GreenPoint>
Legal

ANTI-MONEY LAUNDERING: HEED THE RED FLAGS OR PAY THE GREEN FINES

Last year one of the world's largest banks was fined $1.9 billion after allegations of money laundering surfaced. Although the suspicion of a connection to drug dealers was never proven, laxity in complying with Anti-Money Laundering (AML) regulations was. It seems compliance—not the crime—is the AML risk benchmark today.

Money Laundering: Classic versus Contemporary

The classic description of money laundering goes like this: illegally obtained funds—whether from drug dealing, gambling or other vice operations—is classified as "dirty" and, therefore, needs to be "laundered" through a legitimate business or bank account in order to be used in commerce.

In 1989, the Financial Action Task Force (FATF) was formed to establish international AML standards to "promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system." In 2012, those measures were expanded to deal with the threat of financing weapons of mass destruction, and, more recently, FATF adopted standards to combat the exploitation of international trade as a venue for moving illicit funds through erstwhile legitimate trade transactions. Accordingly, trade-based money laundering (TBML) is now a focus of compliance monitoring. Clearly, the definition of "money laundering" has expanded.

FINRA's Red Flags

In 2013, the Financial Industry Regulatory Authority (FINRA) imposed $900,000 in fines against firms deemed to have "inadequate Anti-Money Laundering Programs." One firm failed to properly investigate six suspicious accounts that were all controlled by one customer using the same mailing address in Costa Rica but an email address for another customer as contact person. This scenario should have raised red flags for the firm's AML Compliance Officer, who was required to monitor potentially suspicious activity and investigate and report such activity by filing a suspicious activity report (SAR)—all of which he failed to do.

PEP—a Major Compliance Tool

The Politically Exposed Persons (PEP) list is made up of individuals flagged as "high risk AML customers" for banks. Compliance due diligence mandates that the list be examined before a bank engages in business with a person fitting the PEP profile or else face heavy fines for doing business with a person listed on the PEP list.

AML Best Practices

Monitoring unusually large deposits by a customer, cash-only businesses, certain service businesses or irregular real estate transfers are all part of AML due-diligence controls. Contact GreenPoint Global today to learn how we can assist your compliance team in creating a robust AML compliance protocol.

PETER K. OVERZAT, ESQ • 212.913.0500 x557 • 917.807.1321 • PETER.OVERZAT@GREENPOINTGLOBAL.COM
DAVID KINNEAR • 212.913.0500 x565 • 917.886.3222 • DAVID.KINNEAR@GREENPOINTGLOBAL.COM • WWW.GREENPOINTLEGAL.COM
A Division of GreenPoint Global