

INTELLIGENCE BRIEF

Extortion Claims Now Route Through Vendors, and the Victims Say So

In November 2026 Visa, Chase, Mastercard, Expedia, TSMC and dozens of Irish credit unions each traced exposure to a third party. Map vendor data flows, tighten vendor access, and rehearse your vendor-incident response.

EDITION

Fall/Winter 2026/2027 Edition

RW-08 · Ransomware ecosystem

PUBLISHED BY

Z7 Solutions LLC

Orlando, Florida

READ ONLINE

z7solutions.com

844-974-8669

01 At a Glance

STATUS

ACTIVE

As of November 20, 2026 Visa, Chase, Mastercard, Expedia and TSMC have not named the providers involved, and the Irish credit union investigation is ongoing. [4]

HEADLINE NUMBERS

43

Irish credit unions served by Wellington IT, out of about 50 in total [4]

48 hrs

Deadline n0n set for Visa and JPMorgan, a claim, not a confirmed leak [1]

KEY FACTS

PATTERN

Victim says a provider was hit, not its own systems [1]

VISA

Third-party provider in Asia Pacific; Visa says its systems were not involved [3]

CHASE AND MASTERCARD

Both point to vendors: marketing data at Chase vendors, limited email addresses at a Mastercard provider [9]

IRISH CREDIT UNIONS

Wellington IT confirmed by a minister as the provider; about 40 credit unions reportedly exposed [4]

EXPEDIA

Confirmed attackers compromised a third-party data platform provider, November 12 [8]

TSMC

Employee data matched records at an unnamed cloud service provider [7]

02 What Happened

Several November 2026 disclosures share one shape: a well-known organization says the problem sits at a provider, while a criminal group or forum seller makes larger claims. Treat the claims as leads and the company statements as the confirmed record.

- A group calling itself n0n listed Visa and JPMorgan Chase on its leak site with a 48-hour deadline, then on November 16 posted data it said relates to JPMorgan cardmember marketing interactions. It has not said how it got in. [1, 9]

- Visa said an incident originated with a third-party service provider in the Asia Pacific region and that its own systems were neither involved nor affected. Visa also said there is no indication payment data such as card numbers was affected. It has not named the provider. [1, 3]
- Early in the week JPMorgan attributed a customer-facing outage to a software bug. [1] On November 20 Chase said it believes attackers accessed certain marketing data held by vendors, that there is no disruption to its services, and that the incident has nothing to do with the earlier customer problems. [9, 10]
- Mastercard told Reuters an incident at a third-party provider exposed a limited amount of email addresses, and said the exposure has been contained. [9, 10]
- Expedia confirmed on November 12 that attackers compromised a third-party data platform provider. n0n claimed Expedia data, per Cybernews as reported by Skift, but Expedia has not publicly tied the incident to that group or named the vendor. [8]
- Ireland's minister of state said Wellington IT is the provider linked to the credit union incident. Irish Times and BleepingComputer report the attacker pulled saved payee records, and Wellington IT said passwords, PINs and balances were not retrieved. [4, 5, 6]
- TSMC told the SEC it found no evidence its systems were compromised and verified that leaked employee data matched data stored in a cloud service provider's system services. A forum seller's 46,000-record claim is unverified. [7]

03 How It Works

01 Pick the provider, not the target

A provider holds data for many customers behind one set of credentials or one platform. One flaw or stolen access can reach all of them at once.

02 Use a flaw or valid access

In the Irish case, notices reviewed by the Irish Examiner describe an automated script exploiting an authorization flaw, with the attacker using valid credentials, per BleepingComputer.

03 Pull records at scale

Reports describe automated requests in the millions retrieving saved payee records. Reporting gives 5 million requests in one source and about 1.4 million in another, so the count is unsettled.

04 Let the customer learn late

Wellington IT said the logs identifying which members were requested are not available, and an early October review found no exposure before a later review changed that conclusion. The minister called the notification delay not acceptable.

05 Extort or sell, publicly

Groups and sellers name big brands on leak sites and forums with short deadlines, such as 48 hours for n0n or one week for the TSMC seller, to create pressure before the facts are known.

04 Who Is at Risk

Any organization that stores member, student, patient or employee data in a vendor's platform inherits that vendor's security and its notification habits.

- Credit unions, banks and other organizations that rely on a single online banking or software provider, as the Irish cases show.
- School districts and agencies whose student information, payroll or case data lives in a vendor-hosted system.
- Organizations whose vendors hold broad API keys or service accounts into their environment.
- Employers whose HR and payroll data sits in a cloud provider, as in the TSMC disclosure.

Sectors in scope: Credit unions and community banks, Payments and financial services, Travel and hospitality, Semiconductors and manufacturing, Any organization that hands data to a software, IT or cloud provider.

05 What Changed Since the Last Edition

EACH CHANGE WITH ITS SOURCE

01 November 16 to 20: n0n posted data it tied to JPMorgan, and Visa, Chase and Mastercard each attributed exposure to third-party providers rather than their own systems. None has named the provider.

SOURCE 9

02 November 12: Expedia confirmed attackers compromised a third-party data platform provider. The vendor and any link to n0n are not confirmed by Expedia.

SOURCE 8

03 November 16 to 19: Irish credit unions were told of the Wellington IT incident, the minister named the provider and criticized the delay, and the Data Protection Commission and Central Bank received breach notifications.

SOURCE 6

04 November 15 reporting: TSMC said employee data was made available on an external website and matched data at a cloud provider, with no evidence of compromise of its own systems.

SOURCE 7

06 What to Do Now

IN PRIORITY ORDER, HIGHEST IMPACT FIRST

01 DO FIRST **Build a vendor inventory with a data-flow map: what data each provider holds, how it gets there and who at the vendor can reach it.**
You cannot scope a vendor incident, as the credit unions had to, until you know what the vendor held.

02 **Put breach-notification clauses in every vendor contract: a fixed hour limit for telling you, what the notice must contain and a duty to keep access logs.**
Wellington IT said the logs showing which members were requested are not available, and the minister called the delay not acceptable. [6]

03 **Give vendors least-privilege access, expire it, and remove service accounts and API keys nobody uses.**
Broad standing access is what lets one vendor problem become many customers' problem.

04 **Require MFA and session limits on every vendor account into your tenant, and prefer named, individually attributable accounts over shared ones.**
The Irish attacker used valid credentials, per BleepingComputer. [4]

05 **Monitor vendor-originated logins and API activity for new locations, unusual volume and off-hours use, and alert on bulk reads of saved records.**
Millions of automated requests are visible on your side if you log and watch for them. [4]

06 **Run a tabletop for the scenario that our vendor got hit: who calls the vendor, what you demand in the first 24 hours and how you decide what to tell customers.**

Visa, Expedia and TSMC each had to speak publicly before the provider was named.

07 **Write a customer communication plan that separates what is confirmed from what is claimed, and warn affected people about phishing that uses payee or contact details.**

Wellington IT warned the exposed payee data could enable phishing. [5]

08 **Treat leak-site claims as leads: verify with the vendor and your own logs before you notify or pay. Z7 offers a security assessment (/security-assessment/) and incident response planning (/incident-response-strategy/) for this work.**

Several of this month's figures are unverified and some are in conflict across outlets.

07 Sources

[1] **Visa confirms apparent cyberattack, hackers also claim hit on JPMorgan** TechRadar · November 18, 2026. https://techradar.com/pro/security/visa-confirms-apparent-cyberattack-hackers-also-claim-hit-on-jpmorgan

[3] **Ransomware gang n0n claims Visa and JPMorgan Chase as victims** The Paypers · November 2026. https://thepaypers.com/fraud-and-fincrime/news/ransomware-gang-n0n-claims-visa-and-jpmorgan-chase-as-victims

[4] **Data breach impacts 40 Irish credit unions in reported IT provider hack** BleepingComputer · November 2026, updated November 19, 2026. https://www.bleepingcomputer.com/news/security/data-breach-impacts-40-irish-credit-unions-in-reported-it-provider-hack/

[5] **Credit union data breach: Minister concerned over delay in disclosing cyberattack** The Irish Times · November 18, 2026. https://www.irishtimes.com/crime-law/2026/11/18/credit-union-data-breach-minister-concerned-over-delay-in-disclosing-cyberattack/

[6] **Data breaches reported to regulator after credit union software flaw exploited** Irish Examiner · November 2026. https://www.irishexaminer.com/news/arid-41938989.html

[7] **TSMC employee data breach linked to cloud provider** BleepingComputer · November 15, 2026. https://bleepingcomputer.com/news/security/tsmc-employee-data-breach-linked-to-cloud-provider

[8] **Expedia Confirms Cyberattack Through Third-Party Vendor** Skift · November 12, 2026. https://skift.com/?p=848794

[9] **JPMorgan, Visa, Mastercard cite third-party incidents amid data leak** SecurityWeek · November 20, 2026. https://www.securityweek.com/jpmorgan-visa-mastercard-cite-third-party-incidents-amid-data-leak/

[10] **Vendor data breach exposes Chase, Visa, Mastercard customer info** BleepingComputer · November 20, 2026. https://bleepingcomputer.com/news/security/vendor-data-breach-exposes-chase-visa-mastercard-customer-info

NEXT STEP

What does this mean for your security?

Bring your questions about Third-party provider extortion, your environment and the controls you rely on. Talk through the most useful next step with Z7 Solutions LLC.

01 / Exposure

Bring one question about how this threat could affect your environment.

02 / Priorities

Bring your current safeguards, open gaps and budget questions.

ALSO IN THIS EDITION

- Qilin still tops most ransomware counts
  More from the edition · z7solutions.com/z7-cyber/qilin/
- Qilin still hits hospitals and infrastructure
  More from the edition · z7solutions.com/z7-cyber/qilin-part-2/
- LockBit 5.0 returns after Operation Cronos
  More from the edition · z7solutions.com/z7-cyber/lockbit/

CALL	844-974-8669
EMAIL	sales@z7solutions.com
BOOK A SECURITY CONVERSATION	Book a Security Conversation ↗

Z7 Solutions™, Z7-Claw™ and Z7-Guard™ are trademarks of Z7 Solutions LLC.