TransilienceAI

Transport for London photocard data compromise

Breach Report · TLP:CLEAR

Transport for London (TfL) · transport

20 Nov 2026

Version 3 · 3 sources

Compiled by Transilience from public reporting. May be shared without restriction.

Table of Contents

BRIEF 3

- Bottom line 3
- For the board 3
- Are you exposed? 3
- What to do 3

TIMELINE 4

HOW THEY GOT IN 4

WHAT WAS TAKEN 4

WHO 4

RESPONSE AND FALLOUT 4

ATT&CK; TECHNIQUES 5

INDICATORS 5

NOT KNOWN YET 5

SOURCES 5

ABOUT THIS REPORT 5

Brief

REPORTED BY A THIRD PARTY — THE VICTIM'S OWN CONFIRMATION IS NOT QUOTED

""While we acted swiftly, we now believe that around 265,000 photocard customers may have had their account details compromised as part of this incident," he warned." [1]

Bottom line

On 16 Nov TfL discovered unauthorized access to its Photocard system that may have exposed about 265,000 account records including names, contact details and security questions; TfL says no passwords, payment data or child DoBs were accessed and the photocard portal is offline. Change photocard passwords and security answers and watch for phishing. [1,2,3]

For the board

A cyber incident on 16 Nov may have exposed about 265,000 Oyster Photocard account records; no evidence yet of payment or child DOB compromise, investigation and customer notifications are ongoing.

Are you exposed?

Came through	How to check
TfL Photocard (Oyster photocard) web portal [1,2,3]	If you run or use TfL Photocard accounts, verify if customers reported unexpected 'create account' emails from TfL and if the photocard portal is offline.

What to do

1. **Force reset photocard passwords and security questions for affected accounts immediately.** [1,2]
   TfL will ask photocard customers to change passwords, security questions and answers after unauthorized access exposed those fields.
2. **Notify customers to ignore unexpected TfL emails and report suspicious messages.** [1,2]
   Attackers sent emails from TfL's system asking customers to create accounts, enabling phishing using compromised contact details.
3. **Lock or keep the photocard portal offline until investigation confirms remediation.** [1,3]
   TfL took the photocard website offline to contain the incident and prevent further unauthorized access.
4. **Notify the ICO and maintain records for regulator queries and affected-user notifications.** [1,2]
   TfL informed the Information Commissioner's Office and is sending breach notifications to impacted individuals.

Also reported as Oyster Photocard · TfL.

Timeline

Date	Kind	What happened
November 16	INTRUSION	discovery / intrusion [1] *“On November 16, unauthorized actors sent emails to Oyster Photocard customers from TfL’s system.”* [1]
November 16, 2026	DISCOVERY	discovery [2] *“The organization discovered the security incident on November 16, 2026, after receiving customer reports about emails requesting them to create an account, which came directly from TfL's mail systems as a result of a compromise.”* [2]
18 November	RESPONSE	notification to affected users [3] *“TfL told affected users in a message sent on 18 November, which one recipient shared on Reddit.”* [3]
2026-11-19 published	DISCLOSURE	public reporting [1] *“Transport for London (TfL) has been impacted by a cyber incident, which may have impacted the personal data of around 265,000 photocard customers.”* [1]

How they got in

Not reported [3]

“The company has not disclosed how the intruders got in.” [3]

What was taken

Count	What
Included in the 265,000 estimate	Potentially affected accounts including children with Zip cards, 60+ and other concession photocards [1] *“Customers whose account details were potentially compromised include children with Zip Oyster cards, whose ages range from 5-18.”* [1]

Who

unauthorized actors — TfL described emails were "generated as a result of the compromise"; no named group. [1]
“On November 16, unauthorized actors sent emails to Oyster Photocard customers from TfL’s system. TfL said these emails were “generated as a result of the compromise.”” [1]

Response and fallout

- Took the photocard website offline and contained the incident; contacted affected customers. [1]
  “the organization immediately took the TfL photocard website down while this was being investigated.” [1]

- Notified the Information Commissioner's Office and sending breach notifications. [1]
  "The body has informed the UK's data protection regulator, the Information Commissioner's Office (ICO), of the incident." [1]
- Locked online accounts until investigation completes; will prompt affected holders to reset credentials when restored. [3]
  "Online accounts will stay locked while the investigation continues. Once the portal is restored, affected holders will be asked to choose a new password, security question and answer." [3]

ATT&CK techniques

ID	Technique	Mapped from
T1598	**Phishing for Information** MAPPED BY NEWSROOM	*"after receiving customer reports about emails requesting them to create an account, which came directly from TfL's mail systems as a result of a compromise."* [2]

Indicators

None published in the sources.

Not known yet

- Precise intrusion vector and initial access method
- Exact fields and records exfiltrated or accessed in backend systems
- Whether data has been copied or published elsewhere
- A named attacker group or attribution beyond 'unauthorized actors'

Sources

#	Outlet	Article	Copy
1	**Infosecurity Magazine** 19 Nov 2026	TfL Warns 265,000 Photocard Customers May Have Had Personal Data Expos	archived copy
2	**BleepingComputer (Bluesky)** 19 Nov 2026	Transport for London breach exposes 265,000 Oyster card users' data	archived copy
3	**Help Net Security** 20 Nov 2026	265,000 Oyster photocard customers' data exposed in Transport for London breach - Help Net Security	archived copy

About this report

Compiled by Transilience Newsroom from 3 public sources. Every quotation is checked against the article it cites; 3 statements were left out because the source did not bear them out. The status is never stated more strongly than its quote shows. ATT&CK techniques marked "mapped by Newsroom" are our reading of the quoted behaviour, not the

source's claim. Version 3, written 20 November 2026, 10:35 UTC (report-2026-09-25c). TLP:CLEAR — may be shared without restriction. The live report: https://threatnews.transilience.cloud/report/incident/mwnhb8whpxcv