Putting the Bite on Money Laundering

Financial Services | Know Your Customer (KYC)

If you work in finance, it will not surprise you to learn that the world's leading enabler of financial secrecy is the US. The US now exceeds Switzerland as the most complicit country for helping individuals hide their finances.

Ironically, in most states, more personal details and proof of identity are required to get a library card than to form a company. And yet, the US is the last of the advanced economies not to require company ownership information that could help crack down on terrorists, human trafficking, drug lords, and those evading US sanctions.

Tracking money is complicated. Today we are not tracking coins from the ancient world, we are monitoring virtual currency and offshore banking on the darknet and in global integrated markets, making it almost impossible to trace money laundering, despite the great cost.

According to a US court settlement in 2014, JP Morgan Chase was fined over $2.05b for ignoring red flags surrounding the dealing of Wall Street financier Bernard Madoff, who used his account at the bank to run a $65b Ponzi scheme. HSBC also got their hands slapped with a $1.9b fine for failing to monitor more than $670b in wire transfers from Mexico and more than $9.4b in purchases of US currency in an elaborate system of deposits and money transfers that allow

Mexican and Colombian drug cartels to launder their illicit proceeds. And more recently, according to the *Miami Herald* headlines, two Ecuadorians are charged with money laundering in Miami that cost a police pension millions.

The economic impact of money laundering for financial institutions is undeniable. But greater still is the impact on socioeconomics, which goes beyond shady transactions. Money laundering finances not only terrorism but also human trafficking, which generates an estimated $150b worldwide per year, according to Financial Crimes Enforcement Network (FinCEN).

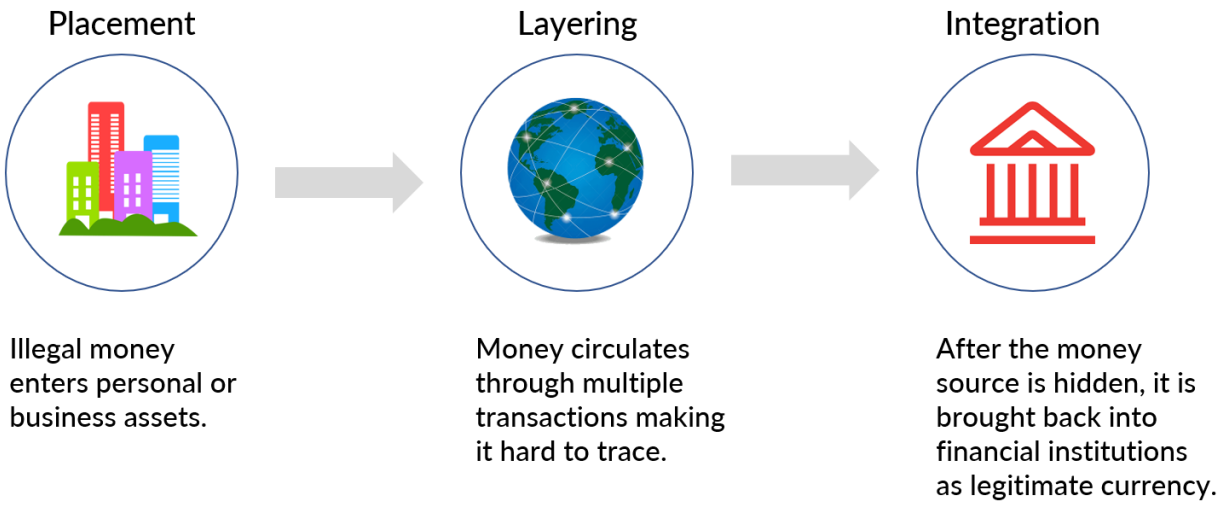
How Money Laundering Works

No one can say when money laundering first began. However, we can be confident that it has been going on for thousands of years—and it has been carried out in the same three basic stages used today. In fact, 2,000 years before Christ, Chinese merchants sometimes hid their wealth to circumvent taxes by investing in businesses in remote provinces or even outside of China.

To develop a strong defense strategy, one must look at how the age-old money laundering process works. And although there are three basic stages, it is important to note that these stages can sometimes overlap or appear in a different order—a nefarious strategy to further confuse regulators.

Stage 1: Placement

This is the riskiest stage for criminals because it can raise red flags for savvy banks who are looking for dodgy payments made into accounts.



At this stage, dirty money moves into the legitimate economy and away from its source. Then the source is hidden from view or disguised. Money laundering abroad is a popular method because it moves the money far from the geographical source.

Afterward, the money moves through financial institutions: shops, bureau de change, and other businesses, both local and abroad. The most viable institutions are those with variable costs, including car washes and casinos.

There are many ways that laundered money can be placed:

- Currency exchanges, through purchasing foreign money with illegal proceeds of crime.
- Smuggling dirty money across borders in suitcases and putting it into a foreign bank account
- Smurfing by sending small amounts of money to bank accounts that are below anti-money laundering reporting thresholds.
- Placing money into offshore organizations

Stage 2: Layering

This stage is often the most complex and involves making the money as difficult to detect as possible and moving it away from the original source.

The process is to layer multiple financial transactions to conceal a trail that could be audited and thus serve as a link to the original crime. It typically means moving money through multiple countries so fast that a financial institution cannot detect it.

Stage 3: Integration

The third and final stage of money laundering is successfully putting the "cleaned" money back into the economy. One of the most common ways of integrating money into the economy is through purchasing property or businesses.

Efforts to Prevent Money Laundering

In **1950**, the Federal Deposit Insurance Act was passed to govern the Federal Deposit Insurance Corporation (FDIC). The bill included a list of regulations that banks must comply with to remain insured by the FDIC, forming the foundation of modern know-your-customer (KYC) laws. Fast-forward 71 years, and financial institutions are still struggling with weak internal KYC policies.

To curtail money laundering, the US developed a legislative regulatory framework known as Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT). AML/CFT was founded on a risk-based approach for more than 20 types of financial institutions, including depository institutions, broker-dealers, money service businesses, mutual funds, insurance companies, and trust companies. Although some may consider this framework as having "weak oversight with dormant enforcement systems," it is, none the less, the basic groundwork that should bring immediate results through KYC policies.

So, if the money laundering process has virtually remained the same of thousands of years, why have we been unable to eradicate it at a fundamental level?

There are two primary components for building a strong KYC program:

1. **Back office**—the system that financial institutions use internally to manage customer onboarding and review documentation.

2. **Front office**—the experience customers have when submitting and verifying application information like name, address, workplace, and income.

Financial institutions have lagged in the adoption of new technology for decades. Although there has been a move to adopt a vigorous FinTech strategy for back offices, there is still a wide gap when it comes to tackling front offices, where institutions are most vulnerable—at the human level. This comes as no surprise; the financial market is highly competitive and introducing any friction in the customer-onboarding process could be costly.

Finding a Non-Compromising Solution

No one believes money laundering will ever be eradicated—after all, look at how long it has been around. There are, however, new technology solutions that are surprisingly easy and economically viable and can help manage risk and minimize the socioeconomic and financial impact of money laundering—all while helping financial institutions meet their compliance mandates.

Introducing a frictionless layer higher in the security stake can help rase red flags on possible criminal activities before they have a chance to create great or irreversible damage. And because we know how money launderers work, we know exactly where to place the traps.

Although passwords and two-factor authentication are good starting points, they are not without vulnerabilities. Humans are attracted to convenience, which is why passwords are easy to guess and seldom changed. And poorly implemented two-factor authentication can be beaten, or even bypassed entirely, just as single-factor authentication can. Verifying the same factor in two different ways is not true two-factor authentication. Although the user must provide a password and a verification code, accessing the code relies only on them knowing the login credentials for their email account, which is simply verifying the same factor twice.

We have already established that we are not going to eradicate money laundering across the board. So how does a financial institution best minimize money laundering?

After identifying their companies' jewels, CISOs will need to access their customer's friction tolerances. For example, members of smaller credit unions and community banks may have a low tolerance to adding additional onboarding friction, whereas investment bankers with high wealth customers may find that adding additional security measures will build greater trust and customer confidence.

For CISOs in the financial sector, having a strategy on a shelf will not be enough to mitigate the risks that come from money laundering. They will not only need to stay abreast of advanced verification and authentication technology but also need to champion changes within their ecosystems that have been in place for decades or maybe centuries—and that is not an easy task.