Carnegie Endowment donor data exposed through breach at fundraising vendor



Carnegie Endowment for International Peace says an attack on its vendor Soapbox Engage exposed donor contact details and giving history. The vendor's access was cut within days, and no full card numbers were exposed.

- The attack hit Soapbox Engage, an online fundraising platform that Carnegie uses for donations; it occurred on October 28 and the attackers were removed on October 30.
- Stolen data included names, email addresses, phone numbers and giving history; no full credit card numbers were exposed.
- An integration with Carnegie's database let the intruders temporarily reach contact information held by Carnegie.
- Carnegie notified everyone in its database, citing European data privacy laws, and hired a

cybersecurity firm to confirm the attackers were gone.

- The number of affected people was not disclosed; DonorPerfect and GoFundMe also reported incidents recently.

What happened

The Carnegie Endowment for International Peace has warned past donors that their information was exposed after an attack on a third-party vendor, Soapbox Engage, an online fundraising and engagement platform for nonprofits. According to the organization, the incident took place on October 28 and the attackers were removed from the vendor's system on October 30.

The stolen data included names, email addresses, phone numbers and giving history. Carnegie says no full credit card numbers were exposed. A spokesperson said an integration with Carnegie's database allowed the intruders to temporarily reach contact information the organization maintains, and that a small percentage of the database was affected. The number of people impacted has not been disclosed.

Wider context

Carnegie notified everyone in its database because of European data privacy laws, and engaged a cybersecurity firm to confirm the attackers were removed. Soapbox Engage did not respond to requests for comment. The incident coincides with reports from other donation platforms: DonorPerfect disclosed a security incident, and GoFundMe reported two separate intrusions in October and November involving limited personal data. The Nonprofit Times reported that the attacks appeared coordinated.

Why it matters for Saudi institutions

The case shows how an integration between a vendor platform and an internal database can widen the reach of a supplier breach. Institutions in the Kingdom that use external platforms for donations, customer engagement or CRM face the same exposure, along with obligations under the PDPL and sector regulators.

What to do now

1. Inventory third-party platforms integrated with your customer or donor databases and document what data each can read or write.
2. Restrict integration accounts and API credentials to the minimum data needed, and review and rotate them regularly.
3. Confirm that vendor contracts require prompt incident notification and support for investigation and containment.
4. Review your PDPL breach-notification process and test it against a supplier-originated incident scenario.
5. Monitor integration activity for unusual access or bulk data extraction, and prepare customer

communications in advance.