Cleverbridge confirms theft of stored payment card data, including CVV codes



E-commerce platform Cleverbridge says an attacker copied stored payment card data, including CVV codes, after detecting intrusion on 4 November 2026. Notifications began on 20 November; the investigation continues.

- Cleverbridge detected unauthorised activity on 4 November 2026 and contained it; systems were back online the same day.
- Copied data includes card numbers, expiry dates and CVV/CVC codes; names, contact and billing details were reportedly not taken.
- The company says it was not ransomware and nothing was encrypted; entry method and number of cardholders are undisclosed.
- Notification letters began on 20 November via TransUnion's Cyberscout.

> - Croatia's CorvusPay separately reported a breach exposing emails and IBANs, with phishing as the main risk.

What happened

Cleverbridge, a platform that handles purchases, payments and subscriptions for other businesses, has confirmed that a third party copied payment card data stored on its platform. The company detected unauthorised activity on 4 November 2026 and moved to contain it. Affected systems were offline briefly and were all restored the same day.

According to the breach notification seen by BleepingComputer, the data includes card numbers, expiry dates and CVV/CVC security codes. The letter states that names, contact details and billing details were not copied. Cleverbridge says this was not a ransomware attack and that no systems were encrypted. It has not said how the attackers gained access, how many cardholders are affected, or which of its clients, if any, had customers involved. Its website lists clients such as Red Hat, Sony, SUSE, Veeam, Tenable and Jamf.

Notification and a related incident

Notification began on 20 November. Letters are sent by TransUnion's Cyberscout on Cleverbridge's behalf. Recipients are advised to check card statements, report unfamiliar transactions to their issuer and ask whether a replacement card is needed. The company stresses it will never request card details, passwords or security codes by email, phone or text.

Separately, Croatia's CorvusPay detected unauthorised access on 17 November to part of the system behind its CorvusPayByIBAN service. Email addresses, IBANs and some transaction details were taken, but not card numbers or payment authorisation data. The company warns of convincing follow-up phishing that cites genuine purchases.

Why it matters

Both cases involve third-party payment processors, where the exposure sits outside the merchant's own environment. Institutions should check whether their cards, customers or suppliers rely on such providers.

What to do now

1. Check whether any vendor, subscription or customer payment flow uses Cleverbridge or similar third-party payment platforms.
2. Ask affected providers in writing for incident status, data scope and whether your cards or customers are included.
3. Review corporate cards used for software subscriptions; monitor statements and ask issuers about replacement where notified.

4. Warn staff and customers about phishing that cites real purchases, and to verify payment requests using known contact details.
5. Confirm third-party contracts require prompt breach notification, and assess PDPL notification duties if personal data is involved.