

Sep 23, 2005

Compromise of FinCEN e-mail service raises questions about data security

Source <http://www.moneylaundering.com/NewsBriefDisplay.aspx?ID=841>

© <http://www.moneylaundering.com>

Subscribers to the U.S. Financial Crimes Enforcement Network's e-mail service got a surprise message this morning after outsiders apparently accessed the agency's public website and sent their own missive.

The e-mail, whose subject line was "child from iraq" included two pictures that appeared to be from the Middle East and bore the message "go away from iraq."

Under the guise of a legitimate FinCEN e-mail, this message caused confusion in a matter of minutes as the Internet spread it across the globe. However, the agency quickly assured subscribers it was aware of the issue, its data was secure, and it was taking action.

Peter Oakes, founder of the Dublin-based consulting firm Compliance Ireland, told moneylaundering.com that he received several calls about the email from banks and companies, some of which are subsidiaries of U.S. firms.

Oakes went on to wonder whether FinCEN's systems remain secure, noting that if someone got into the email, they could have gone further.

"If, and it's a big if, FinCEN's systems were hacked, did the hackers penetrate the server on which STRs [suspicious transaction reports] are received and stored?" he said. "It is all conjecture, but if this happened, could it mean that details of STRs, including details of persons filing the STR, have been seen by the types of persons who have been reported?"

However, FinCEN underscored in a statement that its core systems were safe, saying that the website is externally hosted and that it resides outside FinCEN's security perimeter. It also said it reported the breach to law enforcement.

Although FinCEN states that Bank Secrecy Act data was "in no way, shape, or form compromised by this incident," experts said the breach could raise doubts about how secure the data is.

Howard Steiner, senior partner of Impact AML, an anti-money laundering consulting firm, said that the e-mail incident demonstrated at least some vulnerability that needs to be investigated, especially, he added because FinCEN collects information on potential terrorists.