Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Goldman's $36M Fine Turns Data Security Scrutiny Inward

By **Allison Grande**

Law360, New York (August 4, 2016, 9:35 PM ET) -- The Federal Reserve on Wednesday flexed its data security enforcement muscles by hitting Goldman Sachs with a $36.3 million fine over a former employee's alleged misuse of confidential information to attract clients, highlighting the need for financial institutions to be mindful of not just external threats, but also internal security risks that could land them in hot water with increasingly active regulators.

The hefty fine imposed by the Fed stemmed from the central bank's investigation into the use of confidential supervisory information by Joseph A. Jiampietro, a former managing director at Goldman's investment banking unit, to improperly attempt to attract and assist bank clients after he received the information from a former Federal Reserve Bank of New York staffer who went on to work for Goldman.

Although the misconduct was orchestrated entirely by its employees and Goldman itself discovered the data misuse through an internal investigation and reported it to authorities, the Fed still directly pinged the company, concluding that the firm had significant shortcomings in its protections against the misuse of confidential supervisory information prepared by banking regulators.

"Undoubtedly, the significant size of this settlement alone will cause every company with whom similar sensitive information is shared by the Fed to stop what they're doing and look closely at the security safeguards they have in place, which I'm sure is what was intended," said Al Saikali, co-chair of Shook Hardy & Bacon LLP's data security and privacy group.

The Fed's decision to go after Goldman for an internal breach of the way institutions and their employees are required to handle confidential information is consistent with how other regulators both inside and outside the financial services sphere — ranging from the U.S. Securities and Exchange Commission and the Consumer Financial Protection Bureau to the Federal Trade Commission and the Federal Communications Commission — have been dealing with data integrity issues as of late, attorneys noted.

"Much like cases earlier this year involving the SEC, this case reflects that in this era of cybersecurity, regulators are acting aggressively," Hughes Hubbard & Reed LLP data privacy and cybersecurity group co-heads Dennis Klein and Seth Rothman said in a joint email.

Like the Fed, the SEC also drew attention to the risk for financial institutions of failing to properly patrol their employees with one of its recent enforcement actions, namely a $1 million settlement with Morgan Stanley Smith Barney LLC announced in June.

In that case, the SEC claimed that the investment adviser did not have proper controls in place to secure internal client information systems from improper access by employees, including one who exposed data on 730,000 accounts to hackers who ultimately publicly posted some of it online.

However, despite its similarities to the SEC action, the case pursued by the Fed differs from myriad other data security actions pursued by a slew of regulators in recent years in that the data was misused internally and not leaked beyond the company's clients and business prospects.

"It's not like this was a hack or a cyberintrusion — it was more like a form of insider trading," Lewis Baach PLLC partner Adam Kaufmann said. "This action shows that there's no doubt that financial institutions are responsible for having control over their employees' receipt of confidential or insider information" in addition to protecting their systems from external threats.

While the majority of actions brought by regulators stem from the mishandling of customers' personal data, the Fed's gripe centers on the misuse of confidential supervisory information, which includes reports of bank examinations and other confidential reports prepared by banking regulators that are illegal to use or disclose without prior approval from the proper banking regulator.

According to the Fed, Jiampietro obtained information that his associate Rohit Bansal received from a former colleague and New York Fed employee, and then used that data in a variety of presentations intended to win clients for his bank regulatory practice to keep them.

The Fed based its decision to penalize Goldman on the premise that it "expects all firms, including Goldman Sachs, to comply with all U.S. laws, rules and regulations," and that the firm failed to have sufficient policies, procedures or adequate employee training in place to ensure compliance with current laws prohibiting the unauthorized use or disclosure of confidential supervisory information.

"This action underscores the importance of having appropriate policies and procedures in place prohibiting not only the disclosure of confidential information, but also the receipt of confidential information," Klein and Rothman said.

As part of the settlement, Goldman is required to improve its internal data processes, including by putting in place controls to ensure the proper identification and management of information, enhancing oversight and employee training, and deleting some confidential supervisory information it holds — obligations that Saikali noted are "general best practices for the protection of highly sensitive information in general."

However, Saikali said that he was struck by the part of the order that faulted Goldman for "failing to monitor electronic mail for documents containing confidential supervisory information," noting that the standard seemed as if it would be "virtually impossible" to meet.

"Even if Goldman could 'tag' the file to know when it is leaving their system — and it should implement controls to limit access to and transfer of the documents — what would stop employees with access from using relevant excerpts?" Saikali said.

But despite the difficulties with preventing individual employees from going off the grid, attorneys said that financial institutions need to keep paying attention to the issue, given that they are unlikely to receive a free pass from regulators for a worker's missteps.

"When companies see an action like this, they should rightly ask themselves what lessons they can draw from it, and the lesson from this is that there needs to be training to teach employees not to misuse confidential information and to raise a red flag within the firm if you suspect someone is doing that," Kaufmann said. "Because increasingly, it's looking like it's zero tolerance for anything that happens at an institution and that there will be a fine, even if it involves a rogue employee."

While Goldman "seemed like it did the right thing" by reporting the misconduct once it noticed it, the settlement made clear that the firm could have done more to prevent the misuse of data in the first place, Laurie Shen, a principal at UHY Advisors Inc., pointed out, adding that having layers of supervision and monitoring could be a key to dodging regulatory scrutiny.

"This action brings awareness to the fact that financial institutions should look at the terms of what programs they have in place and make sure they are working and effective," Shen said.

Attorneys also noted that, even though Goldman took a hard hit, employees shouldn't expect to get off scot-free if they don't follow applicable laws and regulations.

Bansal, the Goldman Sachs employee who initially received the information, and Jason Gross, the New York Fed employee who funneled the information to Bansal, both pled guilty in November to one misdemeanor count each and were sentenced to community service. Jiampietro, the managing director who was given the data by Bansal, was fired in 2014 after Goldman determined that he hadn't reported the leak to the necessary parties, and the Fed announced Wednesday that it was starting enforcement proceedings that seek to ban him from the industry and impose a $337,500 fine against him.

"With this action, the Fed is showing that regulators are very interested in personal accountability as well," Kaufmann said.

The Fed's enforcement action also raises questions about the data security within the regulator itself, given that the incident appears to have originated from the New York Fed employee's decision to leak the data to his former colleague at Goldman.

"The funny thing about this is that the confidential information that was improperly used at Goldman came from the Fed," Kaufmann noted. "So the question becomes who regulates the regulator, and is the Fed going to require itself to improve its own security practices?"

The wrinkle adds to the punch delivered by the Fed's enforcement action, which was the second such hit delivered by a regulator over the misuse of data at Goldman, following in the footsteps of a $50 million settlement the firm reached with the New York Department of Financial Services in October.

"That's the unfortunate thing for financial services companies — they've got multiple regulators that are looking at them that could have the same findings or different findings and perspectives on the same issues, and they have to deal with them separately," Shen said.

And with cybersecurity continuing to gain steam as an issue that all regulators want in on, attorneys predict that this enhanced scrutiny and potential for overlap won't diminish any time soon.

"As people's access to information continues to increase, it's likely that we'll only see more regulatory actions focusing on the misuse of information from regulators in general," Kaufmann said.

Goldman is represented by Steven R. Peikin of Sullivan & Cromwell LLP.

Jiampietro is represented by Adam C. Ford and Kevin J. O'Brien of Ford O'Brien LLP and Samuel T. Hirzel, Melissa N. Donimirski and Aaron M. Nelson of Proctor Heyman Enerio LLP in his litigation against Goldman.

The cases are In the Matter of The Goldman Sachs Group Inc. et al., docket numbers 16-011-BH-C and 16-011-CMP-HC, and In the Matter of Joseph Jiampietro, case number 16-012-E-I and 16-012-CMP-I, before the Board of Governors of the Federal Reserve System.

--Editing by Katherine Rautenberg and Philip Shea.
