US announces its largest scam crackdown, with nearly $17 billion in illicit funds seized



The US Department of Justice reports a crackdown on more than 800 alleged scammers, with the FBI seizing nearly $17 billion and dismantling over 29 scam compounds abroad. Fraud-prevention teams should review exposure to similar scam patterns.

- The DOJ says the effort covers more than 400 cases in 85 federal districts and over 800 alleged scammers; 30 defendants were extradited.
- Under Operation Blackout, the FBI seized nearly $17 billion, dismantled over 29 scam compounds and helped bring home over 2,200 trafficked workers.
- The State Department helped freeze over $1 billion in stolen cryptocurrency and remove more than 1.4 million fraudulent websites and accounts.
- Cases included a list broker selling personal data of elderly people to scammers, and prison inmates

using smuggled phones for fraud calls.

- The FCC approved a rule on November 19 allowing prisons to use jamming against contraband phones.

The US Department of Justice has announced what it describes as its largest-ever crackdown on scams targeting Americans. The effort covers more than 400 cases across 85 federal districts, with new charges, guilty verdicts and sentences, and 30 defendants extradited. US agents worked with police in more than 10 countries to raid call centers and compounds abroad.

What was reported

Under Operation Blackout, the FBI seized nearly $17 billion in illicit funds, dismantled more than 29 scam compounds and helped bring home over 2,200 trafficked workers. The State Department helped freeze over $1 billion in stolen cryptocurrency and take down more than 1.4 million fraudulent websites and accounts.

Several cases involved the trade in personal data. A list broker in Mexico allegedly sold names and contact details of elderly Americans to dozens of scammers. In another case, inmates in Georgia prisons allegedly used smuggled phones to pose as court officials and demand payment, which prompted the FCC to approve a rule allowing jamming of contraband phones in prisons.

Why it matters for Saudi institutions

The source describes scams spreading from Southeast Asia into other regions, including the Middle East. The tactics it describes, such as impersonating authorities, using purchased personal data and moving funds through cryptocurrency, are not specific to the US. The source does not report any Saudi cases.

For regulated institutions, the practical lesson is that fraud depends on data exposure and on weak customer verification. Reviewing both is a sensible response to this news.

What to do now

1. Review customer-facing verification and call-back procedures so staff and customers can tell genuine contact from impersonation of authorities or the institution.
2. Check how customer personal data is shared with third parties and brokers, and confirm that contracts and PDPL obligations are enforced.
3. Run awareness messaging for customers, especially elderly ones, on payment demands made by phone under threat of arrest or fines.
4. Make sure fraud monitoring covers transfers to crypto-related destinations and that escalation paths to law enforcement are tested.
5. Brief the fraud and SOC teams on the reported patterns and add them to scenario exercises.