacement.	Evidence, configuration findings, compatibility results and a pilot-ready plan.

CONFIDENTIAL

1 | BAJAJ OBJECTIVE

A focused first move, not a full-estate replacement

Based on our discussion, Bajaj is evaluating how to protect long-lived customer and business data against harvest-now-decrypt-later risk while preserving the current operating environment.

Bajaj priority	Implication for the programme
Internet-facing systems first	Begin with domains, Super App/API traffic and the CDN-to-origin path.
Use existing platforms	Validate Cloudflare and Akamai capabilities before adding new infrastructure.
Avoid broad replacement	Prioritise configuration, compatibility and targeted remediation.
Prepare for governance and audit	Create evidence, ownership, an initial CBOM and a phased roadmap.
Move in controlled stages	Validate first, pilot second, then expand to internal systems and long-lived data.

QuReady view

Enabling hybrid ML-KEM at the edge is a strong near-term action. It is not, by itself, proof of end-to-end quantum resilience. The client, edge, origin, certificate, shared-connection and fallback paths must be validated together.

The decision Bajaj needs to make

Which external-facing paths can be protected now, what remains classical, what could break, and what evidence is required before production rollout?

Four phases, each with a decision gate

Phase	Practical work	Decision output
1. Validate	Map selected traffic paths; verify negotiated algorithms, certificates, fallback and coverage.	Go / no-go for a controlled pilot.
2. Pilot	Implement agreed settings and origin changes in a contained production-like scope.	Validated configuration, performance and rollback.
3. Discover	Extend into CBOM, crypto-agility, internal services, code and vendor dependencies.	Prioritised enterprise migration plan.
4. Scale	Execute migration work packages and establish ongoing governance.	Repeatable quantum-resilience programme.

Why this structure works for Bajaj

- It starts with the scope Bajaj has already prioritised.
- It tests existing vendor capabilities before recommending additional products.
- It keeps the first engagement measurable and low-risk.
- It creates an auditable foundation for the subsequent CBOM and internal migration work.

What QuReady does not propose

- A generic awareness exercise or a high-level report without technical evidence.
- Replacing Bajaj's current security stack before its capabilities and gaps are validated.
- Calling a domain fully quantum-safe based on one configuration setting or one scanner result.

3 | PROPOSED FIRST ENGAGEMENT

External-Facing PQC Readiness and Architecture Validation

Client	Cloudflare / Akamai	Origin / API	Application services	Data stores
Browser, mobile, API	Edge TLS and routing	Origin TLS and trust	Service-to-service crypto	Long-lived PII and records

Indicative scope

- 8-12 priority domains or hostnames
- Selected Super App and API paths
- Cloudflare- and Akamai-managed properties
- Representative origin services
- Representative browser, mobile and API clients

Validation activities

- Client-to-edge and edge-to-origin mapping
- TLS 1.3 and X25519MLKEM768 negotiation
- Public and private certificate authentication posture
- Classical fallback, shared connection and bypass scenarios
- Client, origin and middlebox compatibility
- Configuration, rollout and rollback requirements

Delivery boundary

No customer PII

The first phase can be completed without accessing customer records.

No private keys

QuReady does not require Bajaj production private keys.

Controlled access

No production credentials unless separately approved for a later test step.

Concrete outputs for management and engineering

Deliverable	Purpose
Executive readiness summary	Clear status, material risks, priority actions and decisions required.
Traffic-path architecture	Client, CDN, origin and application trust boundaries for the selected scope.
PQC status matrix	Hostname-by-hostname view of key agreement, TLS, certificate and fallback posture.
Vendor configuration review	What Cloudflare and Akamai protect, require or leave outside scope.
Compatibility test results	Representative browser, mobile, API, origin and middlebox behaviour.
Remediation and pilot plan	Prioritised changes, success criteria, rollback and production-readiness steps.
Initial external CBOM baseline	Cryptographic components and dependencies identified in the selected scope.
Audit evidence pack	Methods, evidence and ownership suitable for internal review and programme tracking.

Indicative plan

Timing	Activity
Week 1	Scope confirmation, evidence request and architecture sessions.
Weeks 2-3	Configuration review, external and authorised internal validation.
Week 4	Compatibility, fallback and gap analysis.
Week 5	Draft findings, remediation options and pilot design.
Week 6	Management review, final report and next-phase decision.

Commercial terms: fixed fee following technical scoping and confirmation of the selected hostnames, application paths, stakeholders and evidence sources.

Quantum-ready is not one checkbox

A TLS connection has separate confidentiality and authentication functions. They must be reported independently.

Layer	Current reality	Validation requirement
Key agreement	Hybrid X25519MLKEM768 can protect session establishment against harvest-now-decrypt-later risk.	Validate actual negotiation on each traffic leg and representative client.
Public certificate authentication	Public web certificates commonly remain based on classical RSA or ECDSA trust chains.	Report authentication separately from PQC key agreement.
Edge-to-origin protection	PQC support depends on origin TLS 1.3, library support, certificate/trust configuration and enforcement.	Confirm the negotiated group and authentication mode at the origin.
Fallback and reuse	Classical fallback, persistent connections and shared certificates can leave traffic on a classical path.	Test fallback, reuse, shared-hostname and bypass cases.
Operational readiness	A technically supported feature can still create compatibility, latency or rollback risks.	Use a phased rollout with explicit success and rollback criteria.

Recommended reporting language

Report PQC confidentiality, PQC authentication, protocol posture and coverage separately. Avoid a single unqualified “fully quantum-safe” result when any material part of the path remains classical.

Technical standards and platform references

NIST FIPS 203, 204 and 205; Cloudflare SSL/TLS Post-Quantum Cryptography documentation; Akamai Property Manager PQC Client-to-Edge and PQC-to-Origin documentation. Detailed references will be included in the final assessment methodology.

Independent specialist, named delivery team

Independent	Founder-led	Hands-on
QuReady is not tied to a CDN, firewall, PKI or cloud product sale.	The people in the proposal perform the assessment and present the findings.	Architecture review is paired with protocol testing, compatibility validation and pilot design.

Xavier Macià

Founder and CEO, QuReady
Director, Quant Dev Pte. Ltd.

- Leads client strategy, readiness programmes, governance and executive delivery.
- Technology entrepreneur and hands-on AI/software engineer with more than 20 years across engineering, enterprise technology and product leadership.
- Double MBA: Nanyang Technological University and Waseda University.
- BEng in Communication and Electronics Engineering, Northumbria University.

Alberto Roura

Co-founder and CTO, QuReady

- Leads cryptographic architecture, cloud/network security, technical validation and implementation design.
- Alibaba Cloud Professional certifications in Cloud Security, Cloud Computing and Big Data.
- Alibaba Cloud MVP of the Year and multi-year Alibaba Cloud MVP recognition.
- Builder of cloud, connectivity, security and open-source systems across international environments.

Core team size: two founders. Any additional specialist required by an agreed scope would be named in advance and subject to Bajaj approval.

Corporate profile

Corporate fact	Details
Legal entity	Quant Dev Pte. Ltd.
Operating practice	QuReady - specialist post-quantum cybersecurity services
UEN	202404137W
Incorporated	Singapore, 29 January 2024
Status	Live exempt private company limited by shares
Registered activities	Software and application development; cybersecurity software development
Website	quready.com
Contracting party	Quant Dev Pte. Ltd. for QuReady proposals, contracts, invoicing and delivery

Supplier assurance

Area	Position
Access model	Named team, least-privilege access and Bajaj-approved collaboration channels.
Initial data boundary	No customer PII, production private keys or unrestricted production access.
Organisational certification	Not currently held. Quant Dev is preparing to initiate CSA Cyber Essentials certification in Singapore.
Corporate evidence	Current ACRA Business Profile and incorporation evidence available during formal due diligence.
Confidentiality	NDA and engagement-specific data handling, retention and deletion controls.

Proposed next step

1. One 60-minute scoping session with security architecture, Cloudflare, Akamai, PKI/certificate management and Super App/API security owners.
2. Confirm the selected hostnames, application paths, evidence sources, testing permissions and success criteria.
3. QuReady issues a fixed-scope, fixed-fee proposal and delivery schedule.

QuReady | hello@quready.com | quready.com