01 / UNDERSTAND THE NOTICE

A supplier incident. Your closure decision.

A working brief for customer security, IAM and service-desk teams.

The current disclosure

On 30 October, Chainalysis reported access to user IDs, names, emails and role labels. Its investigation had found no indication of access to specified credentials or investigation content. Organisation-level record scope was still being determined.

Our assessment: identity context still matters

A name, employer and role can make a fraudulent reset request sound credible. This is a plausible follow-on risk, not a claim that such activity has occurred. Assess your own exposure before deciding the response.

Source: Chainalysis, "Security Incident Information", 30 October 2026. Investigation ongoing at source review on 2 November.

chainalysis.com/blog/security-incident-october-30/

02 / RUN A PROPORTIONATE REVIEW

Four checks. Four pieces of evidence.

MicroApz suggested workflow for customers; adapt it to your own incident process.

01 Confirm the affected population

SUPPLIER OWNER

Request the organisation-specific record breakdown through a known contact. Retain the reply and unresolved scope questions.

02 Brief the people handling resets

SERVICE-DESK LEAD

Reconfirm established identity-verification steps. Retain the briefing and a sample check that staff use known channels.

03 Check authentication signals

IAM / SOC

Review unexpected reset requests and MFA prompts for the scoped users and review period. Record queries, timestamps and findings.

04 Make and record the decision

INCIDENT OWNER

Verify two-factor authentication status. Escalate suspicious activity; record what remains unknown, the next review and its owner.

03 / COPY THE RECORD

Give leadership a decision, not a headline.

Illustrative template only. Replace every bracketed field with verified internal evidence.

Supplier-incident review record

Scope	[Supplier] / [affected users] / [review period]
Evidence	[Supplier reply] + [IAM query] + [desk briefing]
Finding	[Observed result] / [coverage or retention gap]
Decision	[Open / escalate / close] + [reason]
Accountability	[Owner] / [next review time] / [approval]

Use this in your leadership update

"We reviewed [population] over [period]. Evidence shows [finding]. We still need [missing evidence]. [Owner] will complete [action] by [time]. Our current decision is [status], for [reason]."

Do not close solely because passwords were not reported exposed. Do not report absence of suspicious events without a completed, scoped review.