Bloomberg Law®

Corporate Law & Accountability Report™

MONEY LAUNDERING

Six Ways to Avoid Being Co-Opted Into a Trade-Based Money Laundering Scheme

By Ariel A. Neuman and Jen C. Won

The client was a company that had been in business almost 40 years, built up from nothing by two friends who immigrated to the U.S. without a penny to their names. It was in the import/export business and, unlike most competitors, did everything by the book: income was fully reported, taxes were fully paid, employees were documented, and there was no hint of the usual inventory- or customs-related shenanigans. But the call came in because – without any warning – all of the company's bank accounts had suddenly been frozen by the Drug Enforcement Administration. Where had this come from? What should they do? And how were they going to keep the lights on?

After a flurry of phone calls and negotiations, we were able to unfreeze the accounts and get a grasp on the situation. The DEA and a US Attorney's Office in a distant southern state suspected our client of laundering money for the Jalisco New Generation Cartel, one of the most violent criminal organizations in the world, best known for kidnappings and beheadings. The drug agents claimed that millions of dollars in drug trafficking proceeds had moved through the company's frozen accounts over the prior three years.

The owners claimed to have no idea. The employees said they had no information. And only after a robust internal investigation did we see what the DEA saw: the company had been used – its bank accounts appropriated, its lowest-level employees fooled – all for the benefit of the cartel. The company was an unwitting participant in the latest variation on one of the oldest crimes on the books – money laundering. And this scheme has a name: Trade-Based Money Laundering, in its most common form referred to as a Black Market Peso Exchange.

Trade-Based Money Laundering, referred to as TBML, involves moving the proceeds of criminal activity through trade accounts and international trade companies. Since the enactment of the Bank Secrecy Act and attendant anti-money laundering (AML) and know-your-customer (KYC) regulations, it has become more and more difficult for cartels and other criminal organizations to clean their money through the banking system. And so they have turned to companies involved in international trade. Companies that are moving merchandise and funds across international borders on a regular basis, whose accounts and businesses can be compromised and appropriated.

As in the case described above, the company management often has no idea that the enterprise has become an unwitting accomplice to a crime. Unfortunately, the fact that upper management may be blind to the problem does not prevent the federal government from going forward with prosecutions. Using some of the most aggressive forfeiture statutes on the books, and with the threat of massive financial penalties and

Former federal prosecutor Ariel A. Neuman is a trial lawyer and principal at Bird Marella, representing both individual and corporate clients confronting government investigations, including for money laundering, securities fraud, False Claims Act violations, health care fraud and other offenses. Neuman is also experienced in conducting internal investigations related to accounting issues, potential FCPA violations, and related matters for national and multi-national corporations. Jen C. Won is an associate at Bird Marella who focuses her practice on complex civil and criminal litigation. They can be reached at aneuman@birdmarella.com and jwon@birdmarella.com or 310-201-2100.

 ISSN 2330-6300

lengthy prison sentences in hand, the DEA and federal prosecutors have extracted felony convictions and huge fines from companies and individuals who found themselves in the middle of TBML operations.

TBML takes many forms. One of the largest TBML enforcement actions to date was in Los Angeles's famed Fashion District in 2014 – the federal government alleged that Fashion District businesses were knowing participants in a Black Market Peso Exchange. Simply put, Fashion District customers in Mexico purchased goods from the Los Angeles-based merchants. The Mexican customers delivered payment for the goods in pesos to an ''exchange house'' – Casa de Cambio – in Mexico, which offered a better exchange rate, lower wire fee, and less scrutiny than the traditional banking system. The Casa de Cambio then contacted associates in the U.S. to report the receipt of payment for a particular Los Angeles-based merchant. Those associates – having in hand cash proceeds derived from the sale of narcotics on the streets of L.A., San Diego, and surrounding areas – then delivered cash payment in dollars to the Fashion District business on behalf of the Mexican customers. And like that, the Mexican customer had paid for his/her purchase, the Los Angeles-based merchant had received payment in full, and the cartels had allegedly ''moved'' their dirty dollars from the United States and received ''clean'' pesos in Mexico.

Not every TBML case involves someone walking in the door with bundles of cash. Other variations range from depositing cash into company bank accounts on behalf of customers, to more complex trade diversion and invoice or bill of lading manipulation. But at the end of the day, the criminals' goals are always the same: to move their dirty money out of the United States while obtaining ''clean'' money in their locations of choice. And while some U.S. business owners are no doubt willing participants or willfully blind, most that we have encountered simply had no idea what was happening.

Don't Let Your Business Be Co-Opted by the Bad Guys

So how does a company that participates in the international flow of goods and funds avoid becoming an unwitting agent for a criminal organization? How do you avoid being caught up in a spiral of law enforcement investigation, sky-rocketing legal fees, and potential devastation of your business? And how do you stay out of jail for something you never knew you were doing? Unfortunately, businesses engaged in international trade have to act more and more like banks with sophisticated AML policies and procedures.

1. No Cash

Do not accept cash. Is it legal tender? Yes. Is it inherently suspicious in the business world? Yes. Can it cause you massive headaches? Absolutely.

We know that smaller foreign customers often prefer cash. We know that they are looking to avoid wire fees, find better exchange rates, and skirt their native-country taxes. And we know that most of them are just hard-working folks who are not doing anything wrong.

But we cannot say this strongly enough: deal in cash, expect to become a target. This is simply a matter of supply and demand. Drug organizations are sitting on so much physical cash that they do not know what to do with it. If you are a business accepting large cash payments, to them, you look like a hole in the dam through which their dollars can flow. And next thing you know, millions in narco-dollars are flowing through your accounts.

And the feds are paying attention. Various regulations require any businesses, and especially banks, to report cash transactions over $10,000. Understand that if the government does not trust people with large bundles of cash, neither should you, unless you are willing to risk coming under the government's microscope.

2. Know Who is Paying You

The vast majority of recent TBML cases in the United States have involved variations on a theme: an unrelated third-party making payments for foreign customers. Whether those payments are made in person, by wire, by ACH, or by bank deposit, third-party payors should send warning alarms through your compliance team. Investigate those who are paying you. Understand why your customers are using third-party intermediaries. Consider whether payment is originating from a location that makes sense (e.g., a Guadalajara-based company that has a third-party agent depositing money into your bank account in Chicago should raise questions).

Often enough, there are legitimate explanations for such practices. But unless a company understands exactly where its money is coming from, and why it is coming from someone other than the customer, management will not be able to answer law enforcement's questions when they come knocking.

Anything that seems out of the ordinary, suspicious, or strange should be looked at. And low-level employees who are usually processing payment and who are best placed to see strange patterns need to be educated. It is all too easy for the federal government to hold a company criminally responsible for the actions of its employees. And even if the DEA decides to give the company a pass on criminal charges, forfeiture and disgorgement of funds can have a devastating impact on your business.

3. Know Your Customers

Beyond knowing your payors, know your customers. Conduct basic due diligence on your customers. Do they have an online footprint? When you check street view/maps – does the address look consistent with expectations? Does it turn out that the customer buying hundreds of thousands of dollars in goods is located on a quiet residential street? Or the foreign equivalent of a Mailboxes, Etc.? Either of these may indicate that you are dealing with a shell company or sham entity, and should raise immediate red flags.

Does the buyer have an online profile? Has the buyer been linked to any negative or adverse news?

Finally, be especially wary of one-off transactions. Consider whether the buyer/transaction is different from those that you would normally engage with (e.g., the buyer's communication/focus, or the complexity or size of the transaction). Convoluted transaction methods should raise a red flag that a buyer wants a smokescreen, and may even be acting in the TBML scheme.

In any of these cases you will not necessarily need to cancel the sale. You will just need to investigate further if you want to protect yourself.

4. Check Your Invoices, Then Check Again

Significant discrepancies between values of goods reported on invoices and the fair market values of those

   ISSN 2330-6300

goods are a TBML red flag, as are shipment locations or terms inconsistent with the relevant customer. Often, one of the parties involved in invoice fraud is a front for a cartel or similar criminal organization. Invoice fraud takes more assistance from insiders, but a few bad apples taking kickbacks on the side can hide large movements of illicit funds.

> Under-invoicing: Under-invoicing involves an exporter selling goods for less than their true values, so that the buyer can then sell the goods on the open market for their fair market values. By doing so, the parties have moved value off-shore from the exporter's country of origin. Often, the exporter and importer have colluded to the point where the importer returns some portion of the additional proceeds to the exporter in an off-shore account. The remainder of the additional proceeds may then be transferred to the criminal organization or onward.
>
> Over-invoicing: Over-invoicing is essentially the reverse of the process described above, whereby value is moved from the importer's country to the exporter's. The exporter issues an invoice for goods in excess of their true values, and the importer pays the inflated prices. Portion of those funds go to pay for the goods purchased, while the remainder is diverted to the criminal organization.

In both of these scenarios, collusion between buyer and seller is necessary, but may not be obvious to upper management. Books, records and accounts may be doctored by insiders who are aligned with the criminal organizations. Thus, to avoid and detect these more sophisticated kinds of TBML, systems of checks and balances have to be instituted to ensure that no single actor can unilaterally alter the internal records to facilitate the illicit transfers of funds.

5. Do Not Be A Bank

This one is simple: if you are asked to pay or forward proceeds to an unrelated third-party, do not do it. Even if the third-party is another merchant selling to the same customer. Do not hold money for customers in your place of business or in your accounts. Your company is engaged in buying and selling goods. Your company is not a bank. And the only reason for someone to try to use your company as a bank is because that person thinks a bank would see whatever is being hidden from you. Do not be a bank.

6. Risky Jurisdictions Mean Risky Transactions

If your buyer is linked to jurisdictions known to be high-risk for money laundering activity, be very cautious. Entities in countries subject to U.S. sanctions or embargoes are working feverishly to launder their funds and send money offshore (and the number of countries on these lists is likely larger than you expect). For example, an Iranian company may set up a front company in Turkey, a popular offshore shelter, to enter into the sales of goods for highly inflated prices and move money out of Iran without alerting any sanctions breach.

As a precautionary measure, if you are doing business with companies in at-risk jurisdictions, be very careful. The U.S. Department of State keeps a list of countries that require extra vigilance (labeled as ''Jurisdictions of Primary Concern'' or, more bluntly, ''Major Money Laundering Countries''). These countries are vulnerable to international money laundering because of their weak or nonexistent enforcement regimes, according to the government. Businesses should closely monitor transactions involving countries on the State Department's list. If anything seems amiss, investigate.

Conclusion

One final note: ''willful blindness'' is as bad as intentional misconduct when it comes to money laundering. If a person turns a blind eye, deliberately avoiding learning facts that would reveal the truth, that person is as guilty as someone who knowingly and willfully engaged in the crime. So if you or your colleagues have any suspicions, take a closer look.

TBML is a recognized and growing problem that law enforcement is attacking from multiple angles. We regularly see innocent companies and executives caught up in investigations and criminal cases because their internal control systems were lax, because a few bad employees took advantage of their authority, or because no one thought to question the sources of funds paid for goods sold.

While companies need not take on the onus of implementing anti-money laundering policies required of banks, those engaged in international trade would be well-served to implement the six lessons above and do a thorough review of books and transactions if any suspicions arise.