THE NATIONAL LAW JOURNAL
MARCH 6, 2018
Online Feature
An ALM Publication

Commentary

SO YOU'VE HAD A COMPLIANCE BREACH—NOW WHAT?

Two compliance professionals offer seven steps to take in response to a major breach.

BY JERRY CUMMINS AND CARL RIZZO

Valuable lessons can be learned from compliance practitioners in the highly regulated financial sector regarding the most prudent steps to take in response to a major breach.

A qualified chief compliance officer (CCO) who is familiar with a firm's specific compliance program and the laws and regulations that apply to the breach in question can play a vital role helping lawyers with fact-finding, developing a remediation plan and preparing clients for regulatory scrutiny, sworn depositions or testimony. Indeed, it is increasingly commonplace for regulators to require respondents to retain independent compliance professionals as part of a firm's settlement order.

The fault line that distinguishes major matters are those that materially impact customers or the company brand. These include systematic compliance failures, or isolated breaches coupled with aggravating factors, including: 1) scienter fraud, 2) harm to clients or 3) recidivist behavior.

When a major breach occurs, an ill-considered response can be costly, especially when—as is often the case—actions taken in haste cannot always be reversed, such as inadvertent breaches of attorney-client privilege. Defendants have been known to waive privilege by simply failing to indicate that attorney-client communications are confidential. Your regulator may ultimately judge a careless response as well.

Depending upon the nature of a breach and the context in which it occurred, there will naturally be variations in the response team's tone and tactics. For instance, the response to an inadvertent breach will contrast sharply from one involving a rogue employee who knowingly or repeatedly broke the law, or a breach that has been covered up for some period of time.

Editor's note: We hope you enjoy this contributed content by Jerry Cummins and Carl Rizzo. Look out for more columns on compliance in The National Law Journal's April special report.

For major compliance breaches, the following seven steps should be taken:

1. Assemble the response team. This could include the CCO and general counsel; outside counsel; senior executives; business managers; information technology (IT) professionals, if needed for forensic data gathering. This may also include external services providers such as an administrator,

which may or may not need to be fully informed of the matter.

2. Gather relevant information. Gather all facts and color surrounding the breach to get the clearest possible picture of what happened and why. The process should be thoughtful, thorough and accurate. Don't jump to conclusions, rush to judgment or rely on untested assumptions in the absence of a careful and unbiased team-based process. Employees should be told by counsel to preserve data and encouraged to report what they know.

3. Identify all nonresponse team parties. This would include culpable individuals and all entities that must be notified—including board members, insurers and independent auditors. This would also include entities that may be notified; state or federal regulators; and impacted parties, such as clients. Companies may also identify outside professionals who have expertise in a particular subject matter, such as cybersecurity.

4. Evaluate the breach. Examine the breach in the context of the company's policies and compliance manual to determine scope and severity, including materiality to impacted parties. Evaluate the degree of culpability of responsible individuals; the effect on impacted parties; and potential penalties and sanctions, such as administrative censure, fines, injunction or deregistration.

5. Appropriately disclose and report. As the response team deems necessary, disclose and report the incident beyond the firm, to clients, insurers, auditors, affiliates and regulators.

Companies that self-report to regulators must work meticulously to ensure that all reported information is accurate and complete. Respondents may opt to defer regulatory reporting until their next examination, except in the most serious breaches.

If the response team deems there is a possibility a breach may be made public, it would be wise to engage a public relations team that is experienced in crisis communications. Professionals can assure customers and the public at large that the matter has been thoroughly addressed.

6. Appropriately manage nonresponse team employees. If the incident was reported by an employee, make sure to observe whistleblower protections, such as U.S. Securities and Exchange Commission (SEC) Rule 21F-17(a), which prohibits actions that discourage whistleblowers, including language in employment and severance agreements. Employees should understand that regulators under such bounty programs may favor reporters who try first to work with their company to resolve matters.

Culpable parties must be dealt with carefully. It may be prudent to train and monitor an individual who unintentionally caused a breach whereas one would likely terminate an unremorseful employee. Regulators expect companies to impose and document meaningful employee sanctions commensurate with the offense.

7. Develop a remediation plan. With an accurate and clear understanding of what happened and all parties involved, the team next needs to develop a remediation plan. The goal is to anticipate what regulators would expect in terms of an appropriate response, especially when parties are harmed. A well-crafted plan can serve as a pre-emptive strike, encouraging regulators to settle instead of imposing stiffer penalties.

At a minimum, the remediation plan should address:

1. Personnel actions undertaken;
2. Implemented enhanced compliance controls;
3. Plans for handling disclosures and reporting; and
4. Monetary restitution, including beneficiaries and calculation methodologies.

A seasoned CCO can work with counsel to help shepherd a breach to the quickest possible resolution. He or she can proffer a remediation plan that provides assurances to all parties impacted and—most importantly—legal and regulatory examiners. Ultimately, the objective is to make all affected parties whole, and to build better compliance controls that prevent the breach from ever happening again.

Jerry Cummins *and* ***Carl Rizzo*** *are directors at Alaric Compliance Services and are part of a team of compliance professionals with experience across all asset classes and investment strategies.*