

Banks that Complied with the FBI May Face Lawsuits, Say Privacy Advocates



April 05, 2007

By Brian Orsak

Banks that provided non-subpoenaed information to the Federal Bureau of Investigations may face civil action, according to privacy advocates and compliance consultants.

The speculation follows a March 2007 report on national security letter subpoenas by the Office of the Inspector General that stated that some companies complying with FBI terrorist investigations provided excessive information about their customers. The information was, in some cases, retained while agents filed backdated subpoenas to justify their possession of the excess.

The disclosure illustrates the informal way in which information is sometimes shared by financial institutions without the legal protection of a subpoena, a route that leaves both investigators and complying institutions open to civil action, say privacy advocates.

"It's something that is extremely dangerous," said Mike German, a former FBI special agent in domestic terrorism and current policy counsel for the American Civil Liberties Union, who added that lawsuits were possible.

Informal information exchanges are the result of a "natural flow" of former law enforcement agents to security positions in the private sector, where the interaction between law enforcement officers and their former co-workers is "too friendly," according to Jim Harper, the director of information policy studies at The Cato Institute, a Washington, D.C.-based libertarian think tank.

A bank compliance officer might pass along informally requested information about a customer with the expectation that a subpoena covering the request would follow within days, according to Harper. Because no manual or electronic log of subpoenas exists, "no one's the wiser" of when they are issued, said Jim Dempsey, the policy director of the Washington, D.C.-based Center for Democracy and Technology.

Information provided in excess to subpoenas was not uploaded into FBI databases, according to the OIG report.

Of the 26 possible violations related to the use of national security letters reported to the FBI between 2003 and 2005, three involved the FBI obtaining information without issuing a subpoena. In one of the three cases, there was no open national security investigation involving the information, according to the OIG report.

Under the Graham Leach Bliley Act, banks are required to protect the non-public information of their customers, but may share it in the case of a criminal investigation. Two types of national security letters may be issued to banks, one under the National Security Act that concerns employees of the executive branch with access to classified information, and another under the Right to Financial Privacy Act that may be used in terrorist investigations. Financial institutions that share information informally are not protected.

"Given the number of lawyers in the country, it's very likely we will see lawsuits," said Harper, adding that lawsuits may not be "fair" but may be filed "just to do the discovery."

Even if financial institutions see some fallout from the OIG report, lawsuits are unlikely to stick, according to Rich Riese, the director of the American Bankers Association's Center for Regulatory Compliance.

"It doesn't take much to initiate action and litigation that has no merit," he said.

Although critics of the FBI have been vocal following the release of the report, proponents of both informal information sharing and national security letters say that the practices protect banks on the balance.

While customer information is informally shared often, it is not “abusively done,” according to Kenneth L. Bryant, the managing director of Bryant & Associates, a Hayesville, North Carolina-based global AML/CFT consultancy. Compliance officers and investigating agents are careful to protect information and preserve what they view as a mutually beneficial relationship, said Bryant, who encourages compliance officers to cultivate relationships with law enforcement agencies.

“At the end of the day, we’re all trying to fight the war on terror,” said Bryant.

Problems pointed to in the OIG report are more administrative and less indicative of power abuse, according to Thomas Cash, an executive managing director for New York-based security consultant Kroll. Because law enforcement agents are busy with legitimate leads, they are unlikely to make information requests in order to “fish” for customer information, said Cash.

“People aren’t pulling names out of the air and then going to investigate them,” he said.

Regardless of the intention of investigators, financial institutions should comply with information requests via a formal process in order to avoid liability concerns, according to Stephen Cesso, general counsel of compliance software company Computershare and an adjunct professor with Boston University’s banking program. Computershare gets illegal requests for information “from time to time,” but the company requests a subpoena, he said.

Additionally, banks should be mindful that subpoena requests do not equal inspection powers, said Cesso.

Although most cases of institutions sharing excessive information are the result of human error, and are therefore afforded good faith immunity, financial institutions and their legal counsels should be certain that any information they disclose is permitted under the applicable statute, said Catherine Milhoan, a spokesperson for the FBI, in an email interview.

One consequence of the OIG report is that U.S. financial institutions and law enforcement agencies will better audit their employees as part of an overall effort to improve information sharing, according to Dempsey. While the U.S. has been vocal in criticizing other countries and offshore financial centers for their financial practices, it still lags behind international AML standards generally, including with respect to how and when information is shared, according to Bryant.

In a March 27 statement before the Senate Judiciary Committee, FBI director Robert Mueller III acknowledged shortcomings in the use of national of security letters and said the agency was overhauling related technology to better track when information is requested and received.

“The FBI is acutely aware that we cannot protect against threats at the expense of civil liberties,” said Mueller.