GlobeTopper attack: stolen API credentials, $70,000 in gift cards redeemed



A cyberattack on gift-card distributor GlobeTopper cost an estimated $2.5 million in lost revenue. The attacker obtained customer API credentials and redeemed $70,000 in digital gift cards.

- Parent company iQSTEL said the intrusion was detected on October 22; the platform was taken offline in the early hours of October 23.
- The attacker obtained API credentials and integration keys of certain business customers; these were revoked and replaced.
- Digital gift cards worth $70,000 were redeemed and cannot be blocked or recovered, so the company bears the loss.
- A rebuilt platform on AWS went live on October 31, with commercial operations restored in stages

from November 1.

- The investigation continues into whether other customer, personal, payment or provider data was accessed.

GlobeTopper, a business-to-business distributor of digital gift cards, suffered a cyberattack that disrupted its operations. Its parent company, iQSTEL, estimates lost revenue at $2.5 million, and says the attacker redeemed digital gift cards worth $70,000.

What happened

According to iQSTEL's filing with the U.S. Securities and Exchange Commission, the intrusion was detected on October 22. Further unauthorized activity was seen the next day, and the company took the platform and all affected servers offline in the early hours of October 23. A completely rebuilt platform on AWS was deployed on October 31, and commercial operations returned in stages from November 1.

The attacker obtained API credentials and integration keys belonging to certain business customers. These have been revoked and rotated, and affected customers received new credentials with additional access restrictions. The company has seen no unauthorized use of them so far.

What remains unclear

The investigation is still examining whether other customer, personal, payment or provider data was accessed. The company says it cannot block or recover the redeemed gift cards. It has not determined the incident to be material. iQSTEL declined to answer further questions, and no ransomware group has listed the company as a victim.

Why it matters

GlobeTopper's platform is used by retailers, fintech apps and rewards platforms through an API. For institutions that integrate with such providers, the case shows how exposed integration credentials can be turned into direct financial loss, and how a provider outage can interrupt services.

What to do now

1. Inventory API credentials and integration keys used with third-party providers, and confirm each has an owner and an expiry or rotation schedule.
2. Restrict keys by IP range, scope and transaction limits, and monitor for unusual redemption or issuance volumes.
3. Confirm that your provider contracts require prompt incident notification and credential revocation, in line with NCA ECC third-party requirements and SAMA CSF where applicable.
4. Test your ability to rotate compromised keys quickly and to run services if a provider goes offline.

5. If you use GlobeTopper, rotate credentials and review activity from late October onward.