Cleverbridge warns of breach exposing card numbers and CVVs



Cleverbridge has warned that attackers stole credit card numbers and CVVs in a data breach, according to BleepingComputer. Organisations that use the company should check their exposure and prepare for card-fraud risk.

- Cleverbridge has warned of a data breach.
- The stolen data reportedly includes credit card numbers and CVVs.
- The report available to us gives no further verified detail on scale or timing.
- Organisations with any link to Cleverbridge should confirm their exposure directly with the company.

What was reported

BleepingComputer reports that Cleverbridge has warned of a data breach in which hackers stole credit card numbers and card verification values (CVVs). The headline finding is that both the card number and the CVV were taken, which is the combination most useful for fraudulent online purchases.

What we do not know

The material available to us does not provide further verified detail, so we do not state how many customers are affected, when the intrusion happened, or how the attackers got in. Readers should avoid assuming scope until Cleverbridge or the affected merchants confirm it.

Why it matters to regulated institutions

Card data with CVVs raises the risk of card-not-present fraud. For banks and card issuers, this means possible fraud attempts on cards used with the affected service. For merchants and software sellers, it raises third-party risk and notification questions under PCI DSS and the Personal Data Protection Law (PDPL).

The sensible response is calm and practical: establish whether you or your customers are connected to Cleverbridge, gather facts from official notices, and prepare fraud controls while details emerge.

What to do now

1. Check whether your organisation, products or customers use Cleverbridge for payments or sales.
2. Contact Cleverbridge or your account manager for an official statement on whether your data is affected.
3. Card issuers: increase monitoring for card-not-present fraud and be ready to reissue cards if exposure is confirmed.
4. Review PCI DSS obligations and PDPL notification duties with legal and compliance teams.
5. Update your third-party risk register with this incident and record the follow-up steps.