US FinCEN Takes Systems Offline After Intrusion and Extends Filing Deadlines



The US Treasury's FinCEN has taken some systems offline after unauthorized access and extended certain filing deadlines to December 30. Few details are public, and the attacker and affected systems remain unnamed.

- FinCEN is investigating unauthorized access to a limited subset of its systems and has taken some systems offline as a precaution.
- The agency has not said who is behind the attack or which systems were accessed.
- A November 24 order gives temporary relief to filers affected by a service disruption.
- Eligible filings or updates due between November 18 and December 29 may be submitted by December 30.
- The incident follows other reported breaches at US federal bodies, including the CIA and ODNI.

The Financial Crimes Enforcement Network (FinCEN), the US Treasury bureau that acts as the country's financial intelligence unit, is investigating a cybersecurity incident. According to a notice on its BSA E-Filing website, an unauthorized party reached a limited subset of its systems, and the agency took some systems offline as a precaution.

What is known

FinCEN collects suspicious activity reports and other Bank Secrecy Act filings from banks and other financial institutions and shares the intelligence with law enforcement. It has said little about the incident, including who is responsible and which systems were accessed. The BSA E-Filing site remains available, but the agency warns some services may be temporarily unavailable.

On November 24 FinCEN issued an order granting temporary, limited relief to filers hindered by the disruption. Judging by its scope, the Secure Data Transfer Mode channel appears affected, as do services used for beneficial ownership information reports and for updating FinCEN identifiers. Eligible filings or updates due between November 18 and December 29 can be submitted by December 30.

Wider context

The disclosure followed a New York Times report that the CIA and the Office of the Director of National Intelligence had a breach involving some unclassified information. Breaches have also been reported at the Department of Agriculture and the FBI (two separate ones), while the Pentagon and Homeland Security have dealt with their own incidents.

Relevance for Saudi institutions

The source does not mention Saudi entities. Institutions with US filing obligations or US correspondent relationships may still want to check their own exposure and deadlines, and use the case to review how they would meet regulatory reporting duties if a filing channel became unavailable.

What to do now

1. Check whether your institution files with FinCEN or depends on US correspondents that do, and note the December 30 extended deadline.
2. Monitor FinCEN's BSA E-Filing notices for updates rather than relying on informal channels.
3. Confirm filings are tracked and evidenced so any delay caused by the outage can be documented.
4. Review the fallback plan for regulatory reporting when a filing channel is unavailable, including contacts at the regulator.
5. Verify that data shared with US authorities or partners is limited to what is required and its handling is recorded.