Supplier breach exposes payee data at more than 40 Irish credit unions



Hackers exploited a flaw at software supplier Wellington IT and accessed payee details of members of over 40 Irish credit unions. The flaw was closed on October 6, but customers were told only on November 16.

- Ireland's Data Protection Commission received more than 40 breach notifications from credit unions that used Wellington IT as a data processor.
- Officials say only payee details held in mobile banking apps run by Wellington IT were affected; members not using the apps were not.
- Wellington IT closed the vulnerability on October 6, but its initial investigation did not identify a data protection breach.
- Affected credit unions were notified on November 16, a delay the Irish minister of state called not

acceptable.

- Authorities report no evidence so far of accessed funds or fraudulent activity.

Payment details of members of more than 40 Irish credit unions were accessed by attackers who exploited a vulnerability in the systems of Wellington IT, a software supplier based in Belfast. Ireland's Data Protection Commission confirmed it had received over 40 breach notifications from credit unions that use the company as a data processor.

What is known

The attack took place in early October, according to the chief executive of the Irish League of Credit Unions. Wellington IT says it closed the vulnerability on October 6, but its first investigation did not conclude that a data protection breach had occurred. The credit unions were informed only on November 16.

Ireland's Minister of State, Robert Troy, said the incident touched only payee details stored by members using credit union mobile banking apps operated by Wellington IT. He and Ireland's National Cyber Security Centre said there is currently no evidence that funds were accessed or that fraud occurred. Wellington IT has brought in outside experts to establish the exact number of accounts and users affected.

The incident spans two jurisdictions. The UK Information Commissioner's Office had not received a report from Wellington IT but was starting to see reports from credit unions, which suggests UK members may also be affected.

Why it matters for regulated institutions

The case shows how a flaw fixed at a supplier can still become a reportable breach for its customers, and how a gap between technical remediation and breach assessment delays notification. Customers remained the responsible parties even though the data sat with the processor.

Saudi institutions that rely on third-party processors for mobile or payment services face the same dependency.

What to do now

1. Review contracts with processors and suppliers to require prompt notification of suspected incidents, not only confirmed breaches.
2. Ask critical suppliers to share the scope of any fixed vulnerability and the evidence used to rule out data exposure.
3. Map which customer data, such as payee details, sits in supplier-run mobile and payment apps.
4. Test your incident process for decisions on notifying SDAIA, SAMA or NCA within required timelines under PDPL and applicable frameworks.

5. Include supplier breach scenarios in third-party risk reviews and tabletop exercises.