

ON GUARD

WITH MORE THAN \$2 TRILLION LAUNDERED BY CRIMINALS GLOBALLY EACH YEAR, ANTI-MONEY LAUNDERING GOVERNANCE HAS BECOME A GROWTH AREA FOR CORPORATES. ROSE CHAPMAN EXPLAINS THE PRINCIPLES BEHIND CONTROL FRAMEWORKS

Money laundering is a growth industry that has taken on a new life online in recent years, proliferating fraud via the internet and resulting in more industries and professional services being subject to anti-money laundering (AML) regulation. There is both opportunity and need for organisations to engage more skilful and knowledgeable people to attend to money-laundering prevention. Money laundering spans across new industries and anywhere on Earth where the intention is for organisations to engage in international trade.

What is money laundering?

Money laundering is an activity that takes place following a criminal act of, say, drug trafficking, corruption, theft, fraud, tax evasion or bribery to make illegal monetary gains look like franked – or clean – money, which the criminal can then use safely and without detection.

So, essentially, money laundering is not the initial crime. A crime of theft, fraud or drug smuggling is perpetrated, and criminals working through the process of disguising the money into seemingly legitimate funds is the money laundering. Doing this well is such a focus for the money launderer that complex arrangements may be devised and more than five steps between carrying

out the predicate crime and benefiting from it would not be unusual.

Money-laundering activity is traditionally explained in the three separate activities of placement, layering and integration, and otherwise legitimate organisations are vulnerable at each stage.

- **Placement** is where the proceeds of crime are introduced to the laundering process. They may be placed in a bank account or other financial instrument, from where they can be forwarded to others.
- **Layering** is where funds are moved around financial services vehicles, such as from a fully paid insurance product that is cancelled quickly and then transferred into an investment product from the legitimate insurance source. The aim is for the bank or investment house to link the name of the insurer with a legitimate source of funds, and by doing this, the money launderer puts distance between the criminal act and the funds gained from it.
- **Integration** occurs once money launderers have distanced the funds from criminality; they can then withdraw funds as seemingly legitimate and more safely purchase retail goods or engage in activities of their choice and benefit from their criminal activity.



However, that process does not cover the many facets of money laundering, and other instances include:

- Facilitation of tax evasion;
- Giving cash payments for high-value goods;
- Hiding beneficial ownership of funds in shell companies; and
- Structuring or 'smurfing' large amounts of cash into smaller deposits and then withdrawing them as legitimate funds.

Money laundering in cyberspace

There is certainly a significant amount of online fraud, including ransomware attacks, where criminals take over computers of whole organisations. These are at such a scale that they receive high-profile attention. However, frauds where individuals are targeted and then led to divulge their bank account details or passwords are also prevalent. Regulatory regimes are expanding all the time to

include online activity. In the UK last year, for instance, HMRC expanded its list of businesses that should register under AML regulations to include online money service businesses, online bill payment service providers and digital payment service providers.

Global approach

Wherever your organisation is in the world today, to operate effectively in the international market, AML controls are increasingly essential for doing business. Countries that were staunchly nationalistic and resistant to the implementation of AML controls are increasingly moving towards them now, although resistance to this trend can sometimes be fierce and sustained. AML controls are defined in local legislation, but the core principles and requirements are all internationally defined.

The source of AML best practice and requirements is the 40 recommendations introduced by the Financial



Action Task Force (FATF), formed by members of the Organisation for Economic Co-operation and Development in 1989. These recommendations, first introduced in 1990, have been updated over time and are increasingly being enacted into local legislation and regulation. They provide a working template to apply locally. As always, implemented laws will differ among jurisdictions, but a globally applicable AML control structure that can be adopted and adapted to local needs would cover:

- A governance and control environment;
- Employee hiring, training and management;
- Business, product, geography and client demographic risk assessment;
- Initial and ongoing customer due diligence;
- Ongoing monitoring and transaction screening of customer activity;
- Data management and flows of information;

- Guidance and support to the business;
- Internal and external investigations; and
- Holistic monitoring and improvement of the system*.

Broader than financial services

Controls on the movement of money started in the financial services sector to stop the funds derived from drug trafficking crossing borders, but the money itself is laundered in the business and personal lives of criminals and, in this way, the proceeds of crime may pervade the otherwise legal income or activity of an organisation. For example, the proceeds of crime may pervade real estate, company services, accountancy and legal advice.

Organisations may also knowingly or unknowingly give criminals access to their services in cash-rich businesses, such as restaurants or launderettes, or by sharing payment services merchant access to the financial system,

giving rise to the risk of being an accessory to a crime. Artworks, diamonds and historical artefacts of high net worth can all be the currency of the money launderer rather than money itself.

The introduction of new legislation, including the EU's Fourth Money Laundering Directive, spreads the reach of financial services regulation ever wider and requires entities to show they have adopted a risk-based approach for AML activity in the financial and professional services sectors, as well as widening the focus of money-laundering control. Indeed, in *Action plan for anti-money laundering and counter-terrorist finance*, published in April 2016, the British government acknowledges the link between money laundering and terrorist financing.

Just as those organisations that are newly obliged to introduce AML controls can learn from those with established control set-ups, each country can benefit from the improvements in legislation taking place in others. Observation of the progress of other jurisdictions saves time and local development costs in coming to an appropriate starting point from which local regulations can be implemented. The controls that organisations, established or newly obliged, have to put in place to satisfy the 40 recommendations of FATF to prevent them being used for money laundering include:

- Assessment of the risk of the organisation being used as a vehicle for money laundering by criminals;
- Carrying out checks to determine the identity of customers, where they are natural persons;
- Checking the identity of the ultimate or beneficial owner of corporates and partnerships with whom

the organisation does business with;

- Having management control systems in place;
- Training employees so that they are aware of AML regulations;
- Monitoring customer activity in the use of the services of the organisation;
- Keeping adequate records of all required activities, including customer identity, beneficial ownership, financial transactions and governance controls, such as policies, procedures and processes; and
- Reporting suspicious activity to local country financial intelligence units via Suspicious Activity Reports.

As long as there is competition among nations for trade, there will be the development of AML laws and regulations providing controls for transactions in global markets. Competent authorities will provide sanctions in the form of fines and the removal of licences to operate in the market, but equally, organisations will wish to find ways to flourish.

I suggest heads of compliance and treasurers alike will need to constantly monitor customer activity to detect potentially suspicious activity being used by criminals to launder money, and to ensure that their organisations keep on the right side of AML compliance controls in finding ways to best develop and grow their business. 📌

Rose Chapman
is global head
of compliance
and ethics at
Travelport Inc



This article is an edited extract from *Anti-Money Laundering: A Practical Guide to Reducing Organizational Risk*, by Rose Chapman (Kogan Page, 2018). *This framework is described in detail in the book.