

CEP

MAGAZINE

A PUBLICATION OF THE SOCIETY OF
CORPORATE COMPLIANCE AND ETHICS

MARIOS SKANDALIS

FCCA, CFE, CFC, FICA, FCG

DIRECTOR OF COMPLIANCE,
BANK OF CYPRUS, NICOSIA, CYPRUS

SUCCESSFULLY WALKING THE CROSSROAD OF SURVIVAL AND EXTINCTION (P10)

Minimize corruption risks by
rethinking your anti-bribery
risk assessment (P16)

Diversity and inclusion
start with us (P20)

How to minimize money
laundering, fraud, and
terrorist financing risks (P26)

Record management 101, Part 1:
Consider these principles (P32)



SCCE®

HOW TO MINIMIZE MONEY LAUNDERING, FRAUD, AND TERRORIST FINANCING RISKS

by Mónica Ramírez Chimal



Mónica Ramírez Chimal
MBA

(mramirez@asserto.com.mx) is
Partner and Founder of consulting firm
Asserto RSC in Mexico City, Mexico.

Money laundering, fraud, and terrorist financing — no one wants to be involved in these crimes, not even by accident. The consequences are momentous! The impact on the company's or involved person's reputation and image can last for years.

So how can an organization avoid being a participant in money laundering and terrorist financing, or becoming the victim of fraud itself?

In order to protect the company from these crimes, you need to learn what these concepts are so that key effective controls can be reallocated or set.

Basic concepts

To define the aforementioned concepts simply, *money laundering* is the process of making "dirty" money — profit from illegal or illicit activities — appear clean. *Terrorist financing* is to provide financial

support to terrorists, which can involve cash and any other type of asset. *Fraud* is the act of intentional deception intended to result in financial or personal gain. As you can see, the three concepts are different, but they have common factors:

- ◆ **Complexity:** All these crimes seek to be anonymous. Obvious, right? No one wants to be known as a launderer, fraudster, or a person who supports terrorism. Therefore, the person who commits these crimes will do it in a way that is complex, using other people (front men), several companies, different schemes, many layers, etc. — anything that helps create distance between the person and the crime.
- ◆ **Money and assets:** Of course, all these crimes involve cash and/or assets. For money laundering, intensive cash businesses are ideal since large amounts of money can

be laundered with relative ease. For terrorist financing, cash is needed, but large amounts aren't. Fraud, on the other hand, can involve cash, assets, and — contrary to the other crimes — even confidential information.

- ◆ **Creativity:** Every case of money laundering, terrorist financing, and fraud is unique, so the success of the crime depends on the sophistication and creativity of the criminal.

Key controls

There are many controls to prevent, deter, or detect money laundering, fraud, and terrorist financing. Some controls are more directly related to one crime, and others can be applied to all three. Here are the most effective controls.

Know your people

Know your customers, third parties, and employees. The criminal knows that companies don't always vet properly, so they take advantage. This is one of the main failures that contributes to the continuance of these crimes.

Know your customer (KYC)

Not knowing the customer leads to the abusive use of front and shell companies by criminals. Here are three basic and effective controls:

1. **Meet the customer in person at least once.** Consider that people can act as front men for criminals or use stolen identities. Meeting customers in person helps you confirm that they exist. Compare the customer's ID photo against the person in front of you, and compare the signature on the ID against the signature on the document. These tiny details
2. **Pay attention to nonverbal language.** Is the customer nervous? Do they have to check in with someone else to answer questions? Do you feel that something is not right? You do not have to be in law enforcement to detect something unusual. Pay attention to the details and trust yourself.
3. **Monitor the customer's activity.** Using what customers tell you, determine their profile to give you a better idea of what to expect. For example, if a customer told you they do business in Mexico, Spain, and Dubai, it would be unexpected if they start doing business in Brazil. Ask for the reason. Does the answer make sense? Is it reasonable? If not, it could be a red flag. Only time will tell if that person told you the truth. Monitoring your customer will help you prevent nasty surprises, like if that person is using your company to send money to terrorist groups.

Know your third parties (KYT)

You should not neglect knowing and reviewing what a provider, supplier, distributor, or agent is doing. Keep in mind that they are working for your company and essentially representing it. So, take your time to:

- ◆ **Make unexpected business visits.** This will help you identify shell and front companies and even slavery risks. And when you visit, ask yourself: Does the operation make sense? Do the facilities comply with all needed measures? Do the employees

look well? Observe these things. By doing so, you are minimizing money laundering, fraud, and terrorist financing risks.

- ◆ **Compare the vendor's database against customer and employee data.** Are there any matches? Criminals incorporate companies by using relatives, friends, or representatives, so some individuals share the same address or last names. Look for matches to avoid fraud procurement and money laundering.

**Every case...
is unique, so
the success
of the crime
depends on the
sophistication
and creativity
of the criminal.**

Know your employee (KYE)

Employees are the best and most important asset any company has, because they can protect it. They are natural gatekeepers if they are happy in the company. Therefore, it is important that companies verify whom they are going to hire and the employees they already have.

- ◆ **For new employees, call former bosses to learn about a person's development and behavior traits.** Do not rely on human resources, because they are going to give you

what is in the employee's file. It is better to invest time and get to know, firsthand, a person's work history. One of the most fraudulent documents worldwide is the résumé. If you add to this that many companies avoid public exposure for financial scandals, then there's a good chance that a criminal could walk freely into your organization. Therefore, it is important to corroborate what the résumé reflects with a person who worked with the candidate. One call could save you from having criminals working in your company. Don't hesitate to do so!

◆ **For both new and current employees, monitor their social network accounts.** In Mexico, we have a saying: "The fish dies by its own mouth." Sometimes ego is bigger than intelligence, and people post what they have done without thinking of the consequences. "I already took revenge on my boss and stole from the company!" or, "I am big fan of ISIS," or, "Just for transporting a package, they gave me a lot of money!" These examples are all red flags that should prompt the company to initiate an investigation. Remember that all information on social media is public, so check social networks every now and then. Much information can be obtained.

Lastly, for everything the customer, third party, and employee has told you, ask for the documents to prove it. That is called evidence. And verify that each document is legitimate and not fake.

Risk management

By knowing which risk is most likely to occur and its impact, companies can prevent it from happening. Knowing which areas, assets, and personnel may be more prone to money laundering risk, fraud, and terrorist financing will help to verify that the controls already in place are effective or if new controls are needed. It all depends on the company's line of business and its processes. For example, if a company is small, it will very likely have a concentration of functions in one person. In this case, the risk of fraud is higher. A person who carries out payments and also authorizes them, without any supervision, has the perfect opportunity to steal money. Similarly, companies that don't know their customers personally and don't run a proper investigation before accepting large sums of money could easily be used to launder money. Also, money donated to a charity by a company could be the perfect front to finance a terrorist group.

Risk management plays a key role to prevent, deter, and detect potential crimes.¹ It must be managed at a detailed level and updated at least once a year. Risks constantly change. What was a high risk yesterday could be a low risk today and vice versa. Risks do not disappear; they can only be minimized with effective controls, so companies should assess all the risks they are vulnerable to in order to avoid their materialization.

Sanctions

Companies must become more aware of how important it is to sanction in an adequate and timely manner.² Unfortunately, when there is a breach of the code of ethics or a policy, most

companies fire the employee or terminate their operations with the third party. The opportunity to continue committing the same crime is still there because the control weakness has not been corrected. Ineffective sanctions also contribute to impunity. And impunity leads to no one speaking up because they are too afraid. This happens for several reasons: fear of losing employment, fear of retaliation, fear that nothing will change. Do not let this happen! Companies must protect those who report and punish guilty parties fairly and within a reasonable amount of time — without exception. Just because a person holds a management position within a company should not mean that person is untouchable.

Training

Many companies see training as just another checklist item. It is often considered to be a burden, an expense, or something with little value. But training is highly related to the effectiveness of the employee. How else can they learn to detect fraud or a red flag for terrorist financing? Train your employees on a recurring basis and, if possible, with an external partner. This way, employees are more open, and best practices are also known. Every employee knows by heart their own processes, and if they also have training³ on money laundering, fraud, or terrorist financing risks, they can help to detect and prevent these crimes. Trained employees are the company's best defense — and investment.

Core values

We are all busy; it's easy to forget what we learned in ethics classes at university. Therefore, a refreshment

of values is needed at least once a year. In the meantime, use reminders for core values.⁴ Make them simple, interesting, and fun. Encourage a positive culture by emphasizing the good. By repeating to employees what good behavior is, they will learn that doing the right thing is what should always be done. By exalting the best of others, you will have more motivated and happier employees.

A note on risk management software systems

Companies should keep in mind that any system by itself does not minimize risk. For that to happen, a risk management system must be adapted to the company's processes and calibrated to produce the desired results. It must also be monitored to ensure the necessary adjustments are made for the system to continue to be effective. It can be the best tool


on the market, but without human intervention and monitoring, it will not work.

The best control is the one that minimizes risk regardless of whether it is manual or automatic. Risks are unique to each company.

It's about the company's controls, not the crime

Criminals have shown us that they are very quick to adapt to new circumstances. They have something we lack: patience. New methods to launder money or to give money to terrorism will arise, new cases of fraud will be exposed, and if we analyze them, we'll see they all have something in common: The criminal is counting

on weakness in the company's processes. The company's failures and ineffective controls make crimes possible.

Criminals look for the easiest avenue. They look for a country with lax laws or a company with employees who can easily be tempted. That's why even if a case is detected and exposed, the same method will be used in another company or another part of the world. But here is good news: Now you know how to lower your organization's risk of susceptibility. If the aforementioned controls are applied correctly, you can protect the company and yourself from money laundering, fraud, and terrorist financing risks. 

Endnotes

1. Mónica Ramírez Chimal, "Oldies but goodies," *CEP Magazine*, April 2016, 67–72, <https://bit.ly/31LT14M>.
2. Chimal, "Oldies but goodies."
3. Mónica Ramírez Chimal, "Get the \$ for your budget," *CEP Magazine*, February 2020, 30–34, <https://bit.ly/2YV1IZ0>.
4. Chimal, "Oldies but goodies."

Takeaways

- ◆ Money laundering, fraud, and terrorist financing have a common factor: Criminals use failures and ineffective controls to continue committing these crimes.
- ◆ Unscheduled business visits are a key control to help detect shell and front companies.
- ◆ Risks do not disappear; they constantly change and are variable. Only effective controls can minimize risks, and for that, risk management is essential.
- ◆ Effective sanctions are important, because if companies — without exception — punish consistently, fairly, and in a timely manner, employees will speak up, and impunity will fade.
- ◆ Providing proper training and reiterating core values help make employees the most protective shield any company can have.