Thought Leadership

US SMEs

Acuris Risk Intelligence

Small or Medium Sized Enterprises - Their Role in Making the World a Safer Place

Money launderers and terrorist financiers have become increasingly skilful at finding ways to sidestep the law and use the global financial system for illegal purposes. Surprising as it may seem, as a small business owner there is still a lot you can do to stop them.

What you need to know?

The good thing about being a small or medium sized enterprise is in general, regulators think you represent lower risk to the global financial system. As a small or medium sized enterprise, you are still expected to abide by the AML/CTF regulations. According to compliance experts, the USA has one of the most robust AML/CTF regimes in the world.

The milestone law for AML/CTF - the Bank Secrecy Act (BSA), has been amended several times since being adopted in the 1970s, most notably by the USA PATRIOT Act after the terrorist attacks in 2001. The key institution safeguarding the US financial system from illicit use in money laundering and terrorist financing, is the Financial Crimes Enforcement Network (FinCEN), a bureau of the US Department of the Treasury.

What you need to do?

FinCEN requires you to confirm the size of your enterprise. There are three entity types each with different obligations – bank institutions, non-bank financial institutions and non-financial institutions. Understanding which category your business falls into is imperative, as is, ensuring your personnel are adequately trained and do not treat the review of AML policies and procedures as a one-off exercise.

Reviewing AML policies and procedures includes verifying the identity of any person you deal with and keeping a record of this information, including their name and address. You will also have to check if your customers have political connections and if they are on the list of known or suspected terrorists or terrorist organizations and/or if they have any sanctions imposed on them.

You will have to "establish risk-based procedures for conducting ongoing customer due diligence", meaning you will need to distinguish between high-risk, medium-risk and low-risk customers and monitor them on a regular basis to detect any significant changes in their profile, such as the volume of transactions made. If you detect something irregular, you will have to file a Suspicious Activity Report.

As of 11 May 2018, entities subject to the Bank Secrecy Act (BSA) will have stricter guidelines to follow concerning corporate clients - these entities will need to verify the identity of beneficial owners of firms they are dealing with, at the point the account was opened.

Translated into compliance language, "have to" means - depending on the type of your business, your customers will need to be screened against different data sets such as – PEPs Lists, Sanctions Lists, Adverse Media and Law Enforcement. For Financial Regulation sources an Enhanced Due Diligence (EDD) report may also need to be completed.

What happens if you don't?

If you **do not** do this yourself or you **do not** have a reliable provider who provides timely and accurate data, you will get fined (you will lose money), and suffer reputational issues and risk losing business partners (you will lose opportunities to make money in the future).

This happened to Miami-based brokerage firm E.S. Financial Services - in February 2016, they paid a $1 million penalty to settle AML charges for allowing foreign entities to buy and sell securities without verifying the identities of the non-US citizens who beneficially owned them.

A few months later, another broker dealer, Albert Fried & Company, paid a $300,000 penalty for failing to file a Suspicious Activity Reports (SARs) with bank regulators for more than five years.

Earlier this year, the small Merchants Bank of California was fined by FinCEN for *"egregious and wilful violations"* of AML laws. The company paid a $7 million civil money penalty for failing to establish and implement an adequate AML programme and conduct required due diligence on its foreign correspondent accounts, to detect and report suspicious activity.

We should always ask - are we happy to pay out large sums in fines if we don't have adequate compliance measures in place? Or could we save money by implementing a strong compliance solution and put potentially lost money to better use elsewhere. The above examples confirm, when it comes to spending money on compliance, investing in a good compliance solution now will save you money later.