THOMSON REUTERS
ACCELUS™

KNOW YOUR CUSTOMER— UNDERSTANDING THE AML THREAT BEYOND THE CUSTOMER

EUGENE McCONVILLE AND STUART WHATLEY

Statement of intent

This paper discusses issues beyond KYC as we know it to mean "Know Your Customer. We also investigate three criminal activities that either facilitate or lead to money laundering and involve seemingly normal business activities – Trade-Based Money Laundering, Missing Trader Intra-Community (VAT fraud) and Human Trafficking. We then spend some time demonstrating how a risk-based approach to KYC can free up compliance resources to focus on these areas.

THOMSON REUTERS™

ABOUT THE AUTHOR

Eugene McConville works as an independent Anti-Money Laundering (AML) advisor providing expert AML advice and training, including on the Suspicious Activity Reporting (SARs) regime. He retired as the head of Financial Intelligence at the Serious Organised Crime Agency (SOCA) in 2010. He has over thirty years law enforcement experience in Customs Investigations and SOCA, working in the UK and internationally on investigation and intelligence development in major drug trafficking cases, large Value Added Tax (VAT) and Excise fiscal frauds. He spent his last 10 years specializing in the anti-money laundering field, initially in investigation of serious money laundering offences by drug traffickers in a joint National Police/Customs team.

Stuart Whatley is Senior Director, Product Management, at Thomson Reuters. Stuart has been in Senior Product Management roles with Thomson Reuters for three years. Previously to that he was Global Product Manager at Complinet for four years. Working in compliance for over 10 years and with his experience as a former MLRO, Stuart brings insight and knowledge to AML and Anti-Corruption solutions and how they can benefit organizations.

CONTENTS

INTRODUCTION

This paper discusses issues beyond KYC as we know it to mean "Know Your Customer. We also investigate three criminal activities that either facilitate or lead to money laundering and involve seemingly normal business activities – Trade-Based Money Laundering, Missing Trader Intra-Community (VAT fraud) and Human Trafficking. We then spend some time demonstrating how a risk-based approach to KYC can free up compliance resources to focus on these areas.

KNOW YOUR CUSTOMER

> "I keep six honest serving-men
> (They taught me all I knew)
> Their names are What and Why and When
> And How and Where and Who."
> - Rudyard Kipling

It is highly unlikely that Rudyard Kipling had KYC in mind when he composed the poem above. But these considerations – What, Why, When, How, Where and Who – neatly encapsulate the process.

The "Who" of KYC

KYC is really about checking and testing a list of entities. While requirements may differ between different jurisdictions and regulatory regimes, you are generally required to understand:

- your clients' circumstances;
- their business;
- their source of funds;
- their source of wealth;
- the purpose of specific transactions; and
- the expected nature and level of transactions.

Regulators also expect that client information is maintained, current and valid – which implies that you should revisit your KYC regularly. If these are not your regulator's expectations, they are certainly KYC best practice.

While we all hope the occurrence of criminals in our customer and supplier databases, and among our business associates, is minimal, money launderers, terrorists and human traffickers are out there and they need the regulated sector to help launder the proceeds of their crimes.

As a Mexican intelligence officer once put it 'Reality is Classified'. Current criminal intelligence is not generally shared by law enforcement with private sector businesses anywhere in the world, and for very good reasons. If you should be so unlucky as to have a criminal as a customer, supplier or business partner, they are highly unlikely to give you any indication of their true activities or any of the dubious partnerships in which they are involved. In fact, they are likely to put considerable effort into passing KYC at take on.

Maintaining current and valid information necessitates ongoing monitoring of customers, and this might need to include knowing their business associates, business partners, customers and clients.

If we move to a consideration of KYC to take into account factors beyond the 'who', there are several aspects well worth looking at.

Know Your Country – the 'Where'

It is obviously important to know the country from which your customer originates, those countries they are involved with or become concerned with. It is important to understand what particular risks dealings with these countries represent to your organization.

As an example, your customer may be dealing with Latvia. You have assessed the risk of this

and you are content this activity is normal. Subsequently, the customer starts to have trade with Sharjah, an emirate in the United Arab Emirates that contains the port of Hamriyah. Hamriyah is a free zone, which, from a customs perspective, should be treated as a potential red flag. Sharjah also has a history as being used as a base for arms traffickers and was particularly Taliban friendly some years ago. So clearly, the countries with which your customer interacts can seriously affect the level of risk they carry.

Know Your Carnet – the 'What'

Where your clients are involved in international trade, how well do you understand your customers' shipping documentation? Do you ever seek access to it? There are definitely situations where you should understand what it is your customer is trading. We go into more details of the red flags in this area later in this paper.

Know Your Car – the 'What'

It is critical to have a strong understanding of your client's business. Take one example in a UK Customs case where the financial transaction seemingly concerned an expensive vehicle, a "Humvee", which was to be imported from the USA. Was it a wedding limousine or might it be a sanctions-busting armored vehicle for an African warlord? In this case the vehicle was purchased in the United States, which means US dollars were used. Which also means it is a financial transaction in which the US financial regulators will have an interest.

That Humvee was in fact seized in America following an investigation by British Customs. It was intended for the Liberian ex-president Charles Taylor, who was recently sentenced for war crimes at The Hague. This particular transaction was organized by a diplomat in London – a Liberian based at the United Nation's International Maritime Organization. It was facilitated by a London lawyer and financed through UK banks. The importation did not happen in this case, but this kind of transaction demonstrates the potential risks. It's worth thinking - what exactly are these goods, what is their purpose?

KYC_{3H8O} - Know Your Chemicals

Another example might include a client arranging finance for a transaction that involves a bulk consignment of a disinfectant - surgical spirits – that might be described in the paperwork as rubbing alcohol. It is often used in hospitals to disinfect hands when people enter the wards. However it also can be used as a precursor in the manufacture of Sarin gas.

So in any particular transaction, some questions you might also consider are:

- Are these dual use goods?
- Is a license required for export or import of these goods?
- Are these items listed on your country's strategic export control list?
- Are these substances subject to any end use controls?
- Are they subject to sanctions?

Linked to this, it is also important to understand your country's proliferation reporting responsibilities if there are any. In the UK, these are available via SOCA's FIU website, which provides a document that gives you guidelines for counter-proliferation reporting.

Know Your Conflicts

The US Department of Commerce reports that more than half the bribe offers reported to them are for defense contracts. Compare this with a share of world trade of less than one and a half percent for the arms industry. The arms trade is an opaque market, dealers operate across all

markets, licit and illicit – the formal, the grey and the black. Trade in weapons is assessed to account for 40% of global corruption. So if there are any indications of arms trading you will need to enhance your KYC.

TRADE-BASED MONEY LAUNDERING

There are three principal ways that money laundering takes place.

- Movement of value through the financial system
- Physical movement of cash
- Movement of value through the trade system

The movement of value through the trade system is what we mean by trade-based money laundering. It is defined as: The movement of value through the trade system using misrepresentation of the price, quantity or quality of imports or exports.

This is one of the principal, most successful and most difficult to detect methods of money laundering. Money laundered in this way is easily in the hundreds of billions of dollars per year.

It is a very challenging problem for everyone involved – law enforcement, regulators and the regulated sector – because individual transactions are hidden behind the immense volumes of trade flows. In 2008, there were almost 15 trillion dollars in global merchandise exports involving enormous volumes of foreign exchange transactions and diverse financing arrangements.

So it is difficult to detect because legitimate and illicit funds are commingled. There is a severe lack of understanding of traditional trade finance and supply chain logistics by law enforcement, as well as some parts of the regulated sector. There are also limited customs resources throughout the world to detect suspicious trade transactions. This all adds up to a significant risk of money laundering in international trade transactions.

Trade-based money laundering is often only detected when there is a specific investigation into a criminal network that reveals it. In recent years in the UK, we have seen money brokers who combine aspects of trade based money laundering with hawala. This involves hawaladars receiving cash from criminals in the UK and then making the value available in another country in whatever currency is required, after subtracting their commission. The hard currency held in the UK is then made available for overseas businesses who may need to make hard currency payments for the supply of legitimate goods abroad.

Trade-based money laundering also features in the money laundering typology, black market peso exchange. We witnessed an example in London a few years ago that involved trade-based money laundering and black market peso exchange conducted with a hawaladar. In this instance, the person conducting the transactions was a Turkish man who lived in Sweden. He flew over to the UK to conduct the transactions through London Money Service Businesses (MSBs). He obtained the funds from a Colombian who was the "cash pickup" man for a British organized crime gang that was importing cocaine in significant quantities into the UK. He gave the MSBs instructions to pay the money he gave them into the bank accounts of a series of legitimate companies in different countries. At the same time he arranged for Colombian pesos to be made available in Colombia to the Colombian drug traffickers. These criminals are out there, they are using the regulated sector, and they are using trade-based money laundering techniques.

While there are a number of variations on trade-based money laundering, it can also be as simple as purchasing commodities with criminal funds and shipping them to another country. That kind of transaction is extremely difficult to detect and to counter.

How value is transferred in trade-based money laundering

There are a number of different ways to transfer value by misrepresenting price and quantity in goods and services. These include:

- Over-invoicing
- Under-invoicing
- Invoicing the same goods and services more than once (double-invoicing)
- Multiple invoicing
- Short-shipping
- Over-shipping
- A deliberate obfuscation of the type of goods shipped
- Phantom shipping, where no goods are shipped at all and all documentation is completely falsified.

Each of these schemes allows movement of value to either benefit the buyer or seller of the goods. By overstating the value of goods shipped, over-invoicing, double-invoicing, under-shipping and phantom shipping allow the seller to gain excess funds as a result of the payment. Under-invoicing and over-shipping allow the buyer to gain excess value when the payment is made.

Red flags for Trade-based Money Laundering

There are a number of red flags that should prompt you to investigate further, when it comes to trade-based money laundering.

- Difficulty in determining the ultimate consignee of the shipments;
- Shipping routes that do not make economic sense;
- The amount of fund transfers is not consistent with the business;
- Shipments going to a known or suspected transshipment country;
- No obvious use for the commodity;
- Products or services don't correspond with the type of business;
- Payment in excess of, or below, the known market value;
- Significant discrepancies between the descriptions of the goods on the transport document (i.e. the bill of lading), the invoice, or other documents (i.e. certificate of origin, packing list, etc.);
- The consignor's business or location differs from the financial documentation;
- High value merchandise (e.g. precious metals and gems) transported to duty free trade zones;
- Third party payments for goods or services made by an intermediary (either an individual or an entity) apparently unrelated to the seller or purchaser of goods;
- Amended letters of credit without reasonable justification;
- Failure to produce appropriate documentation (i.e. invoices) to support a requested transaction.

Due to the difficulty in identifying this kind of money laundering, further investigation will require that you see a lot more than just the invoices around the transaction. You need to be able to understand bill of ladings and the other shipping documentation and you need to have a good grasp of whether the transaction makes sense.

An example of this was a trade-based money laundering scheme detected by US customs involving significant value of gold apparently exported from Uruguay. Ultimately, the customs officials realized that it was simply impossible for Uruguay to produce so much gold.

In my experience, if criminals have a scheme that is working for them, they will carry on with it for as long as it works. If they have help from someone in the regulated sector and no questions are asked, they will use the scheme as much as they can until the day it is stopped.

Two documents from the Financial Action Task Force (FATF) provide further information on trade-based money laundering:

- Best Practices on Trade-Based Money Laundering[1] – which provides useful background on the issue
- Global Money Laundering & Terrorist Financing Threat Assessment[2] – an extremely useful document for anyone involved in compliance. It looks at best practice as well as the "enablers" for money laundering activity. Often the key enabler for money laundering is the financial system – someone in the regulated sector. This document examines the drivers of a particular type of money laundering and lists the features of each type. This is very useful when conducting a risk assessment of your organization's vulnerabilities from money laundering. And not surprisingly, the list of best practices includes a recommendation that banks should examine import documentation.

MISSING TRADER INTRA-COMMUNITY (MTIC) FRAUD

Missing Trader fraud is a European Union (EU) fraud principally arising from the many different VAT rates across the EU. Where a customer in Country A acquires goods from a supplier in Country B (both in the EU), the customer acquires the goods free of VAT. The supplier (exporter) can reclaim that VAT he paid his supplier when he bought those goods, from his own national authorities. If the customer (importer) in Country A sells these goods, he should charge VAT on them and pay this over to that Country A's tax authority. If he goes missing and does not pay this VAT over, the tax authorities lose out, both through failing to collect the tax due and through making repayments to fraudulent claims.

Wikipedia defines MTIC as follows: "Missing trader fraud (also called Missing Trader Intra-Community, MTIC, or carousel fraud) is the theft of Value Added Tax (VAT) from a government by organized crime gangs who exploit the way VAT is treated within multi-jurisdictional trading where the movement of goods between jurisdictions is VAT-free."

One form of MTIC is carousel fraud. The HM Revenue & Customs website[3] in the UK gives several detailed examples of how criminals set these structures up, including one called contra trading. These structures seek to hinder the detection of the MTIC fraud. They do this by putting in various companies as buffers in the chain to sell goods on to people who will become missing traders. The goods are finally

exported out of the EU country and the VAT paid on purchase of the goods reclaimed. There were severe problems with these structures in the past, some of which started in the UK.

This fraud became quite prevalent in the mid-2000s and amounted to around £5 billion a year in the United Kingdom. Estimates in the EU put the cost of this fraud to governments around €100 billion per annum.

Europol's current assessments are that there are criminal groups based in the UK, controlled by masterminds in Dubai, who specialize in VAT fraud. These groups are actively creating networks of companies throughout the EU to establish fraudulent trading chains. Simultaneously, they are establishing accounts on financial trading platforms outside the EU to evade the attentions of financial regulators. Their aim is that most of the financial transactions will happen outside the EU for trading within the EU, and the groups will profit from fraudulent reclaiming of VAT from different national governments. This fraud is organized by criminals with active and sometimes passive cooperation of others who are looking to make fast and easy profits.

What does a missing trader look like?

The missing traders themselves are key to this fraud. They are the people that allow the criminals to claim they have paid the output VAT and therefore entitled to reclaim the input VAT they have paid. Missing traders are often young men, small fish who are easily replaced.

But they are not always young. One VAT investigation in the early 2000's involved a group of five London gardeners. These men went from gardening for around £25 a day to suddenly being involved in transactions of hundreds of thousands of pounds per day. This investigation led to the discovery of the trading of millions of pounds of computer CPUs by another new company, which had just registered for VAT. This new high-tech company was apparently being run by an 83 year old who had never been a director before, and whose address was a rundown social housing block in East London. This led to a new investigation, however within three months this company had become missing traders, leaving a VAT debt of £13 million. The gardeners were caught because the investigators knew who they were, but the masterminds behind this particular fraud remained undetected.

This extremely lucrative criminal business can be difficult to identify because it seemingly involves legitimate trading activity. HM Revenue & Customs (HMRC) have made a number of attempts to thwart this fraud which often involves zero-rating certain goods.

MTIC$_{O2}$

Carbon credit trading created a serious VAT fraud issue in the EU. Carbon credits are allowances for businesses to emit certain levels of carbon dioxide. As intangible goods that were subject to VAT, criminals quickly realized this was a fantastic fraud opportunity since there was no need to move any physical goods. All that was required was the transfer of carbon credit certificates.

A series of individuals received significant prison sentences for carbon fraud trading recently. Their scheme had set up bogus companies to import carbon credits, which were free of VAT because they acquired them in the EU. They then sold them on, charging VAT, and controlled all the different elements of the carousel, finally selling them on to legitimate companies to make the trade appear legitimate. The VAT charged by

these missing traders was then transferred to offshore accounts, in this instance to the United Arab Emirates, where it was shared between the gang. The proceeds were later transferred back to the United Kingdom. The ringleader, who was sentenced to 15 years imprisonment, used his proceeds to buy a million pound house in Gloucester Terrace in London as well as a Rolls Royce.

The authorities countered this fraud by zero-rating carbon credits. It is important to remember that this form of fraud can involve intangible as well as tangible goods.

While it is not possible to put an accurate number to MTIC fraud, a graph in a November 2012 Bank of England report indicated that MTIC is big enough to feature at the macro level.

There is a significant amount of criminal proceeds washing around under a veneer of commercial activity. Certainly, in the UK, customs has cracked down strongly on it and many UK fraudsters are likely to be involved in fraudulent chains that stretch into other EU countries where the authorities may not be focusing on it quite as strongly. These criminals are extremely clever and this is a very lucrative fraud.

A few of the red flags include:

- A new business operated by young men with no track record in that industry. The gardeners in the scheme we investigated went from £25 a day, to over £200 000 worth of turnover a day.
- Existing businesses that change their focus overnight. Businesses that already have a VAT number are the key to this fraud. So a red flag would be a business involved in trading clothing that suddenly gets involved in computer chips or some other high value goods.
- New people that have taken over a business and appear to be running it instead of the original owner.
- Has the turnover of the business grown unrealistically fast?
- Consistent, constant profit margins – you may find the business makes the same amount on each item sold.
- Dealing with goods from particular EU countries. From the UK perspective, the common starts to these carousel chains are the Netherlands, Spain and France and the common destinations are Dubai and Hong Kong.
- Financing suddenly received from foreign family members or from residents in countries where this fraud is organized (such as the UAE).
- Financing provided from within the trading chain itself. This includes back-to-back deals where the supplier is paid after they have been paid by the customer.

The initial goods these criminals favored - CPUs and the mobile phones – are now less of a problem because HMRC are very focused on compliance activities within that area. But these criminals are clever, they are determined and they will find other goods to deal in. It is critical that even those organizations operating outside the EU, who may feel that this does not affect them, are aware that they may be dealing with the proceeds of this crime.

HUMAN TRAFFICKING

The criminal proceeds from human trafficking probably already surpass drugs and it is likely they will surpass drugs and arms trafficking in economic terms in the very near future. At the same time, the risks to the traffickers are certainly very much lower than for other forms of trafficking.

Human trafficking is defined by the United Nations Office on Drugs and Crime (UN ODC) as: "the movement of a person from one place to another in conditions of exploitation using deception, coercion, the abuse of power or the abuse of someone else's vulnerability"

There are around two and a half million people trafficked every year, 80% of which are women and girls and 50% are minors. The true scale is very difficult to establish because of the covert nature of the crime - there is a lot of deception involved.

There are four broad categories of exploitation:

- sexual exploitation
- forced labor
- domestic servitude
- organ harvesting

Human trafficking generates considerable amounts of cash, much of which becomes visible in places such as Romania, where traffickers build huge houses, buy expensive cars and are in possession of large amounts of cash.

This is something that does occur in the UK. A recent case in the UK involved exploitation of forced labor in the tarmacking and block paving industry, controlled by members of the UK Traveler community. One extremely vulnerable individual had been too afraid to take his boots off at night for 15 years in case the people who controlled him called on him to conduct some minor domestic task. So there is slavery in modern UK.

A KPMG report into the 2013 horsemeat scandal highlighted the additional risk supply chains revolving around a web of international partners can bring. One study showed that from conception to consumption, there are more than 450 critical control points. That is up to 450 farmers, renderers, processors, packers and retailers in the average lasagna. This means there are opportunities almost every step of the way – the abattoir, the processing plant, the packaging plant – where checking needs to be done, not just at the end of the production line. While this report looked at the supply chain for fraudulent use of horsemeat, it could also be an indicator for the use of trafficked labor.

While human trafficking does not have a direct impact on the regulated sector, you will be dealing with companies in these industries - logistics businesses, labor-intensive businesses, hospitality, entertainment service and retail businesses. Where these businesses are harboring or deploying trafficked labor - unwittingly or otherwise - they can also be used for money laundering fronts and you may therefore be exposed to the proceeds of crime.

So human trafficking is our business, it is a big problem which we need to be aware of. FATF published a document in July 2011 called Money Laundering Risks Arising from Trafficking in Human Beings and Smuggling Migrants[4] which is very well worth reading.

Another document that covers this topic (as well as being very much up to date) is called 'It Happens Here', published by the Centre for Social Justice[5].

RELEASING RESOURCES TO LOOK BEYOND THE CUSTOMER

One of the major challenges facing compliance departments is freeing up the resources to do the extended due diligence that is required beyond the basics of KYC. Key to this is establishing efficient and effective customer screening programs. These allow you the opportunity to look at the other risks around transactions and behaviours that may expose your organization to the threat of money laundering or terrorist finance.

Such a screening program could consist of the following five steps:

1. Implement a risk-based approach

Focus your compliance efforts in the areas that pose most risk to your organization helps release the resources required to dig further and deeper into higher risk customers and transactions.

FATF released guidance in an update early in 2013 which defines a risk-based approach as focusing on "... risks in relation to types of customers, countries or geographic areas, particular products, services, transactions or delivery channels". The first part of this paper focused on products, services, transactions and delivery channels. The sections that follow focus on customers, countries, and geographic areas.

Identify and organize customers and/or suppliers in a meaningful way

The first step in implementing a risk-based approach is to identify and organize your customers in a way that ranks your risk. This allows you to record where your risk lies and what activities you have conducted on high-risk customers. It also allows categorization of medium and low risk customers. Customers should go through the risk-based approach methodology on a regular and ongoing basis to make sure changes in risk profiles are captured as customers move from low to medium risk, medium to high risk or even down from high risk. Important features of an effective screening program include:

- The ability to organize continual monitoring by customer risk priority – your screening policy may require you to perform adverse media scans for high-risk customers. You then need to be able to separate high-risk customers out of your database or you may end up screening every customer. This would generate a lot of material to go through. So the ability to risk rank allows you to focus your effort on high-risk customers.
- The ability to arrange the screening regime around risk priority – this ties in with how often you screen the various customer risk categories and what you screen those against. Hopefully your screening data can be adjusted to reduce screening on low-risk customers and increase it on high-risk. Reduced screening means fewer false positives to deal with and therefore fewer compliance resources required simply to clear down false matches against your low risk customers.
- Access to specific data such as country risk information - The first part of this paper highlighted the significance of geographic location in customer risk and this is corroborated by the FATF definition above. You need access to a service that will provide you with objective information to rank the risk associated with geographic areas. No country is exempt from risk, but where you have a small percentage of your customers operating in an acknowledged high-risk jurisdiction, it makes sense to focus more due diligence on those customers. That sort of approach should satisfy most regulators.

2. Know who you are monitoring and why

Many organizations underestimate the risk posed to their organization by bad data. For example, a customer database that lists a customer simply as 'Ahmed' or 'Mrs. Smith' makes it extremely difficult to do the correct amount of due diligence. It starts at the very core of your organization's data. If your data, your data collection and your historical data improvement policy and procedure

are not sound, there is already a serious risk before you even start screening, conducting enhanced due diligence or other additional KYC activity. The integrity of your customer data needs to be addressed as a priority.

Technology is no substitute for customer knowledge and good core customer data
Some technology companies will tell you they can embellish, enhance or clean your customer data. But your core system may well be subject to a review or audit at some point. It is critical that your core system is at the point where you know your customers as far as possible. At that point, you can pass the data on to your additional services, rather than relying on your additional services to attempt to clean it programmatically.

Data is the biggest cause of false positives
Poor data quality is one of the biggest, if not the biggest, causes of false positives. A name like 'Ahmed' will generate many hits against any screening database and data quality should be a key consideration of all compliance departments. When your team has to work several hours to clear down matches against 'Ahmed', and finding out who 'Ahmed' is in the first place, that is valuable time they could be spending on a higher risk customer.

The key message is that more false positives mean less time to focus on where the risks really are. If your data is right, you will know whom to focus on and you will have the resources to focus on where the real risk is.

3. Use well-researched data to create and facilitate a risk-based approach

The risk database against which you screen should be as broad as possible – definitely going beyond the normal regime of collating sanctions lists, regulatory lists, law enforcement lists and establishing a list of Politically Exposed People (PEPs). A list that highlights risk in an individual or entity before they appear on the official lists is invaluable, especially if it is built from independent research and analysis of publicly available information.

Once someone appears on the official lists, it is unlikely that you will want to do business with them. But a well-researched database starts a decision process of whether or not you want to do business (or continue to do business) with these people. And if you do, what further enhanced due diligence is necessary to provide you with the comfort you need to continue. Do you need to start looking more closely at shipping documents and the other considerations mentioned earlier in this paper?

There is an enormous amount of new risk data that becomes known each month, which brings tens of thousands of new people and entities onto risk databases or updates a similar number of existing profiles. So an entity on your books that has already passed onboarding may have new information revealed about them that might make you reconsider your relationship with them. This new information must be acted on in a fast and efficient way.

4. Screen names accurately at on-boarding

There are opportunities within certain systems to have different settings for initial screening and ongoing screening. So with a risk-based approach you could choose to do an adverse media search at the point of onboarding and not as part of ongoing screening.

- Identify the risk the customer presents as part of on-boarding
- Continually screen – work with a software partner that offers choices and understands one approach does not fit all.

An effective screening program continually screens for changes in risk of customers already onboarded. There are simple ways technology can help this process. These include flagging where a customer's address changes a lot, or where there are more than one customer with the same address. Another thing would be to look at how many customers you have with the same phone number. All of these things can be indicative of risk and flag areas where more attention is needed. Your software provider should be able to deal with client requirements on a client-by-client specific basis to get you what you need from a data and software perspective.

5. Regularly rescreen and perform enhanced due diligence for those flagged as high risk

Regular screening is very important and should form a significant part of a risk-based approach. This is in addition to the enhanced due diligence on those organizations, customers or suppliers that your programs highlight as high risk. Where your organization does not have the resources to justify setting up a full-time team of researchers, enhanced due diligence reports are essential tools for demonstrating deep research on high-risk customers. Essentially your organization can leverage the research capabilities of the service provider to gather a high degree of information on a high risk customer and file these against the customer profile for proof of due diligence should the regulators come to review your system.

CONCLUSION

There are several areas to consider beyond the common conception of KYC as well as some specific types of money laundering that should be factored in when structuring effective screening programs. In all situations, a risk-based approach to screening combined with relevant risk research data is not only best practice compliance, but also focuses compliance efforts on high-risk areas. This frees up resources to extend KYC efforts beyond basic onboarding and rescreening to best protect your organization from the risk of doing business with the wrong people.

This Expert Talk was adapted from the Webinar "Know Your Customer – Understanding the AML Threat beyond the Customer" presented by Eugene McConville and Stuart Whatley in March 2013. For a more comprehensive look at this issue you may like to view the recording of the webinar available at ***http://world-check.thomsonreuters.com/screening_kyc_aml_webinar_post-event***

Resources:

[1] http://www.fatf-gafi.org/media/fatf/documents/recommendations/BPP%20Trade%20Based%20Money%20Laundering%202012%20COVER.pdf

[2] http://www.fatf-gafi.org/media/fatf/documents/reports/Global%20Threat%20assessment.pdf

[3] http://www.hmrc.gov.uk/manuals/vatfmanual/VATF23300.htm

[4] http://www.fatf-gafi.org/media/fatf/documents/reports/Trafficking%20in%20Human%20Beings%20and%20Smuggling%20of%20Migrants.pdf

[5] http://www.centreforsocialjustice.org.uk/UserStorage/pdf/Pdf%20reports/CSJ_Slavery_Full_Report_WEB(5).pdf

POWERED BY WORLD-CHECK™ A THOMSON REUTERS BUSINESS

THOMSON REUTERS ACCELUS™

The Thomson Reuters Governance, Risk & Compliance (GRC) business delivers a comprehensive set of solutions designed to empower audit, risk and compliance professionals, business leaders, and the Boards they serve to reliably achieve business objectives, address uncertainty, and act with integrity.

Thomson Reuters Accelus connects business transactions, strategy and operations to the ever-changing regulatory environment, enabling firms to manage business risk. A comprehensive platform supported by a range of applications and trusted regulatory and risk intelligence data, Accelus brings together market-leading solutions for governance, risk and compliance management, global regulatory intelligence, financial crime, anti-bribery and corruption, enhanced due diligence, training and e-learning, and board of director and disclosure services.

Thomson Reuters has been named as a category leader in the Chartis RiskTech Quadrant™ For Operational Risk Management Systems, category leader in the Chartis RiskTech Quadrant™ for Enterprise Governance, Risk and Compliance Systems and has been positioned by Gartner, Inc. in its Leaders Quadrant of the "Enterprise Governance, Risk and Compliance Platforms Magic Quadrant." Thomson Reuters was also named as Operational Risk Software Provider of the Year Award in the Operational Risk and Regulation Awards 2013.

For more information, visit accelus.thomsonreuters.com

THOMSON REUTERS™