BOARD MEMORANDUM · ONE PAGE · DECISION REQUESTED

DOC KIT-20261129-4A133F
FOR Alderbrook Fintech Ltd
UTC 2026-11-29T15:02:58Z

Post-RSA status and 30-day plan

TO Board of Directors, Alderbrook Fintech Ltd

FROM Executive sponsor · security@alderbrook.example

DATE 29 November 2026

STATUS Preparedness review — no confirmed public cryptographic break.

POST-RSA READINESS SCORE

48 /100

PARTIAL EXPOSURE

Transport is largely protected but RSA signatures still sign tokens, certificates or keys somewhere customers can reach. Planning is urgent but bounded.

01 Situation

Preparedness review — no confirmed public cryptographic break. As of 29 November 2026, NIST, the UK NCSC and US CISA have not confirmed a practical break of RSA or elliptic-curve cryptography; current reports are unconfirmed. This memo sets out Alderbrook Fintech Ltd's exposure if RSA, or RSA and elliptic-curve cryptography, stopped being trustworthy, and a 30-day plan to reduce that exposure now. Alderbrook Fintech Ltd is not reporting an incident. Across the 6 providers assessed for alderbrook.example, 4 of 24 cryptographic surfaces document post-quantum protection and 6 still depend on RSA. Providers with RSA in authentication or key custody: AWS, Okta, Stripe, GitHub, SendGrid. Providers with hybrid post-quantum key exchange on transport: Cloudflare, AWS. Current readiness band: Partial exposure.

02 Scope assessed — 6 third-party providers in the alderbrook.example stack

PROVIDER	CATEGORY	TLS KEX	TLS CHAIN	APP AUTH	KMS / HSM
Cloudflare	CDN & Edge	PQ	UNK	UNK	UNK
AWS	Cloud & Compute	PQ	UNK	RSA	PQ
Okta	Identity & Auth	UNK	RSA	RSA	UNK
Stripe	Payments & Fintech	UNK	RSA	PQ	UNK
GitHub	Code & CI/CD	UNK	UNK	RSA	UNK
SendGrid	Email & Messaging	UNK	RSA	UNK	UNK

PQ: NIST post-quantum or hybrid documented. ECC: classical elliptic curve — unaffected by RSA-only factoring, not post-quantum. RSA: exposed under RSA break. UNK: undocumented or not applicable. Counts: 6 RSA surfaces, 4 PQ surfaces across 24 assessed.

03 Budget and authority requested

LINE	WHAT IT BUYS	EFFORT
Inventory and freeze	Complete cryptographic inventory of certificates, JWT and SAML signing keys, SSH keys, DKIM selectors and KMS keys. Freeze new RSA issuance.	10 person-days
Readiness sprint	Plan hybrid ML-KEM key exchange on every endpoint we control, pilot ML-DSA (FIPS 204) for internal issuers, and record which RSA keys would be rotated first. Treat elliptic-curve moves as RSA-only containment, not a post-quantum fix.	25 to 40 person-days
Vendor governance	Issue the supplier letter to every processor, track written migration dates, add PQC clauses at renewal.	6 person-days
Evidence and assurance	Readiness re-score, regulator-ready log of actions, board paper at day 30, customer FAQ kept current.	5 person-days

Decision requested: approve the four lines above as a priority programme, with authority to pause releases that add new RSA dependencies, and name an accountable executive. No production change is forced by a confirmed break today; the plan reduces exposure ahead of one.

04 30-day milestones

DAY	MILESTONE	OWNER	EVIDENCE
D+2	Cryptographic inventory started; every RSA and elliptic-curve artefact tagged with an owner.	Head of Security	Inventory register
D+5	Customer FAQ published; supplier letters requesting written PQC dates issued.	CEO / CTO	Sent log
D+10	Hybrid ML-KEM key exchange enabled where our providers support it.	Infrastructure lead	Scan report
D+15	ML-DSA pilot on one internal issuer and verifier; RSA rotation runbook rehearsed.	Platform lead	Test run
D+20	KMS, SSH, Git signing and DKIM dependencies mapped with rotation order.	Platform lead	Key register
D+30	Readiness re-scored; break-response triggers agreed; board update delivered.	Executive sponsor	Board paper

CUSTOMER LETTER · SEND TODAY · CEO OR CTO SIGNATURE

DOC KIT-20261129-4A133F
FOR Alderbrook Fintech Ltd
UTC 2026-11-29T15:02:58Z

What the end of RSA means for your data with us

FROM Alderbrook Fintech Ltd · security@alderbrook.example

TO Our enterprise customers and partners

DATE 29 November 2026

> You may have seen unconfirmed reports about RSA and elliptic-curve cryptography. No national cyber agency or NIST has confirmed a practical break. We are writing so you know where Alderbrook Fintech Ltd stands before anyone asks.
>
> What we have checked. [CONFIRM: customer data at rest is encrypted with AES-256]. [CONFIRM: connections to alderbrook.example use TLS 1.3]. Where our providers support it, hybrid post-quantum key exchange already protects traffic: Cloudflare, AWS.
>
> What we are doing. We are inventorying every place RSA and elliptic-curve keys sign or protect something in our stack, and we have asked each supplier for a written post-quantum date. [CONFIRM: supplier letters sent on <date>].
>
> What happens next. If a primary source confirms a break, we will write to you the same day with what changed and what we are rotating. Until then this is a preparedness review, not an incident.
>
> If your procurement or security team needs detail, our pre-filled questionnaire responses are available on request at security@alderbrook.example.
>
> **Alderbrook Fintech Ltd** security@alderbrook.example

05 External FAQ — answers you can publish or paste into support replies

Q1 Has my data been breached?

No incident has been identified. [CONFIRM: no evidence of unauthorised access to personal data found in our review dated 29 November 2026]. Reports about RSA and elliptic-curve cryptography are unconfirmed, and an unconfirmed report is not an incident on our infrastructure.

Q2 Is data I sent you in the past exposed?

Not by any confirmed event. If a practical break were confirmed, traffic protected only by classical key exchange would be at risk from anyone who recorded it. Hybrid ML-KEM key exchange protects new traffic where our providers support it.

Q3 Can I still trust your website certificate?

Yes. Certificates for alderbrook.example chain to certificate authorities that use classical algorithms, which remain trusted today. The CA and browser ecosystem controls the timetable for post-quantum certificates.

Q4 Do I need to do anything?

No action is required today. Keep browsers and clients up to date so hybrid post-quantum key exchange is negotiated automatically.

Q5 What will you do if a break is confirmed?

We will write to you the same day, rotate affected keys on a published plan, and keep this page current with dated updates.

DOC KIT-20261129-4A133F
FOR Alderbrook Fintech Ltd
UTC 2026-11-29T15:02:58Z

Eight answers procurement teams are asking for this week

Each response is written in the first person for Alderbrook Fintech Ltd. Bracketed fields are deliberately left for your security lead to confirm. Vendor facts reflect the public documentation snapshot recorded in the footer of this pack; verify anything older than seven days before you sign.

Q1 · TLS key exchange **Do you support hybrid post-quantum key exchange on customer-facing TLS endpoints?**	Providers documenting X25519MLKEM768 hybrid key exchange: Cloudflare, AWS. [CONFIRM: origin endpoints are TLS 1.3 only and refuse static RSA key exchange]
Q2 · Certificate chains **What signature algorithms do your TLS certificates and chains use?**	[CONFIRM: signature algorithm of the served chain for alderbrook.example]. Publicly trusted post-quantum certificates depend on CA and browser roll-out; we track them as an upstream dependency.
Q3 · Application auth **Which algorithms sign your JWTs, OIDC tokens and SAML assertions?**	[CONFIRM: signing algorithms of each token issuer]. We are mapping RSA and elliptic-curve issuers and piloting ML-DSA for one internal issuer.
Q4 · Key management **How are encryption keys protected in your KMS or HSM, and do any depend on RSA?**	[CONFIRM: data encryption keys are AES-256 and wrapped by cloud KMS root keys]. We are recording every asymmetric KMS key and where ML-KEM / ML-DSA (FIPS 203 / 204) support exists.
Q5 · SSH and code signing **Do you still use RSA for SSH access, deployment keys or commit signing?**	[CONFIRM: SSH host, user and deploy key algorithms and commit-signing algorithm]. We are adding post-quantum key exchange (sntrup761x25519 or mlkem768x25519) where OpenSSH supports it.
Q6 · Vendor governance **How do you manage post-quantum readiness across your sub-processors?**	We maintain a cryptographic register for 6 providers across TLS key exchange, certificate chain, application auth and KMS surfaces, scored against public documentation. Providers currently showing RSA in authentication or key custody: AWS, Okta, Stripe, GitHub, SendGrid. [CONFIRM: written requests for migration dates sent to every supplier on <date>]
Q7 · Data at rest and email **Is stored data or email authentication affected?**	No break is confirmed. [CONFIRM: data at rest uses AES-256]. Transactional email providers predominantly sign DKIM with RSA; DKIM is an ecosystem dependency, not a confidentiality control.
Q8 · Timeline and evidence **What is your post-quantum readiness timeline and how can we verify it?**	A 30-day readiness plan with dated milestones and owners. Evidence is available under NDA on request from security@alderbrook.example. [CONFIRM: board approval date]

SUPPLIER LETTER · EMAIL TO EVERY VENDOR IN THE STACK

DOC KIT-20261129-4A133F
FOR Alderbrook Fintech Ltd
UTC 2026-11-29T15:02:58Z

Request for a written post-RSA migration date

FROM Alderbrook Fintech Ltd · security@alderbrook.example

TO Security or account lead at each supplier and sub-processor

RE Written post-RSA and post-quantum cryptography commitments · response requested within 10 working days

Alderbrook Fintech Ltd relies on your service as a supplier or sub-processor. Following the unconfirmed public reports about RSA and elliptic-curve cryptography, our board and our customers require us to document the cryptographic posture of every provider in our stack and to hold written migration commitments from each of them.

We are not alleging an incident on your side. We are asking for the facts and dates we need to complete our own regulatory triage and customer communications, which we are obliged to keep accurate.

We ask you to confirm in writing:

1. Whether any customer-reachable TLS endpoint, API or console still negotiates RSA or classical-only key exchange, and the date by which TLS 1.3 hybrid post-quantum key exchange (X25519MLKEM768) is or will be default.
2. The signature algorithms used on certificates we are served, and your plan and date for ML-DSA (FIPS 204) certificates when the public ecosystem permits.
3. Whether any token, assertion or webhook signature you issue to us (JWT, OIDC, SAML, webhook) still uses RSA, and the date post-quantum signing becomes available.
4. Whether any key that protects our data in your KMS, HSM or vault is wrapped or signed with a classical public-key algorithm, and the rotation date.
5. Whether any SSH, SFTP or Git integration you provide requires RSA keys, and the date non-RSA keys and post-quantum key exchange are accepted.
6. A named contact and a written post-quantum migration plan with dates, which we may share with our customers and regulators.

Please reply within ten working days to security@alderbrook.example. Where a date cannot be given, say so and tell us why; an honest unknown is more useful to us than a vague assurance. We will record your reply in our supplier register and review it at renewal.

Alderbrook Fintech Ltd security@alderbrook.example

Suppliers in this pack's scope: Cloudflare, AWS, Okta, Stripe, GitHub, SendGrid. Send the same letter to every processor not listed here.

DOC KIT-20261129-4A133F
FOR Alderbrook Fintech Ltd
UTC 2026-11-29T15:02:58Z

Deprecation is not a breach: what to do and when to notify

06 Regulatory triage checklist — UK ICO / GDPR · EU DORA · PCI DSS

READ FIRST: DEPRECATION IS NOT A BREACH

No algorithm has been deprecated by a primary source. Record unconfirmed reports as a horizon risk, not an incident. If a break is later confirmed, cryptographic deprecation is the loss of confidence in an algorithm; a personal data breach under UK GDPR Article 4(12) is a breach of security leading to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The first does not by itself constitute the second. Record the assessment either way.

REGIME	WHAT TO DO IN THE FIRST 30 DAYS	TRIGGERS A FORMAL NOTIFICATION ONLY IF
UK GDPR and ICO Arts. 5(1)(f), 32, 33, 34 · ICO breach guidance	☐ Log the unconfirmed reports as a horizon risk with the date and an owner. ☐ Assess whether any evidence suggests personal data was accessed or decrypted; record the conclusion. ☐ Update the Article 32 security measures description and the sub-processor register with migration dates. ☐ Keep the 72-hour clock in mind: it starts when you become aware of an actual breach, not of the deprecation.	Evidence or reasonable belief that personal data was accessed, decrypted or altered through a failure of RSA. Then notify the ICO within 72 hours and affected individuals where high risk exists.
EU DORA Reg. (EU) 2022/2554 Arts. 9, 17 to 19, 28 · RTS 2024/1774 Arts. 6, 7	☐ Update the ICT risk register and the cryptographic policy required by RTS Articles 6 and 7 to reflect the status of RSA. ☐ Review third-party ICT provider contracts and the register of information for cryptographic commitments. ☐ Classify the event under the major-incident criteria; a deprecation alone normally does not meet them. ☐ Document management-body awareness and the remediation plan.	A major ICT-related incident meeting the classification thresholds, for example service disruption or data loss caused by exploitation. Then initial notification within 4 hours of classification and 24 hours of awareness.
PCI DSS v4.0.1 Reqs. 4.2.1, 12.3.3, 12.3.4, 12.10	☐ Record RSA in the cryptographic inventory with its status and a replacement date (Req. 12.3.3). ☐ Confirm cardholder data in transit uses TLS 1.3 with strong, non-RSA key exchange (Req. 4.2.1). ☐ Review technology end-of-life for hardware and software that depends on RSA (Req. 12.3.4). ☐ Inform your acquirer and QSA of the compensating controls and timeline.	Confirmed or suspected compromise of account data. Then follow the Req. 12.10 incident response plan and notify the payment brands and acquirer as contractually required.
Sector and contractual NIS2, FCA / PRA operational resilience, customer contracts	☐ Check contractual security schedules for algorithm-specific commitments and notify counterparties of the plan. ☐ For regulated financial firms, record the event against operational resilience tolerances and the Bank of England / PRA / FCA quantum resilience expectations. ☐ Keep a single dated log of all decisions and letters sent so the record is regulator-ready.	Breach of a contractual notification duty or an incident that threatens an important business service. Apply the relevant regime's clock.

GOVERNANCE TEMPLATE, NOT LEGAL ADVICE

This kit is a governance and communications template prepared from public documentation for Alderbrook Fintech Ltd. It is not legal, regulatory or compliance advice, not a security audit, and not a determination of whether any notification duty has arisen. Statutory references should be confirmed against the current text and interpreted with qualified counsel for your jurisdiction. Degaus Ltd (England and Wales) accepts no liability for reliance on it. Vendor facts reflect the PostRSA public-documentation snapshot named in the generation record and may change.