COMPLIANCE WEEK
THE LEADING INFORMATION SERVICE ON CORPORATE GOVERNANCE, RISK, AND COMPLIANCE

Hurry-Up Offense on Employee Surveillance

By Jaclyn Jaeger

Employee surveillance is one of the most sensitive—and yet, rapidly evolving—areas of compliance for financial services firms today. Initially a response to regulatory pressure, surveillance obligations are now becoming an integral part of a robust internal control system.

That does not mean those obligations are easy to fulfill.

Monitoring employee activities to detect and prevent illegal conduct—fraudulent trading, benchmark rate manipulation, or any other offense—is not a new concept per se, especially for large financial institutions. Both the Securities and Exchange Commission and the Financial Industry Regulatory Authority, for example, have long required banks to monitor their employees' personal trades. Traditionally, however, the data generated by such surveillance activities has been done in a manual, cumbersome, and often siloed fashion. That approach left significant gaps in oversight.

Taking harsh lessons learned from the financial crisis, and still reeling from the billions of dollars in fines resulting from the LIBOR scandal, financial services firms now want ways to monitor employee activity actively, rather than responding to regulatory demands. "They're no longer just complying with regulations," says Jake Frazier, senior managing director at FTI Consulting. "They want to take it to the next level."

JPMorgan's Corporate & Investment Bank (CIB), for example, said it launched a comprehensive review last year to analyze and make improvements to its sales and trading practices and related communications. "We recognized that enhancing market conduct would require using multiple preventive and detective levers in a coordinated way," the bank stated in a report to shareholders. That review considered various means to:

- Establish information barriers;
- Conduct communications and transaction surveillance;
- Adopt policies;
- Implement training; and
- Incorporate enhanced supervision, compensation, and disclosure practices.

"In the first phase of the review, the business enhanced information barriers by implementing new policies around electronic chat and launched an effort to increase and improve communications guidelines and surveillance of chat and e-mail," JPMorgan said. "In the second phase, we are carrying out a review of information flows in the markets businesses, further refining electronic chat guidelines, continuing enhancement of surveillance, and prioritizing other issues for review."

JPMorgan added that the project "seeks to identify certain per se prohibited communications and set forth principles governing permitted communications, including information to be shared on a need-to-know basis and only for legitimate business purposes, such as trade execution or clarification of operational details."

Financial services firms are realizing they can "better protect their employees and their brand by having more clearly defined policies and exceptions to those policies," says Scott Rister, vice president of compliance solutions at Charles Schwab. For example, some firms historically have allowed employees to maintain personal investment accounts anywhere they wanted, as long as the firm could get a paper statement at least quarterly. Now they're refining those policies, requiring employees to use broker-dealers who provide an electronic data feed, so that the firm has better access to real-time information—usually next day—and can analyze it in a more efficient manner, he says.

Another approach that many banks have developed as part of their surveillance programs is a "hub and spoke type of model," Frazier says. Under that model, a compliance committee, or even a group of compliance liaisons, serve as the central hub, disseminating relevant information down to the business units, he says.

JPMorgan, for example, established a steering committee, tasked with develop-

JPMORGAN SALES, TRADING PROCESS

Below is an excerpt from JPMorgan's "How We Do Business" report, describing its revised sales and trading practices.

In the first quarter of 2014, the CIB launched a comprehensive review to analyze and make improvements to our sales and trading practices and related communications. We expect our sales and trading personnel not only to treat customers fairly but to act in a manner that supports well-functioning, transparent markets.

We recognized that enhancing market conduct would require using multiple preventive and detective levers in a coordinated way. For example, the review took into consideration various means to establish information barriers; conduct communications and transaction surveillance; adopt policies; implement training; and incorporate enhanced supervision, compensation and disclosure practices.

In the first phase of the review, the business enhanced information barriers by implementing new policies around electronic chat and launched an effort to increase and improve communications guidelines and surveillance of chat and email. In the second phase, we are carrying out a review of information flows in the markets businesses, further refining electronic chat guidelines, continuing enhancement of surveillance and prioritizing other issues for review.

The project seeks to identify certain per se prohibited communications and set forth principles governing permitted communications—including information to be shared on a need-to-know basis and only for legitimate business purposes, such as trade execution or clarification of operational details.

Source: JPMorgan.

Reprinted from Compliance Week, May 2015

ing a global governance framework. "The committee is charged with setting policy and standards and creating an operating model to support a global communications surveillance program," the bank said.

Advanced Analytics

As the industry has evolved, and as technology has evolved, financial services firms now also have the ability to gain greater insight into potential illegal conduct across various business units, and at speeds once inconceivable. Although regulations still drive most employee surveillance activities, "most financial institutions are much more proactive in how they monitor, meaning they are looking to leverage technology to get more timely access to information and better identify potential issues," Rister says.

Newer surveillance technologies, for example, employ analytics that use not just structured data—such as trading activity—but also unstructured data generated by e-mails, text messages, phone conversations, and social media. The goal of marrying together structured and unstructured data is "to find patterns that wouldn't otherwise pop up for an investigator or an auditor if they were looking exclusively at one of those two silos," says Joram Borenstein, vice president of marketing at NICE Actimize.

Many banks today also are implementing audio communication surveillance capabilities, which employ a real-time phonetic index of telephone conversations, much in the same way that a keyword search can analyze electronic communications. "For example, if a broker says on the phone, 'I guarantee you five times your money back on this investment,' then the phonetic indexing will catch that," Frazier says. Historically, such information may not have been captured until an investigation ensued, he says.

Companies now can also overlay this data with information from other departments such as HR records and financial records. The overall intent is to look at employees' personal behaviors in the context of their IT behaviors, to see whether there is a heightened risk, or a shift in behavior, that suggests something needs to be investigated, says Greg Henderson, government healthcare director in the security intelligence global practice of SAS. If an employee suddenly is taking a lot of vacations and traveling to suspect foreign destinations during a time when his IT activity is also suspect, those factors together might be a red flag to the company that the person needs to be investigated further.

With today's advances in IT, even small firms are now able to implement a system that meets their needs, as more vendors offer monitor capabilities that can be scaled to the size of the firm. "That's definitely made it easier for firms of all sizes to conduct surveillance in a more cost-effective and expedient manner," says Amy Lynch, founder of FrontLine Compliance, a financial services consulting firm.

> "Financial services firms are realizing they can better protect their employees and their brand by having more clearly defined policies and exceptions to those policies."
>
> Scott Rister, VP of Compliance Solutions, Charles Schwab

For financial services firms still developing their employee surveillance and monitoring activities, Borenstein says compliance officers shouldn't simply rely on whatever regulatory framework they're required to comply with—whether that's Dodd-Frank, the Sarbanes-Oxley Act, or any other regulation. "They shouldn't take a check-the-box approach," he says. Instead, they should satisfy those regulations as a minimum standard, and then take a step back and ask where else their institution might have risks that the regulatory framework might not completely cover. ■