STEPTOE OUTSIDE COUNSEL

Top signs it's time for an internal compliance investigation

Export control and sanctions enforcers give credit to companies that self-initiate investigations, remediate breaches, and self-disclose violations of law in a timely manner. Sometimes, a compliance hiccup can be closed out with a light touch with no further investigation required. In other cases, a small mishap is a sign of a much larger problem, even a legal risk. When is it time to start digging? Here are three signs based on past investigations.

1. Major malfunctions

When a critical process breaks down – customer due diligence, name screening, management approvals, to name a few – a violation of law might not be far behind. Testing and auditing are meant to head off a compliance catastrophe, but control failures have been known to go on for months or years before detection. This is especially true where critical compliance processes are managed through IT systems with little oversight.

Take for example a US exporter whose logistics team became complacent about clearing name-screening alerts. Dozens of shipments left the warehouse for denied parties or sanctioned jurisdictions over several months. A routine compliance audit spotted the issue. Upon closer inspection, the shipments had been flagged by the screening system but never checked.

In another case, a sales team in the Asian office of a US company conspired with a distributor to ship controlled items to a prohibited destination. The tip off? A whistle blower uncovered fake documents in an ERP system. An internal investigation found a long-running scheme with multiple co-conspirators inside and outside the company.

The bigger the breakdown, the more important it is to assess the potential risk, scope, and employee involvement. A short-lived gap involving low-risk customers may not warrant a deep dive. Evidence of fraud or carelessness in a key function deserve a closer look.

2. Wayward counterparties

Imagine: the name of a major customer is splashed across the headlines. For years, they've been running a secret business in a sanctioned territory. Worse, it sounds like your company's highly sensitive products might have been involved. Who knew? When did they know it?

In a well-publicized case, a European manufacturer shipped industrial goods to an overseas customer only to have them re-exported to an embargoed territory. Local media in the receiving country had reported on the sale – including the equipment's ultimate destination – before the shipment took place.

Suppliers can easily get drawn into law-enforcement investigations of customers' misconduct. An effective internal review can spell the difference between being viewed as a cooperator versus a potential enforcement target.

Things to look for in retrospect include evidence that employees had knowledge (actual or constructive) of the counterparty's scheme, and irregularities in orders, shipments, or communications that should have been spotted.

3. Missed payments

Even more than regulators, eagle-eyed banks can push their customers to undertake internal investigations. It usually begins when the bank's sanctions controls detect a potentially unusual transaction. A frozen or rejected payment is a strong sign that something is amiss.

Consider the case of the US exporter whose financial institution blocked a letter of credit after detecting a sanctioned party on a bill of lading. Finance employees circumvented the bank's controls by processing a sizeable wire transfer instead. The breach came to light the following year when a potential investor asked about sanctions compliance.

An isolated example it is not. Numerous settlements by the Office of Foreign Assets Control ("OFAC") underscore that the subjects were put on notice when banks refused to process their payments, but failed to investigate or react. Often, the banks are obliged to report details of rejected or blocked transactions directly to OFAC – providing fodder for future enforcement actions.

Final thoughts

At the start of any investigation, important decisions arise about scope, roles and responsibilities, and conflicts – individuals or departments that caused a breach should not investigate themselves. A decision not to investigate further, and the reasons, should be documented and filed.

With the enforcement landscape heating up, more companies are adding investigations protocols to their export control and sanctions policies. Key topics include investigation triggers, roles and responsibilities, and guidelines for protecting the attorney-client privilege. ■

About the authors:

Ali Burney (aburney@steptoe.com) is a Partner and Nicholas Turner (nturner@Steptoe.com) is of Counsel in the Hong Kong office of Steptoe.

Reprinted with permission from the July/August 2020 issue of Export Compliance Manager
www.exportcompliancemanager.com