Cardholder Information Data Breach : PCI DSS Incident Response Plan

Detection of Breach

Alert of potential breach received from either:
A) Automated system monitoring (ITS)
B) Member of staff
C) Customer / Student
D) University acquirer or other external provider

Has the alert reached been officially reported to the Finance Service Desk?

Report incident to the Finance Service Desk on 01273 877172

Does the incident involve a PDQ or university owned device?

Yes

No / Unknown

Initial Investigation And Control (first two hours)

Check that the device has been physically secured, labelled as not in use and removed from the network, but the power supply retained.

Contact other members of incident response team and book a meeting room.

Create a new incident report log and complete known information..

Assign a member of the incident response team to record all actions, discoveries and discussions from this point forward.

Perform root cause analysis to ascertain how breach arose and asses current impact

Inform line managers in areas affected / possibly affected, to be vigilant

Dispatch a member of the team to inspect possibly affected physical components and secure as necessary.

Acquire copies of machines / system logs possibly involved and examine for typical indications of malicious activity. Begin to investigate and identify suspicious changes.

Member of Staff to inspect Firewall Rules and Access Control List for unexpected changes / vulnerabilities / alerts.

Begin monitoring media outlets for evidence of external reports of the incident.

Ongoing Investigation

Do the team believe a breach / compromise may have occurred?

Yes / Possibly

No

Record that there is no evidence a breach has occurred. Inform all members of staff in affected areas.

Reporting (within 24hrs)

Incident Controller to contact University acquirer (Global Payments) and pass on all known information.

Does the acquirer wish to inform card payment providers at this stage?

Yes

Record acquirers decision and time at which they state they will inform card providers.

No

Do the team believe sensitive personal data, including but not limited to card information, was potentially exposed?

Yes

Data Protection Officer to report breach to the ICO (Information Commissioners Office)

No

Incident controller to inform senior team (Director of Finance, Director ITS, SIRO. Provide details of incident, actions taken and discoveries so far.

Do the senior team believe this constitutes escalation to a major incident?

No

Continue investigation, keeping the senior team informed of developments.

Can the team be certain that they have discovered the full extent of the breach, and is it small scale with no loss of SAD data?

No

Recruit a PFI (PCI Forensic Investigator) to perform a dedicated forensic investigation.

Acquirer / incident controller to notify affected payment brands if the acquirer has not already done so.

Yes

Notify the NCA (National Crime Agency) **0370 496 7622**

Notify Action Fraud 0300 123 2040

Press Officer to contact Financial Fraud Action UK (020 3217 8436), provide information requested via their secure portal and present any agreed communications for approval by the senior team.

Yes

Scope and agree action plan with PFI. Agree reporting timelines and method for monitoring progress. E.g. Action plan with RACI.

Yes

Formal Investigation

Investigation by nominated PFI

Findings of PFI investigation and recommendations for remediation.

Summary of investigation sent to acquirer and involved card providers.

Review and enact recommendations.

No

Have all recommendations made by the PFI been enacted succesfully?

Follow procedure for a Major Incident.

Yes

Eradication and Recovery

Counter Compromise: review and, where possible, reset potentially compromised user IDs, passwords, email accounts and firewall rules within the wider environment.

Has all Sensitive Authentication Data (SAD) been removed?

Yes

No / Unsure

Remove all SAD data in line with PCI DSS requirements.

Is the CDE network secure and are any vulnerabilities discovered within systems or processes remediated?

No

Remediate vulnerabilities

Yes

Post Incident Review

Reconvene PCI DSS incident response team

Highlight lessons learnt.

Log changes to:
- Systems,
- Equipment,
- Monitoring,
- Training
- Procedures

Update incident response process to reflect changes.

Contact an independent QSA to validate the re-configuration of our CDE environment following the breach.

Validation by QSA

Following changes, is the University PCI compliant?

Yes

No

Enact any further recommended changes to the CDE environment.

Has confirmation of full remediation been received by payment brands in the form of a QSA validated ROC?

Yes

No

Request validation from the QSA.

Have all stakeholders been informed of conclusion to investigation?

Yes

No

Inform stakeholders through appropriate channels.

Archive incident log, titled with date of incident, for at least three years