Reading the signs

Mónica Ramírez Chimal outlines some key detection methods for fraud and money laundering

Much has been written about fraud and money laundering (ML) prevention methods, but what about methods of detecting these crimes? Of course, fraud and ML are not the same thing. Broadly, fraud detection refers to the question: *"where is the money?"* while ML detection refers to the question: *"where does the money come from?"* However, fraud and ML do have a common denominator: the criminal seeks to hide the crime. Therefore, the detection methods described in this article can be applied to both (please note that the methods outlined below are not exhaustive).

Hotlines or reporting mechanisms

The key to ensuring that employees use hotlines or reporting mechanisms is that the individual reporting the fraud or ML must be protected and that the information must be treated confidentially. Moreover, it is important that reporting mechanisms are also available to providers and third parties (strategic alliances, partners, etc). You would be surprised at how many people are willing to talk using such mechanisms, but only if they perceive them as a serious tool and ►

In Brief

- **Similar methods can be applied for the detection of both fraud and money laundering**
- **Hotlines and surveys should ensure confidentiality and protection**
- **Exit interviews should be performed by someone from Compliance or Internal Audit**
- **"Keep an ear to the ground" and monitor both individuals' behaviour in the workplace and on social networks**
- **Seek to identify relationships between data from different sources**

are confident that the company will take action. Many companies assume that if they receive no reports, then everything is ok. They are mistaken! People often don't use hotlines either because they are afraid of the consequences of doing so, or because they don't perceive them to be a reliable source.

Surveys

Similar to hotlines, surveys should cover both employees and third parties, and should assure their confidentiality and protection. Moreover, surveys should be distributed on a random and ongoing basis. Survey questions should be phrased in a way that provides respondents with the confidence to answer without fear of retaliation. For example, you might ask third parties *"Do you enjoy a positive / professional relationship with our employee?"* or *"Do you want to change our representative?"* as opposed to *"Has our employee tried to bribe you?"* If the provider is honest, this will give them ample opportunity to report any misconduct on the part of your employees. It will also help you to measure employees' performance. For employees, change the wording to: *"Do you enjoy a positive / professional relationship with our suppliers? Which supplier gives you a 'headache'?"*

Audits or reviews

Your employees may well be jaded with the number of reviews carried out either by external auditors, internal auditors, compliance, or the regulators. Therefore, internal areas that manage the risk of fraud and ML are advised to conduct reviews on a random basis, so that employees cannot simply rely on the same reporting period or documentation used in external reviews. Methods and scope should be updated frequently and the review plans for these two areas should be rotated so that people do not know when the audit will take place.

Monitor

Once reviews or audits have been made, what happens next? In theory, auditors or the authorities will return the next year to perform a follow-up. In practice, however, resources do not always allow for this, meaning that audit/review reports may simply be "filed"/ignored.

The most important thing about any review is not what is observed, but how and when the company responds to any findings or recommendations. If an individual does not want to follow a review's recommendations to improve a process, this should be regarded as unusual. If their reason for not taking action is vague – or *"we have not had enough time"* – then this may be regarded with some suspicion.

People know that, whenever an audit takes place, the probability of having a follow-up may be low, due to time and resources. However, for effective detection, follow-up is a key tool. It is also important to keep track of those areas that have had more observations and the people involved in them. This should be compared with the information generated from surveys and hotlines, which could reveal "red flags" worth examining in greater detail.

Exit interviews

When people are about to leave a company they are more likely to speak openly and honestly about their experiences there. Exit interviews are therefore a key tool to evaluate performance, but also to glean information that could uncover fraud and ML activity.

The key to ensuring that employees use hotlines or reporting mechanisms is that the individual reporting the fraud or ML must be protected and that the information must be treated confidentially

In many companies, exit interviews are performed by HR. This is a mistake. Although HR may find something wrong, it is preferable if the interview is handled by someone skilled and experienced in identifying red flags. An individual's nonverbal communication – the way he looks at you, his gestures, how he is seated – can be revealing, while just one comment can provide an indication that it is worth asking more. However, if the interviewer is not trained to identify such signs, then the opportunity to acquire more information will be lost.

The solution is to appoint somebody either from Internal Audit or Compliance, who is trained to read such signals and can handle the interview appropriately. The interview should not become interrogatory, but nor do you want to miss opportunities.

It is also important to remember that fraud and ML can be performed by individuals of different genders, backgrounds, and job titles, including employees in cleaning roles, security, messengers, secretaries, and so forth. Do not be selective.

Look

It is important to get out of your office and study people and their place of work. Do you notice any changes that appear suspicious? Perhaps a photo on someone's desk of their latest expensive vacation? Have they recently bought a new house or car? Or have they recently revamped their image: a new watch, expensive jewellery or mobile, designer clothes or accessories? If any such purchases seem unusually extravagant or inconsistent with the individual's pay bracket, they may point to illicit activity. We have a saying in Mexico: *"the fish dies by its own mouth"*, so pay attention to details and be alert to individuals "showing off" newly-acquired wealth.

Social networks

Similarly, it is important to verify that Internal Audit and Compliance include in their plans the periodical monitoring of social networks. If someone is discrete in his outward behaviour or appearance, he may be less so in his online activities on Facebook, LinkedIn, Twitter, etc. Many cases have been reported of the police pursuing investigations after individuals have posted *"I killed my mother in law"* or extravagant pictures of guns, drugs, and so forth onto social media sites.

Use data

A wealth of information is available to you. It is important not keep this information in "silos", but to look instead for relationships between data from different sources. For example, if your company is a restaurant, the data from purchases, inventory and sales should be compared. If the restaurant has experienced increased demand, then you will have sold more, and this implies that more purchases of food and drink should have been made and so the inventory should have experienced high turnover. In other words, the three areas should be correlated. If not then something may be wrong. As another example, compare data from providers, employees and clients. Check for matches. This could be a helpful means of detecting fraud and ML as well as conflicts of interest. In both examples ask: do the findings make sense? If not, question the individual(s) concerned, and do not be satisfied unless they provide a reasonable explanation.

The most important thing about any review is not what is observed, but how and when the company responds to any findings or recommendations. If an individual does not want to follow a review's recommendations to improve a process, this should be regarded as unusual

Blind confirmations

Blind confirmations can be used with third parties and clients, who are debtors with your company. Write to them confirming that an amount is due but do not include the amount (hence "blind"). Compare their response with your records. Are they correct? If not, who is dealing with that client or vendor? The results of blind confirmations can be compared against the results of surveys, hotlines, audits and reviews mentioned above.

Visit

This is my favourite! Many companies do not take the time to visit a vendor or client's premises, due to lack of time or resources. In practice, if such a visit is undertaken before any commercial relationship is established, this can be a powerful prevention method to deter fraud or ML. I have witnessed many cases of major providers who, upon an unannounced visit, have turned out to be operating from facilities that either don't exist, are empty buildings, or are residential properties.

Keep an ear to the ground

Every company will have rumours or gossip circulating, either at the water cooler, in the aisles, in the smoking area, or the parking lot. Do not dismiss such information out of hand, as it may provide an indication of whether someone has addiction problems (drugs, alcohol, gambling), financial problems, or even a lover! This may sound laughable, but such matters have been proven in the past to be indicators that an individual is involved in a fraud or ML scheme.

Once fraud or ML is detected, it is important that the company follows up and takes action. Otherwise prevention mechanisms will not be effective because people simply won't take them seriously. Remember: actions speak louder than words...

Mónica Ramírez Chimal is Partner and Founder of Asserto RSC in Mexico City. (www.TheAssertoRSC.com)