Handling Anonymous Allegation Letters

By Peter Humphrey

DEZAN SHIRA & ASSOCIATES

The General Manager of "We're Okay Thanks Inc.'s" China operation is feeling proud of himself. Three years in this job, he is now transferring home to Europe with a sparkling record. He has diligently built up the business, three factories and a national dis-tribution chain, sales have steadily grown, importation of components is going smoothly, reliable suppliers have been set up for raw materials and packaging, and all-in-all he thinks he has a winning business. But then an anonymous letter lands on his boss's desk at HQ alleging his Shanghai CFO and his National Sales Manager have been booking fictitious sales, they personally own some of the suppliers and distributors, which they run at the multinational's expense, they are filching the designs to set up a rival business, and to crown it all they have been orchestrating frauds against the Tax and Customs bureaus.

Should you believe it? What should the company do with the letter? Shred it? File it away? Keep quiet? Don't rock the boat?

The crimes alleged in this letter could clearly happen anywhere in the world. And China is not the only culture where people air grievances by writing an anonymous complaint. But denunciation letters have a long history here. In imperial times citizens reported on their neighbours in a system of mutual social policing. In Communist China, people have been encouraged to do it through posters or letters to the authorities. Legal hotlines have appeared in recent years. Some police stations, such as in the port of Dalian, advertise their "Reporting Mail Boxes" for people to denounce the crimes of fellow citizens, with special codes and password systems to protect informers and rewards for reports that lead to successful prosecutions. Such an anonymous letter accusing staff at a company in Shenzhen of a 730,000 RMB fraud led to a 13-year jail term for the main culprit. So, if the Chinese police take anonymous letters seriously, perhaps you should too. Many cases of fraud and employee corruption at business operations in China have demonstrated that you turn a blind eye to such an anonymous allegation letter at your peril.

In my experience, the anonymous letter is the most common means whereby a fraud is exposed in a China business operation. Of course there are other indicators: an auditor may discover ledger entries have been whitened out and overwritten, for example, or finance staff - peculiarly - are unwilling to take their holidays, or a customer complains about an inaccurate invoice, or customs officers suddenly raid your premises, or there is a pile of problematic receivables that none of our staff seems willing to pursue, and so on. There may be various triggers for a fraud investigation, but the most recurrent one in most of the frauds I have looked at in China is the ubiquitous anonymous letter. Either the anonymous letter exposed the fraud, or, while the case was being probed, it was discovered that there had been an anonymous letter some time ago pointing to this fraud, but it had been ignored or possibly even deliberately covered up.

The allegations contained in the vast majority of such letters turned out to be fairly accurate - once they were investigated. The motivation of the authors, however, was quite another matter and varied considerably.

A multinational retail chain in China received a spate of letters leveling a

range of fraud allegations against various managers in purchasing, real estate acquisition, packaging, and store operations. I concluded that the letters came from various sources with different motives. One set targeted a purchasing manager who had her eye on the other woman's turf. Another letter had come from a woman whose husband had been sacrificed to the police as a scapegoat after some irregularities had been discovered, and had ended up in jail. Another letter was written by a jilted lover getting revenge on her former Romeo.

In another instance involving a medical accessories manufacturer the letter came from an honest man who had been driven out of the company by corrupt elements because he was not one of the gang. His allegation that the national sales manager owned the distributors was bang on target.

In another case, the general manager of a healthcare company was the victim of a poison pen letter that - apart from accusations of embezzlement - alleged he had AIDS and syphilis! The letter came from a jilted lover.

Some letters related to multi million dollar frauds, others to smaller matters such as an administrator taking kickbacks from the printer and the travel agent, or owning an interest in a business that cleaned the firm's uniforms. Small though they may be, these deeds can equally corrode a firm's staff, become the company's culture and erode the bottom line.

In China, virtually nine times out of 10, the allegations touch on a Supply Chain Fraud situation. The classic scenario is that a senior local salesman or purchaser has set up his own companies and hijacked the sales or procurement business to enrich himself and his cronies. Typically he was hired early on when you were setting up shop, he became the key person and perhaps eventually a de facto general manager. He was the link in the big cultural and linguistic gap between the local people and the multinational. He brought with him a coterie of people who had worked with him before or were his college buddies or relatives. Together they set up what eventually became a shadow business, a parasitic business within your business that fed off the host body until it virtually killed it.

On the procurement side, a key employee or manager may have set up a string of vendors that supply your company with goods, materials and services. His companies are often registered under nominees to avoid detection. These vendors of his are phantoms that have virtually no physical existence. They have been inserted into the supply chain to take a cut - as much as 30% -- of all business.

On sales, a corrupt employee may have set up fictitious distributors that also have no physical entity but are inserted into the distribution chain to take a slice of profit for the rogue manager and his pals. Inevitably, this will also involve extensive kickback schemes, as well as smuggling, some of which may involve bribing local tax and regulatory officials and the officers of state owned enterprise, thus additionally exposing your company to prosecution under anti-bribery laws. In time, many of the receivables piled up by such rogue employees turn out to be uncollectable, possibly even fictitious.

So what do you do with these allegation letters?

Certainly, you do not shred them or toss them in the bin. File them away? Okay, but why not read them first? At least have a look at the letter and appraise its contents. Best of all, have a well-defined policy and a set of procedures for dealing with such letters and with all allegations of unethical behaviour. Anyway, whether the allegations are true or not, the letter is nonetheless an indication that all is not well within your operation. You have a problem - either white-collar crime or a problem of poisoned workplace relations and staff friction. As a manager, you need to be aware of these issues, and take action.

First, the letters will require analysis to assess the allegations and try to identify the author. In serious cases it is worth having the writing forensically analysed, comparing it to handwriting specimens of your employees; or if printed, then determine the type of printer, computer and paper used, because this could help you narrow down the likely origins of the letter; try to relate the contents to facts that may be contained in HR files, supplier lists, internal audit reports, recent dismissals and resig-nations, or to other letters received some time ago (if you didn't shred them).

An ethics hotline or similar whistle blowing mechanism is desirable to receive and process reports of unethical conduct - allegation letters, faxes, emails, voicemail or other communications. Operated by trusted and experienced HR and security professionals, the mechanism is an important tool to manage this information confidentially and to trigger the appropriate alarms and reactions when serious allegations come to the fore.

Having analysed a missive, the best course is to try discreetly to verify the allegations. The effort that goes into this can be based on the gravity of the allegations, for example how much money is at issue? Verification may sometimes be possible through simple checks of the HR file of the employee and one or two discreet interviews with any of his known enemies. You might, if you are lucky, match up the name of an employee's father with the name of a supplier. However, in practice, in most cases it will not be that simple. Verification will require a more thorough investigation.

Such investigation should be conducted by professionals, either an in-house security director, or a professional investigation firm, possibly both, and working closely with trusted internal auditors. They will need to conduct inquiries to determine the ownership of certain companies, they may need to conduct asset searches against key suspects and investigate past behaviour, track record and reputation as well as monitor their workplace activity. In some instances, it may be wise to arrange forensic examination of computers to search for evidence. Based on what is learned, it may become necessary to take countermeasures such as disciplinary actions, dismissals, lawsuits or file crime reports to the police. Whatever action a company selects, it should be based on an information first approach. Make sure that you have investigated the matter thoroughly, marshaled all the facts and consulted experts before taking punitive actions.