Brought to you by the publishers of COMPLIANCE WEEK

INSIDE THIS PUBLICATION:

The Challenges of Fighting

Money Laundering

An e-Book publication sponsored by pitney bowes

COMPLIANCE WEEK

Compliance Week, published by Wilmington plc, is an information service on corporate governance, risk, and compliance that features a weekly electronic newsletter, a monthly print magazine, proprietary databases, industry-leading events, and a variety of interactive features and forums.

Founded in 2002, Compliance Week has become the go-to resource for public company risk, compliance, and audit executives; Compliance Week now reaches more than 60,000 financial, legal, audit, risk, and compliance executives.

pitney bowes

Pitney Bowes (NYSE:PBI) is a global technology company offering innovative products and solutions that enable commerce in the areas of customer information management, location intelligence, customer engagement, shipping and mailing, and global ecommerce. More than 1.5 million clients in approximately 100 countries around the world rely on products, solutions and services from Pitney Bowes.

In the financial sector, Pitney Bowes makes it easy to overcome data limitations, so you can detect and resolve financial crime in less time with fewer resources. Our integrated, proven approach to entity resolution lets you quickly find, link and visualize complex relationships across parties, accounts and transactions. Key applications include:

- Anti-money laundering (AML)
- Know Your Customer (KYC)
- Fraud prevention
- Bank Secrecy Act compliance
- Sanctions screening
- Financial Action Task Force (FATF)

For additional information, visit Pitney Bowes at www.pitneybowes.com or request a meeting.

Inside this e-Book:

U.S. and U.K. Treasury Revisit AML Risks

by Jaclyn Jaeger

For the first time in ten years in the United States—and for the first time ever in the United Kingdom—financial institutions have some much-needed insight into how these two countries intend to prioritize money laundering and terrorist financing risks, enabling compliance officers in the financial services industry to better allocate their limited resources.

In October 2015, the U.K.'s HM Treasury and Home Office published its first national risk assessment of money laundering and terrorist financing risks. The report follows the release of the U.S. Treasury Department's own first-ever national terrorist financing risk assessment as well as an update of its national money laundering risk assessment, which was last updated in 2005.

Compliance officers will want to revisit these reports, given that regulators intend to use these assessments to inform new regulations. "We will use the information in these assessments to continue to adjust or develop policies to ensure that we continue to effectively combat money laundering and terrorist financing," Jennifer Fowler, deputy assistant secretary for the Treasury Department's Terrorist Financing and Financial Crimes, said in a statement.

Fowler cited as an example the Treasury Department's Financial Crimes Enforcement Network's customer due diligence rule, intended to clarify requirements for banks, broker-dealers, and other financial firms under the Bank Secrecy Act. The final FinCEN rule, published in May 2016, includes a new requirement to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions. The final rule takes effect on July 11, 2016.

Compliance officers in the United Kingdom can similarly expect a sharper focus on AML efforts. "The findings of the [national risk assessment] will shape the government's response to money laundering and terrorist financing and will inform the risk-based Anti-Money Laundering Action Plan that the Home Office and HM Treasury have committed to producing," the report said.

Some of the stated priorities of the action plan include:

- Enhance law enforcement response to tackle the most serious threats
- Reform the suspicious activity reports (SARs) regime
- Address inconsistencies in the supervisory regime that have been identified through this assessment
- Transform information-sharing between law enforcement agencies, the private sector, and supervisors

At a minimum, the AML reports give financial institutions more facts and trends to bolster their own AML risk assessments. "These reports should complement existing tools and resources for a risk-based approach to compliance," says Alex Zerden, founder and principal of Toccoa Strategies, an international risk advisory firm.

Vulnerabilities

In its AML report, U.S. Treasury said the underlying money laundering vulnerabilities remain largely the same as those identified in its 2005 report. These include:

- Use of cash and monetary instruments in amounts under regulatory recordkeeping and reporting thresholds
- Opening bank and brokerage accounts in the names of nominees to disguise the identity of the individuals who control the accounts
- Creating legal entities without accurate information about the identity of the beneficial owner
- Misuse of products and services resulting from deficient compliance with AML obligations
- Financial institutions wittingly facilitating illicit activity

"The first thing financial institutions can do is ensure that their anti-money laundering risk assessments provide broad coverage that addresses the specific money laundering threats detailed in the reports," says Fred Curry, a principal of Deloitte. An example of that, he says, might be focusing more on alternative payment mechanisms, including funds moved through mobile devices, pre-paid cards, crypto currencies, and third-party payment processors.

> "The first thing financial institutions can do is ensure that their anti-money laundering risk assessments provide broad coverage that addresses the specific money laundering threats detailed in the reports."
>
> Fred Curry, Principal, Deloitte

Additionally, Curry says compliance should target their training so that employees responsible for client on-boarding, account maintenance, and transaction monitoring know how to identify, investigate, and report unusual activity that may relate to the specific threats that are discussed in these reports.

Both the U.S. and U.K. AML assessments also similarly identified systemic failings in banks' AML compliance programs as another vulnerability resulting in the misuse of products and services to facilitate money laundering and terrorist financing. "Banks put themselves in a vulnerable position when they fail to maintain effective compliance programs," U.S. Treasury said in the AML report.

In the United Kingdom, the financial sector faces "significant intelligence gaps, in particular in relation to 'high-end' money laundering," the U.K. report said. "This type of

laundering is particularly relevant to major frauds and serious corruption, where the proceeds are often held in bank accounts, real estate, or other investments, rather than in cash."

The Home Office and HM Treasury judged the threat in this sector to be significant. Sixty percent of current money laundering cases under investigation by HM Revenue and Customs, the U.K.'s tax and customs authority, are the result of funds that were initially moved through banks, compared with 11 percent moved through money service businesses.

In fact, as part of its AML action plan, the Home Office and HM Treasury said in the report that one of its priorities will be to plug these intelligence gaps, "particularly those associated with 'high-end' money laundering through the financial and professional services sectors."

Emerging Threats

Fowler cautioned financial institutions to remain vigilant in updating their AML compliance programs, given that criminals are always finding new ways to exploit new products and services. "We expect institutions to identify and manage their own risk," she said.

One emerging threat identified in both reports, for example, are virtual currencies—BitCoin, in particular. "BitCoin and virtual currency operators can pose heightened money laundering risks as parties involved in such transactions are typically anonymous," says Curry.

Exacerbating the risk of virtual currencies is that many still have a limited understanding of how digital currencies are used for money laundering, according to the U.K.'s AML report. Nonetheless, the U.K. Treasury said "the money laundering risk associated with digital currencies is low, though if the use of digital currencies was to become more prevalent in the United Kingdom this risk could rise."

Terrorist Financing

U.S. and U.K. regulators' interest in terrorism financing also continues to rise. From a compliance standpoint, the United Kingdom noted a "marked overlap between money laundering and terrorist financing; both criminals and terrorists use similar methods to raise, store, and move funds."

Unlike the United Kingdom, the U.S. Treasury devoted an entire 70-page report to terrorism financing, warning that banks are an attractive means for terrorists "because of the speed and ease at which they can move funds within the international financial system." In particular, the report warned that some correspondent banking relationships inherently pose a higher risk due to the challenges of "intermediation," where multiple intermediary financial institutions may be involved in a single funds transfer transaction.

These relationships could potentially indirectly expose a U.S. financial institution to risk, including terrorism financing, if the foreign financial institution does not effectively implement AML and CFT (combating the financing of terrorism) controls, the report said. Knowing your customers and conducting enhanced due diligence on high-risk foreign correspondents are ways to mitigate financial crime risk, the report said.

Several banks today—such as Deutsche Bank, Barclays, JPMorgan, Citi, HSBC, and many more—are more efficiently reducing their risk related to correspondent banking through SWIFT's KYC Registry, an industry-driven financial crime compliance initiative. The KYC Registry is a secure place where banks can exchange KYC information on correspondent banks and share that information with selected counterparties in turn.

Treasury Acting Under Secretary Adam Szubin discouraged financial institutions from simply "de-risking" their operations by terminating, restricting, or denying services to high-risk clients. "We believe that most risks can and should be managed, not simply avoided altogether," Szubin said.

"We tell financial institutions to take a reasonable risk-based approach that addresses illicit finance risk on a client-by-client basis," Szubin added. "That means that we require institutions to be vigilant as they identify potential risks that different clients present and to design and implement effective AML/CFT programs that assess and address those risks." ■

AML CONTROLS

Below is an excerpt from the U.S. Treasury Department's anti-money laundering national risk assessment, outlining the Financial Crimes Enforcement Network's advisory to financial institutions.

In August 2014, FinCEN issued an advisory to financial institutions, including banks, calling attention to recent anti-money laundering (AML) enforcement actions and emphasizing the culture of an organization is critical to its compliance. FinCEN advised financial institutions that they can strengthen their organization's [Bank Secrecy Act] compliance by ensuring that:

- Its leadership actively supports and understands compliance efforts;
- Efforts to manage and mitigate BSA/AML deficiencies and risks are not compromised by revenue interests;
- Relevant information from the various departments within the organization is shared with compliance staff to further BSA/AML efforts;
- The institution devotes adequate resources to its compliance function;
- The compliance program is effective by, among other things, ensuring that it is tested by an independent and competent party; and
- Its leadership and staff understand the purpose of its BSA/AML efforts and how its reporting is used.

Source: U.S. Treasury Department.

Investment Advisers Next to Feel AML Scrutiny

by Joe Mont

Picture anti-money laundering regulations as a wall around the U.S. financial system. Despite the increased focus in recent years on these controls, two major gaps remain: the poor job institutions do assessing beneficial ownership, and the quiet fact that investment advisers for hedge, private equity, and other funds have no AML obligations at all.

That latter gap in AML defenses may soon be plugged. On Aug, 25, 2015, the Treasury Department's Financial Crimes Enforcement Network issued a notice of proposed rulemaking that would clarify the regulatory definition of "financial institutions" to include investment advisers with more than $100 million in assets under control and that are registered with the Securities and Exchange Commission.

For the first time, investment advisers would be required to establish a comprehensive anti-money laundering program and comply with reporting and record-keeping requirements under the Bank Secrecy Act. These programs will be subject to SEC oversight and examinations.

If all this sounds familiar, it should. This is FinCEN's second attempt to bring AML requirements to investment advisers. It proposed similar rules in 2003 that were seemingly abandoned. The proposed rule was published on Sept. 1, 2015, triggering a public comment period that ends on Nov. 2, 2015. The new requirements would go into effect six months after the release of the final rule.

"It is certainly déjà vu," says Duane Thompson, a policy adviser for fi360. "This has always been on the back burner, but a lot of people forgot about it because it has been a dozen years since FinCEN looked at it seriously. A lot of times when you see an agency come in and revise or impose new rules it means that somewhere there has been a problem." And yet, he adds, there is no record of any recent AML-related enforcement action against an investment adviser.

So why now?

"With the recent expansion of regulations into the non-bank financial institution space, coupled with the boon of money in hedge, venture capital, and other investment vehicles, the investment advisers area became a hole too big to ignore," says Micah Willbrand, director of global AML product marketing for NICE Actimize.

"I think regulators take the view that this is incremental," says Kim Mann, a partner with the law firm Pillsbury Winthrop Shaw Pittman's corporate and securities practice. "Now that we have gotten more advisers registered and subjected to additional rules and regulations, this is just one more look inside advisers and their funds."

Aaron Hutman, Mann's colleague at Pillsbury, sees the proposed rules as a side effect of "a surge in the AML space outside of core banking."

"Regulators have been hitting casinos for AML violations," he says. "They have gone after money services businesses and virtual currencies. There is real concern that there are more ways where money can slip through the cracks. Investment advisers are another opaque wall, behind which regulators would like to look and have confidence that there really is good oversight."

The proposal would require investment advisers to implement and maintain a written AML program, adapted to its business and clients on a risk-adjusted basis. Specific requirements include:

- Filing suspicious activity and currency transaction reports;
- Creating and maintaining records for each transmittal of funds greater than $3,000 and informing the next financial institution in the chain;
- Filing Suspicious Activity Reports (SARs) for transactions involving $5,000 or more in cash or other assets, if there is reason to suspect that the funds were derived from illegal activity, the transaction is structured to avoid BSA requirements, or it has no apparent legitimate business purpose.
- Filing Currency Transaction Reports (CTRs) for transfers of more than $10,000 in currency in the course of one business day, including multiple transactions by an individual or parties acting on their behalf.

Even for firms that already have an AML framework in place, a new rule would bring new costs and challenges.

In Aggregate, a Challenge

Costs may come from having a designated AML officer, bringing in external expertise, or appointing in-house SAR teams. "For some advisers, it will be a matter of human resources and human capital," Mann says. "Because compliance officers are stretched very thin right now, advisers are a little reluctant or unable to add staff to handle the additional regulatory requirements."

> "The best advice I can give is to be vigilant at account on-boarding to identify who an individual is, who they are transacting with, where their assets are coming from and what they are doing with those assets."
>
> Micah Willbrand, Director of Global AML Product Marketing NICE Actimize

The costs may be disproportionate for smaller firms, but "expensive for the big guys too," Hutman says. "They are going to have to engage in an AML risk assessment that goes beyond what they are already doing."

One challenge is likely to be the aggregation of transactions and identifying when a SAR or CTR must be filed,

plus what information needs to be included with it.

"These reports, even for experienced financial institutions, can be difficult to produce and populate with all of the required information," Willbrand says. "The best advice I can give is to be vigilant at account on-boarding to identify who an individual is, who they are transacting with, where their assets are coming from and what they are doing with those assets. The problem financial institutions get into, when they are not vigilant about the identification of their customers, business partners and assets, is that once an unidentified relationship or transaction enters the system, it's very difficult to trace back and identify."

Thompson also questions whether there will be regulatory redundancy because advisers conduct financial transactions through other financial institutions, such as banks and broker-dealers, that are already subject to AML requirements. Does it make sense to have the same compliance requirements at both the advisory and custodial firm level?

FinCEN did at least try to address redundancy, says Thomas Bock of K2 Intelligence, an investigative consultancy with an AML practice. The proposed rule says that if two parties are involved in a transaction, only one SAR needs to be filed. A related change may be more problematic. Historically, banks, broker-dealers, and mutual funds have shared SARs within their organizational walls. The proposed rule prohibits investment advisers from doing so in the absence of future FinCEN guidance.

The proposal doesn't require Customer Identification Programs, an odd omission given the focus on Know Your Customer requirements for other financial institutions. "It likely will be coming down the pike," Mann predicts. "It is really hard to imagine an effective program that doesn't incorporate some sort of KYC policies and procedures."

"I don't know if FinCEN is perhaps thinking this is something they want to expand to other areas and other entities that have to file SARs, but that is a very unique omission here," says Dana Syracuse, former associate general counsel of the New York State Department of Financial Services, now managing director of K2 Intelligence's AML practice.

And with new requirements also come new fears of CCO liability—a subject under much discussion at the SEC this summer, with dueling commissioners saying that fear is real or exaggerated. "These new requirements will likely bring more liability concerns to the CCOs of investment advisers, primarily because it reclassifies these firms as financial institutions which brings a higher level of scrutiny," Willbrand says.

While firms await the final rule, and take part in the ongoing public comment process, there are some steps to start considering. "Many of the large investment advisers do have, in some shape or form, AML policies and procedures in place," Bock says. "They should be taking a closer look to make sure that everything is covered and meets what the final rules may be."

Now is the time, he says, to develop a comprehensive understanding of all the different businesses and industries they work at and to develop a comprehensive, firm-wide approach.

Thompson is hopeful that FinCEN will act judiciously and consider the costs and challenges. "If you are an investment adviser out in Peoria, Illinois with $101 million under management and just barely eligible to register with the SEC, you might be a little bit perplexed," he says. "I hope FinCEN looks at either de minimus requirements or at specific business models to assess where the highest risk is to allow for reasonable carve-outs and exemptions for firms that don't pose any remote kind of threat." ■

PLUGGING THE GAP

Below is an excerpt from the Financial Crimes Enforcement Network's proposed money laundering rules for investment advisers.

As of June 2, 2014, there were 11,235 investment advisers registered with the Securities and Ex-change Commission, reporting approximately $61.9 trillion in assets for their clients.

As long as investment advisers are not subject to AML program and suspicious activity reporting requirements, money launderers may see them as a low-risk way to enter the U.S. financial system.

It is true that advisers work with financial institutions that are already subject to BSA requirements, such as when executing trades through broker-dealers to purchase or sell client securities, or when directing custodial banks to transfer assets. But such broker-dealers and banks may not have sufficient information to assess suspicious activity or money laundering risk.

When an adviser orders a broker-dealer to execute a trade on behalf of an adviser's client, the broker-dealer may not know the identity of the client. When a custodial bank holds assets for a private fund managed by an adviser, the custodial bank may not know the identities of the investors in the fund. Such gaps in knowledge make it possible for money launderers to evade through investment advisers rather than through broker-dealers or banks directly.

In addition to offering services that could provide money launderers, terrorist financers, and other illicit actors the opportunity to access the financial system, investment advisers may be uniquely situated to appreciate a broader understanding of their clients' movement of funds through the financial system because of the types of advisory activities in which they engage.

If a client's advisory funds include the proceeds of money laundering, terrorist financing, and other illicit activities, or are intended to further such activities, an investment adviser's AML program and suspicious activity reporting may assist in detecting such activities. Accordingly, investment advisers have an important role to play in safeguarding the financial system against fraud, money laundering, terrorist financing, and other financial crime.

Source: FinCEN.

Follow the money.

New technologies aid in the fight against money laundering, improve bank compliance.

Al Capone didn't invent money laundering — bandits have been concealing the origins of illegally obtained cash for thousands of years — but his actions may have birthed the term. Folklore has it that Capone, operating more than nine decades ago, legitimized his money through a commercial laundry.

The passage of time has lent Capone a little bad-boy glamour. Today, he's often viewed as less of a monster, more of a rogue. So he ran a little booze, banked a few games, bought a couple of politicians. These things happen. Chicago tourists now flock to ersatz speakeasies and take Untouchable Tours highlighting the city's gangster past.

No one will ever frame today's money launderers in such nostalgic terms. They're drug traffickers, human traffickers, arms dealers and terrorists. Sometimes, money laundering encourages crime by legitimizing its proceeds: it's fair to say that the child sex trade would stop if the cash it generates could not be used without swift and near-certain prosecution. Other crimes are actually enabled by money laundering. Al-Qaeda laundered money through the European banking system to fund the 9/11 attacks in the United States; drug trafficking proceeds now subsidize ISIS.

These activities are almost unimaginably broad in scope. The Financial Action Task Force, an international body that helps banks combat financial misdeeds, estimates that crimes giving rise to money laundering constitute between two and five percent of the gross world product, or between US$1.38 and US$3.45 *trillion* annually. This white paper will examine the current money laundering climate, anti-money-laundering (AML) regulations and new technologies that can help banks comply with them.

New criminal activity spurs increased regulation

Governments worldwide began ramping up AML regulations in the years following the September 11th terrorist attacks. "The number of AML regulations really ballooned, and continues to increase," said Richard Stocks, Pitney Bowes solution director for financial crimes and compliance. "Once upon a time, banks worked with a certain set of known rules and regulations. Things moved more slowly. You had time to learn how to accommodate the next regulatory change, the next risk. No more."

The barrage of new AML regulations ranges from Know Your Customer laws in about 80 countries to Financial Transactions and Reports Analysis Center guidelines in Canada, and from Anti-Money Laundering and Solvency II directives in the European Union to the Patriot Act and Foreign Account Tax Compliance Act in the United States. Additional regulations arose from bank self-policing organizations.

These regulations attempt to keep ahead of an evolving criminal marketplace. At a time when international crime is growing more vicious, new technologies offer innovative ways to engage in illegal activity. The Dark Web — a huge collection of web sites that hide the IP addresses of the servers running them, and that cannot be found via search engines — provides fruitful grounds for the purchase of armaments, explosives, drugs and even human beings. The rise of global financial markets, web-based bank-to-bank transfers — including transfers to "offshore banks" in countries with no AML laws — wire transfers, prepaid credit cards and hard-to-track Bitcoins and other virtual currency make layering easier.

That's why regulatory bodies not only pass new AML regulations, but also strictly enforce compliance. In a host of nations, regulators now scrutinize AML more than any other banking task. Failure to comply puts banks at risk of fines that can run into the billions of dollars, pounds, Euros or yen. Compliance failure also puts bank executives at risk of prosecution in some countries.

But despite banks' significant investments in AML manpower, platforms and processes, compliance isn't easy. Opaque and incomplete views of both internal and external customers stymie AML efforts.

The compliance challenge

Money laundering depends on anonymity: on the obfuscation of entities and transactions. Entity resolution and transaction monitoring systems can do much to hinder money laundering attempts. But like the analytic risk-scoring and re-scoring processes that gauge a client's propensity to launder money or commit other financial crimes, they work only as well as the data behind them.

Most banks today can only claim opaque and disjointed customer views. Customer information is often siloed, housed in databases on dispersed systems that have no way of communicating with each other. These include everything from customer information management systems to employee spreadsheets. And separate customer profiles may appear in different arms of the bank: in retail banking and mortgage departments, for example, or in commercial banking and credit card divisions.

The result of all this? Individual customers often have multiple profiles containing inaccurate, incomplete or conflicting information.

One entity, many names

Name variations are just one example. A married woman named Mary Anne Jones may have signed her name, on different accounts in the same bank, as Mary Anne Jones, Maryanne Jones, Mary A. Jones, or M.A. Jones. Another set of accounts may use these same variations attached to her maiden name, Brown. A third group of accounts may use these variations plus a hyphenated last name, Brown-Jones. Most banks cannot effectively coalesce all the information contained in these various accounts into one profile for this single entity. Therefore, banks are unable to examine this entity's transactions, networks, and the locations in which she does banking business.

"The way things are now, I may have a retai banking perspective of Mary Anne Jones," said Robert Smith, Pitney Bowes financial crimes managing director. "I can see that she has a healthy checking account, that she pays the same bills every month. But I can't connect her with the Mary Anne Jones working in the institutional arena. I can't see that she works for a large corporation that manufactures bomb parts, and that's trying to do business in Syria. So the bank has an extremely low risk score for the first Mary Anne Jones, and an extremely high risk score for the second. Banks need more clarity into whom they're doing business with in order to have more confidence in their risk profiles."

Unresolved identities also bedevil transaction monitoring systems (TMSs), which screen for and alert to 26 money laundering scenarios based, in part, on the entity's risk scores. To work effectively, transaction monitoring systems (including programs from NICE, Oracle and Norkom, along with home-grown systems) and bank customer information management systems need a clear and complete view of each entity doing business with the institution.

A deluge of false alerts

Inefficient entity resolution and transaction monitoring put banks at risk for non-compliance. False negatives occur when the TMS doesn't alert as it should and criminal actions go undetected. Far more often, up to *95 percent* of the time, by some estimates, the system will return a false positive. Current inefficient, manual investigative practices leave bank investigators needlessly wading through 95 percent of the entire alert pool simply to reach the five percent of all alerts that truly need scrutiny.

How can this inefficiency play out? Let's reconsider bank customer Mary Anne Jones. The bank is concerned that Jones may be trying to structure money through its system, regularly making individual deposits of $3,000, $3,000 and $4,000. The bank believes these deposits may represent an attempt to skirt United States AML laws, which mandate that any single transaction of $10,000 or more be investigated. But because the bank was never able to fully resolve the identity of the Mary Anne Jones with the possibly-structured

Technology can help resolve entities

To more effectively and cost-efficiently comply with AML mandates, banks can deploy software systems that improve entity resolution by **finding** and **linking** data and by improving investigators' ability to **visualize** relationships.

These systems help organizations **find** customer information wherever it lives in disparate, siloed systems and departments within the bank. They scour retail banking, credit card, mortgage, business and investment accounts, among others, to automate the process of compiling a comprehensive profile of each customer, and on the external parties with whom bank customers do business, in accordance with Know Your Customer and Know Your Customer's Customer requirements.

Software systems can then **link** data from multiple sources to a specific entity and its customers. Insight into the method of money transfers used, including bank transfers, wire transfers, counter withdrawals, checks and credit cards, should be included. This linkage eliminates the need for investigators to follow or manually reassemble long digital or paper trails to uncover information about a specific bank customer and the entities in the customer's network.

Information should be digitally presented in such a way that bank investigators can easily **visualize** the client's history with his or her networks and the institution itself. Additional capabilities should enable modeling of relationships across roles, processes and interactions.

The Pitney Bowes solution

Pitney Bowes Entity Resolution for Financial Crimes and Compliance is a software solution that helps banks worldwide more efficiently and cost-effectively detect and investigate financial crimes. It builds on Pitney Bowes Spectrum® technology and advanced algorithms to provide the find-link-visualize capabilities previously discussed.

Pitney Bowes software first **finds** customer records from across the myriad systems in which they reside. It then leverages Pitney Bowes' database of millions of addresses, names and name variations — covering 143 cultures and 240 geographies — to **link** records to unique parties and to determine inter-party relationships.

These capabilities, coupled with the ability to transliterate non-Latin alphabets into into the Latin alphabet and vice versa, enable banks to take into account name and address variations when resolving entities globally. The solution helps banks see, for example, that a customer going by the first name "Michael" in the United States may use the first name "Mikhail" in Russia or "Muhammad" in Egypt. Or that addresses recorded alternately as 42 Oakdale Street and 42 Oak Dale Rd. coalesce into 42 Oak Dale St. (See Figure 1).

Linking continues as the Pitney Bowes solution normalizes and standardizes names and addresses, so that each entity doing business with the bank can be provided its own unique identification number for use throughout the institution. Data from multiple sources can then be appended to this specific entity, improving insight during investigations. Records can be compiled on an individual, household, or organizational basis.

Pitney Bowes' **visualization** capabilities allow investigators to access this information via a single link in a Pitney Bowes knowledge hub. There, they find all the information the bank has compiled on a given customer appended to that customer's unique identification number. This process eliminates the need to follow long, confusing paper trails.

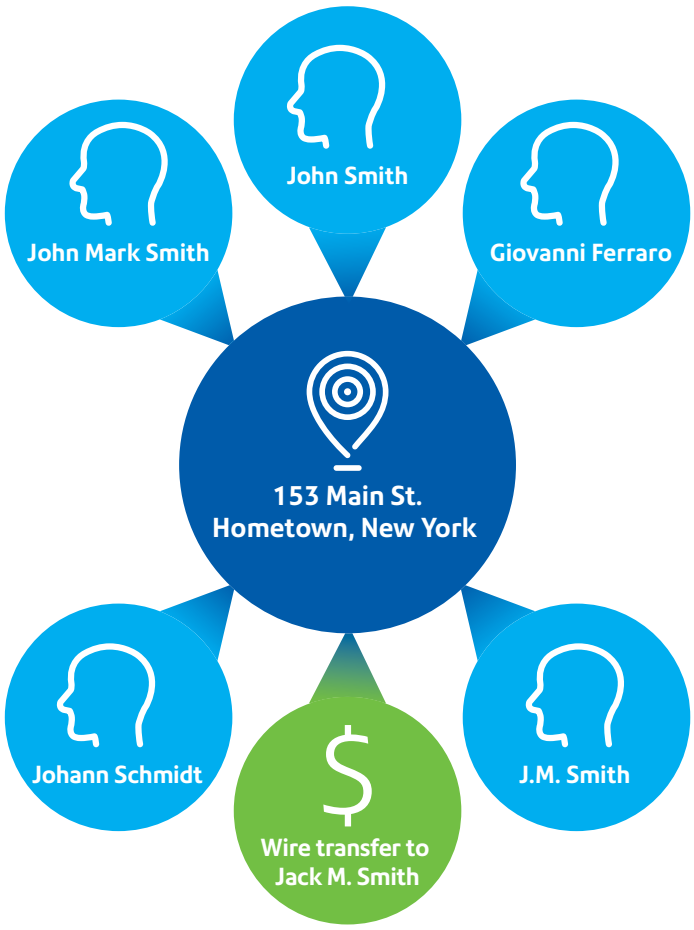


Figure 1: Pitney Bowes Entity Resolution for Financial Crimes and Compliance can help coalesce many names into a single entity. As illustrated here, the solution is helping the bank coalesce six name variations into a single entity by linking all those names to the same home address.

Benefits

By improving entity resolution, the Pitney Bowes solution can help banks avoid the fines and prosecution that accompany non-compliance. Since the solution improves investigative efficiency, it can save banks from the need to hire new personnel. Additional benefits include the solution's ability to unlock value from existing AML investments and to improve marketing efforts. .

Pitney Bowes Entity Resolution for Financial Crimes and Compliance is not a TMS or customer information management system. Rather, the solution improves the accuracy and precision of data flowing through existing platforms while comprehensively orchestrating that flow to support existing systems and processes. This saves organizations from the burden and expense of replacing TMS and customer information management systems in order to improve entity resolution.

In addition, banks often find that, while the Pitney Bowes solution has been designed to help with the mandates of Know Your Customer and other AML regulations, it can also aid in achieving the 360° customer views needed to optimize marketing efforts. With a complete view of each entity doing business with the bank, the financial institution can better tailor marketing to meet the needs and circumstances of each customer.

Improve entity resolution at your bank

Money launderers are always looking for new ways to integrate the proceeds of their crimes into the legitimate financial stream. Today, money launderers in the United States hire broad networks of "smurfs." These are low-level criminals who will deposit amounts of just under $10,000 into launderers' accounts, circumventing AML laws.

Criminals are also increasingly laundering money through smaller regional banks, believing that these institutions do not have the millions to invest in the processes and technology needed to effectively resolve entities.

To curb this scourge and comply with the ongoing barrage of AML regulations, banks need to improve entity resolution. Cutting-edge technology can help in this effort. Pitney Bowes has been in the business of data structuring and linkage for more than 95 years. Our solution calls upon our proven technologies in data intelligence to help in the fight.

For more information, visit us online:
pitneybowes.com/us/aml

For more information, visit us online: pitneybowes.com

RECYCLE PLEASE
recycleplease.org
15-MKTC-09969

FIFA Saga Makes Banks Fear Due Diligence Failures

FIFA lesson: "It is not enough to know your customer. You have to know what to expect from your customer," says Washington attorney Ross Delston

by Joe Mont

All over the world, media outlets have detailed the bribery scandal that toppled leadership of the Fédération Internationale de Football Association, the international governing body of professional soccer.

In May, the Justice Department indicted 14 people on corruption charges. Among the allegations are that Jack Warner, FIFA's former vice president, accepted a $10 million bribe to secure South Africa's bid to host the 2010 World Cup.

The indictment names 26 banks that did business with FIFA—including Bank of America, Barclays, HSBC, Citigroup, and JPMorgan Chase—in its litany of various bribery schemes. No wrongdoing on the banks' part is alleged, but financial institutions can expect to be on the hot seat for a long while as their role is scrutinized.

Banks received grand jury subpoenas because the government needed to find the FIFA money trail, explains John O'Donnell, a partner with the law firm Herbert Smith Freehills' corporate crime and investigations group. He believes the banks should now step back and evaluate whether they committed any compliance missteps that could cause headaches later.

"Anybody who received a subpoena will want to take a look at the account that is at issue, how the account came to be opened, and what know-your-customer due diligence was done with respect to the account," he says. "Some of these accounts were set up as pure conduits for the bribe payments, so they are a little suspicious in terms of who the account holder was, where they were located, and things like that. I suspect that the government will have conversations with these banks about what kind of due diligence was done in terms of opening the accounts."

Banks, already under heightened scrutiny by regulators for their KYC and anti-money laundering programs, can expect more of the same in the aftermath of the FIFA sandal.

"Part of our investigation will look at the conduct of the financial institutions to see whether they were cognizant of the fact they were helping launder these bribe payments," Kelly Currie, acting U.S. Attorney for the Eastern District of New York, said at a press conference announcing the FIFA indictments. "It's too early to say if there is any problematic behavior, but it will be part of our investigation."

Currie's words make it clear, particularly for banks that opened and maintained accounts used by the recipients of bribe payments, "that they have to be very concerned about what procedures they followed when opening those accounts," O'Donnell says.

Many banks, O'Donnell expects, will defend their due diligence efforts by noting that transactions were funneled through legitimate sports marketing companies, masking indications that bribe payments were made. "One argument they can make is that there wasn't a real pattern that would raise a red flag," he says. "The defense would be that these were legitimate people."

On the other hand, O'Donnell adds, "the government's response will be that FIFA has been fairly well-known to be corrupt for years, and that should have prompted more scrutiny to some of these related accounts. The takeaway is that even accounts that appear on the surface to be legitimate accounts sometimes require an added layer of scrutiny and due diligence."

Another scandal-related lesson for banks is to pay more attention to "politically exposed persons" (PEPs) and non-governmental organizations, focusing on due diligence controls that may flag problematic situations, says Henry Balani, head of Innovation for Accuity, a firm that provides AML and compliance solutions for banks and corporations. Transaction-level oversight by banks could have prevented years of bribery, "and banks should have known better," he said.

Balani emphasizes the importance of maintaining and consulting PEP lists. The challenge is that no formal PEP database exists—nothing akin to, say, the sanctions list maintained by the Treasury Department's Office of Foreign Assets Control. Companies must develop or acquire PEP lists themselves, typically following definitions developed by the groups such as the Financial Action Task Force or the Organisation for Economic Co-operation and Development. The lists include individuals who are (or have been) governmental figures, senior executives of state-owned corporations, political party officials, or prominent members of an international organization.

A check of the PEP list Balani's firm maintains, for example, that both Warner (the league official featured prominently in the indictments, and a one-time politician in his native Trinidad and Tobago) and Sepp Blatter (the former FIFA president who stood for a fifth term in office in 2015, won re-election, and then promptly resigned) are on the list. This indicates that FIFA deserved greater scrutiny from an anti-corruption standpoint than it received, Balani says.

"It is not just simply looking at politically exposed persons as an entity. The next step is trying to understand the risk that particular organization poses by having PEPs on [the company's] board," Balani says. "A lesson learned here is that banks didn't do adequate due diligence around FIFA because it wasn't flagged as a potential PEP-related organization. Now [banks] may want to go back to major corporate clients and start to understand whether they also have PEPs or not, asking whether they effectively assessed the risk levels associated with those organizations."

Banks will also need to pay extra attention to due diligence efforts for high-net-worth customers, says Ross

Delston, a Washington-based lawyer and AML compliance expert. "It is not enough to know your customer," he says. "You have to know what to expect from your customer. If you are getting money transfers in amounts and volumes and originators who any one of which you are having trouble understanding or explaining, you need to look further."

The good news for banks is that financial regulators have already been leaning on them to improve onboarding and monitoring processes anyway; the FIFA scandal simply underlines the point in a dramatic way. "That means that a bank can never do enough customer due diligence," Delston says. "They can't ever understand the customer's business and personal transactions enough to ever rest."

In the past, FIFA would have been overlooked as an organization that warranted an extraordinary degree of due diligence. "I think it is clear now that no company, organization, or individual is exempt from a higher level of due diligence," Delston says. "There was a time when high-net-worth individuals, and people associated with prominent companies and organizations, would have been exempt from additional scrutiny. Today, not only is no one exempt, but those types of individuals should be subject to greater scrutiny and the banking regulators expect it."

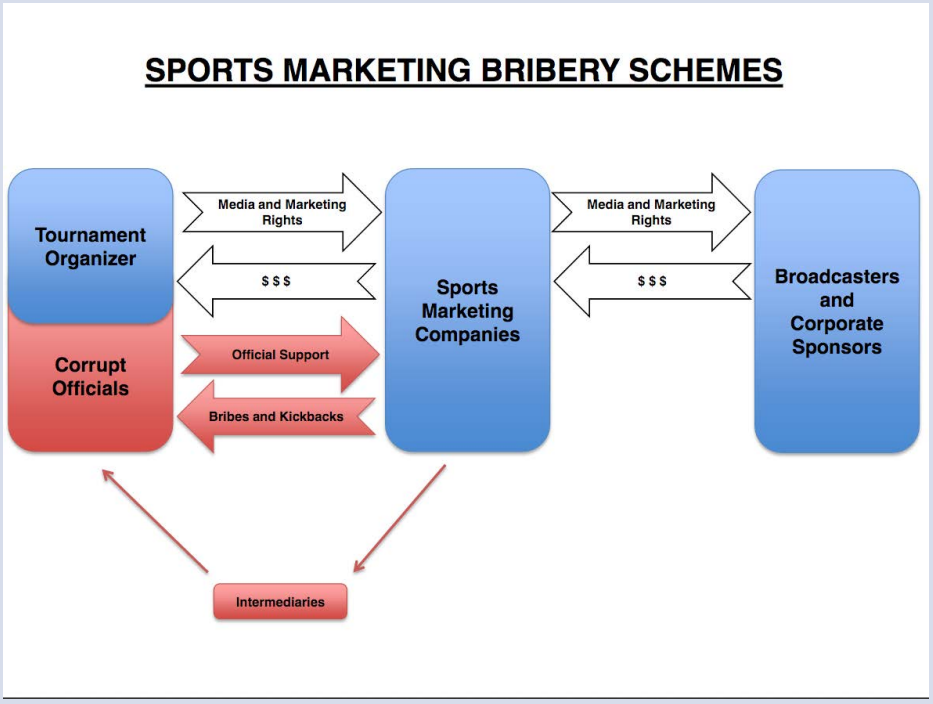
In recent months, bank regulators have constantly stressed the importance of institutional culture. "Healthy culture starts at the top, and we look to the board of directors and senior management to set a tone that encourages ethical and responsible behavior and demands individual accountability for failure to act accordingly," Comptroller of the Currency Thomas Curry said in a speech at a banking conference in early June.

That warning echoes one of the key lessons banks should learn following the FIFA indictments, says Andrew Foose, vice president of advisory Services for NAVEX Global. While "culture" may be "a worn out word" in compliance and regulatory circles, "the indictments provide a living example of why it is important," he says.

"Culture is something that builds over time, whether it is a positive culture or a negative culture," he says. "What FIFA allowed to happen was for relatively small transgressions—small gifts and small favors given to officials decades ago—to slowly build into a system where officials were routinely expecting lavish treatment and special gifts. That created an environment where they became entitled and expected bribes. What everybody should be outraged about is not just the bribery, but the culture that allowed it." ■

THE MONEY TRAIL

This graphic from the Department of Justice illustrates the complex money trail at the root of FIFA indictments.



Source: Justice Department.

Treasury Crackdown on Cash-Only RE Transactions

FinCEN demands that title insurance companies report the beneficial owners behind firms that pay in cash for high-end residential real estate in Manhattan and South Florida

by Joe Mont

For all its efforts to combat money laundering—and there have been many in the United States—the real estate sector has remained strangely untouched by them. Efforts to suss out the beneficial owners behind shell companies is an ongoing concern, one repeatedly flagged in assessments by the international Financial Action Task Force and its task force on money laundering, as post-crisis real estate bargains attract a flurry of multinational buyers.

Concerns that all-cash purchases of residential properties, lacking bank financing, may be used to hide illicit assets through limited liability companies or other opaque structures has prompted the enforcement arm of the Treasury Department—known as the Financial Crimes Enforcement Net-work, or FinCEN—to issue new Geographic Targeting Orders (GTOs). On March 1, the agency temporarily began to require title insurance companies to identify and report the natural persons and beneficial owners behind companies that pay in cash for high-end residential real estate in Manhat-tan and Miami-Dade County, Florida. The orders, barring an extension, expire on Aug. 27, 2016.

"Over the years, our rules have evolved to make the standard mortgage market more transparent and less hospitable to fraud and money laundering," FinCEN Director Jennifer Shasky Calvery said in a statement. "But cash purchases present a more complex gap that we seek to address."

FinCEN says it will take this approach because title insurance is a common feature in the vast majority of real estate transactions.

The recent GTO is the latest in the increasing use of that investigative tool by FinCEN. In April 2015, the agency targeted Miami-area businesses in its pursuit of money laundering plots. It did so by targeting electronics exporters in Miami-Dade County, focused on suspicions of trade-based money laundering schemes that used drug cartel proceeds to buy electronics that were later sold in South America, effectively converting ill-gotten gains into local currency. The GTO lowered the standard $10,000 reporting threshold for currency transactions to $3,000 (in either a single transaction, or series of related transactions) for covered businesses. The Treasury Department has a specific protocol, Form 8300, for filing those reports.

In little more than a year, other GTOs have targeted various potentially problematic businesses. One GTO targeted check cashing services in south Florida. Another GTO expanded the reporting and recordkeeping obligations to garment and textile businesses, show stores, flower shops, and beauty supply businesses in the Los Angeles garment district. And yet another GTO targeted busi-nesses based near the San Ysidro and Otay Mesa ports of entry on the California/Mexico border.

While there is nothing inherently illegal about all-cash real estate purchases or the use of shell companies to ensure buyer anonymity, the practices can be a go-to tool for money laundering. Investigative reports by the New York Times have uncovered not only a large number of questionable real estate deals, but also this tidbit: nearly half of all homes purchased across the U.S. valued at $5 million or more were made through transactions with shell corporations. A recent investigation by officials in New York City led to the discovery that Bank Melli, owned by the government of Iran, was the 40 percent owner of an office tower in midtown Manhattan.

> "Over the years, our rules have evolved to make the standard mortgage market more transparent and less hospitable to fraud and money laundering, but cash purchases present a more complex gap that we seek to address."
>
> Jennifer Shasky Calvery, Director, FinCEN

"For those trying to hide their identity, this is going to be a major blow," says Fred Curry, a principal in Deloitte's anti-money laundering consulting practice. "Hiding illegal assets and concealing the identity of bad actors has been a way to use the real estate market to launder the proceeds of illegal activity. This is a very important step for law enforcement that gives them greater transparency into the transactions. As money launderers become more sophisticated in how they move their funds through LLCs and other opaque vehicles, FinCEN must be proactive in addressing it. That is what they are doing here."

Concerns regarding the GTO include fears it will slow the pace of real estate transactions or, conversely, lead to a flurry of cash transactions before the March 1 deadline. Ross Delston, a Washington-based lawyer and AML compliance expert, poses another concern: Does targeting title insurance amount to a wild goose chase? Buyers who are paying in cash generally don't need title insurance, especially if they are simply recycling corrupt money. "I don't think anyone's going to be worried about title insurance in that situation," Delston says.

In the meantime, expect officials to continue their struggle regarding beneficial ownership due diligence. FinCEN's own rule proposal, lingering for nearly a year, may not go far enough in Delston's opinion because it only requires self-certification by owners. "There are large swaths of the

real estate sector that are currently not covered at all under the regulatory regime," he says. Real estate agents, in particular, are targeted by FATF's international standards, as embodied in its AML recommendations. The U.S. is not in compliance with international standards, Delston explains, because FATF has stated in its mutual evaluation of the U.S. that they are going to find, as they have in the past, that large sectors, including real estate agents, are not covered by measures such as the requirement for an AML program, the filing of Suspicious Activity Reports, and appointment of an AML compliance officer.

"It can be easy to determine if the buyer is a nominee or is a straw buyer in some cases," Delston adds. "A simple internet search will uncover the fact that they are a lawyer accountant or consultant who wouldn't ordinarily be buying this level of real estate. What's really difficult, and sometimes impossible, is when the nominee is a family member, a close family friend, a business associate, and perhaps someone with a different last name and from a different country. When you have the kind of wealth this order is aimed at, you can find lots of people who will help you do things."

The limited scope of the GTO suggests that FinCEN wants to evaluate its effect before deciding to broaden its attack, says Eric Berg, special counsel with Foley & Lardner and a former trial attorney at the Department of Justice, who conducted financial and real estate investigations connected to foreign corruption with the DoJ's "Kleptocracy Initiative," and who is an expert on the use of electronic surveillance in undercover criminal investigations. "They will certainly look at the effect it has because it is only a temporary measure. Future moves will be based upon it," he says.

"It is sensible to use GTOs because they can help FinCEN determine whether there really is a problem, and whether further regulation of a segment is necessary," says Stephen Heifetz, a partner with the law firm Steptoe & Johnson. "The industry might say, as they often do, that if there may only be one in 10,000 transactions by some bad seed, then is this really the most efficient way to use society's resources? That's a fair query."

FinCEN, however, needs to determine whether there is a problem, and with these GTOs and the increased transparency they provide to be able to determine whether further regulation is necessary, he says. "It is a way FinCEN can be active and properly demonstrate they are keeping their eye on the ball, but doing so in a measured way."

As for future FinCEN targets, Heifetz sees a likely increase of scrutiny related to casinos, Bitcoin-related businesses, crowdfunding initiatives and money services businesses.

"An important thing for any financial institution under the very broad FinCEN definition is that you can come into compliance pretty easily," he says. "It generally doesn't take a lot of work to have a basic compliance program that is a satisfactory and reasonable deterrent. I don't think that in these areas the federal government is playing a 'gotcha' game. They are expecting a fairly basic level of compliance, even by smaller institutions." ■

NOT SO LITTLE GTOS

The following is from a Geographic Targeting Order issued by FinCEN to title insurance companies in Manhattan.

Reports Required to be Filed by the Covered Business

1. If the Covered Business is involved in a Covered Transaction, then the Covered Business shall report the Covered Transaction to FinCEN by filing a FinCEN Form 8300 within 30 days of the closing of the Covered Transaction. Each FinCEN Form 8300 filed pursuant to this Order must be: (i) completed in accordance with the terms of this Order and the FinCEN Form 8300 instructions (when such terms conflict, the terms of this Order apply), and (ii) e-filed through the Bank Secrecy Act E-filing system.

2. A Form 8300 filed pursuant to this Order shall contain the following information about the Covered Transaction: Part I shall contain information about the identity of the individual primarily responsible for representing the Purchaser. The Covered Business must obtain and record a copy of this individual's driver's license, passport, or other similar identifying documentation. A description of such documentation must be provided in Field 14 of the form.

Part II shall contain information about the identity of the Purchaser. The Covered Business should select Field 15 on the FinCEN Form 8300, which will enable reporting of multiple parties under Part II of the form. Part II shall also contain information about the identity of the Beneficial Owner(s) (as defined in Section III.A of this Order) of the Purchaser. The Covered Business must obtain and record a copy of the Beneficial Owner's driver's license, passport, or other similar identifying documentation. A description of such documentation must be provided in Field 27 of the form.

Retention of Records: The Covered Business must: retain all records relating to compliance with this Order for a period of five years from the last day that this Order is effective (including any renewals of this Order); store such records in a manner accessible within a reasonable period of time; and make such records available to FinCEN or any other appropriate law enforcement or regulatory agency, upon request.

Compliance: The Covered Business must supervise, and is responsible for, compliance by each of its officers, directors, employees, and agents with the terms of this Order. The Covered Business must transmit this order to each of its agents. The Covered Business must also transmit the Order to its Chief Executive Officer or other similarly acting manager.

Penalties for Non-compliance: The Covered Business and any of its officers, directors, employees, and agents may be liable, without limitation, for civil or criminal penalties for violating any of the terms of this Order.

Source: FinCEN.

Firms Prepare for Heightened AML Expectations

Expect an even greater focus on anti-money laundering efforts in coming examinations by the Securities and Exchange Commission and Financial Industry Regulatory Authority, said the regulators at a recent event

by Joe Mont

Looking ahead, financial firms can expect examinations by the Securities and Exchange Commission and Financial Industry Regulatory Authority to place an even greater focus on anti-money laundering efforts, even as the Treasury Department's enforcement arm hammers out new demands on that front.

On July 14, 2015, the Commission hosted an estimated 1,000 financial services professionals, in-person and online, for what was billed as its "Compliance Outreach Program." Agency officials briefed banks, brokerages, and commodity traders on various compliance examination plans, and many involved anti-money laundering protocols and customer due diligence.

"An AML compliance program can serve as the cornerstone of an effective overall compliance program," according to Denise Saxon, assistant regional director of the Commssion's Denver office. "AML will be treated as an exam priority."

Expect continued scrutiny on Suspicious Activity Reports, a regulatory priority SEC officials have mentioned several times during the past two years. In a February 2016 speech before a gathering of AML professionals, Director of Enforcement Andrew Ceresney sounded the alarm over the seem-ingly lackadaisical approach broker-dealers were taking to SARs, averaging roughly five reports each year per firm. He also expressed concern with the quality of the reports that are filed.

"With some firms, narratives differ by only a few words from one SAR to another, revealing a check-the-box mentality," he said. "With others, the narratives never exceed a total of about 14 words."

Ceresney's warning to take SARs seriously was repeated throughout the event. "There is a renewed focus on compliance with suspicious activity monitoring and reporting requirements," Sax-on said. "Statistics really call into question whether the industry as a whole is really fulfilling its obligations in this space. It is concerning."

One underlying problem may be misperception of risk. "A lot of folks think they don't have drug cartels or human traffickers, so they have no reason to file SARS, but there are a lot of things that can be reported and there are checkboxes for a lot of things that you might not otherwise think you need to report," said Sarah Green, FINRA's senior director of enforcement.

What exactly are those items you should report, but might not have occurred to you? Many were included with the most recent update to the SAR form nearly two years ago: insider trading, micro-cap fraud, wash trading, identity theft, and cyber-breaches, Green said.

"When you think about your [compliance] program,

REVISITING THE FOUR PILLARS

The following is from the Treasury Department's Financial Crimes Enforcement Network's proposed rule to clarify customer due diligence obligations for banks, broker-dealers, and other financial firms.

> For FinCEN, the key elements of customer due diligence (CDD) include: (i) Identifying and veri-fying the identity of customers; (ii) identifying and verifying the identity of beneficial owners of legal entity customers (i.e., the natural persons who own or control legal entities); (iii) understanding the nature and purpose of customer relationships; and (iv) conducting ongoing monitoring to maintain and update customer information and to identify and report suspicious transactions.
>
> Collectively, these elements comprise the minimum standard of CDD, which FinCEN believes is fundamental to an effective AML program. Accordingly, this Notice of Proposed Rulemaking (NPRM) proposes to amend FinCEN's existing rules so that each of these pillars is explicitly referenced in a corresponding requirement within FinCEN's program rules. The first element, identifying and verifying the identity of customers, is already included in the existing regulatory requirement to have a customer identification program (CIP).
>
> Given this fact, FinCEN is addressing the need to have explicit requirements with respect to the three remaining elements via two rule changes. First, FinCEN is addressing the need to collect beneficial owner information on the natural persons behind legal entities by proposing a new separate requirement to identify and verify the beneficial owners of legal entity customers, subject to certain exemptions. Second, FinCEN is proposing to add explicit CDD requirements with respect to understanding the nature and purpose of customer relationships and conducting ongoing monitoring as components in each covered financial institution's core AML program requirements.
>
> Within this context, FinCEN is also updating its regulations to include explicit reference to all four of the pre-existing core requirements of an AML program, sometimes referred to as ''pillars,'' so that all of these requirements are visible within FinCEN's rules.

Source: FinCEN.

and whether you are filing the SARs that you should, start thinking about risk," Green suggested. What are the products that have fraud or money laundering risk? What type of clients do you have? Do you have foreign clients? Are there systems in place to pick up on those risks?

If your company has a system to monitor and flag potential problems, regardless of whether it is manual or automated, the SEC's staff and examiners will assess whether those alerts are investigated properly with adequate staffing to do so.

What Examiners Want to See

A proper AML system, and one that generates and responds to SARs appropriately, will require an integrated approach to trade surveillance and asset movement because "the securities industry is one of the few, if only, industries where you can both generate illicit proceeds as well as launder them," said Sterling Daines, managing director of Goldman Sachs' global compliance division. "Many of the actions brought by FINRA and the SEC against AML programs involve illicit or suspicious trading activities, such as price manipulation and insider trading. There are a lot of different types of securities fraud that can occur. If your AML program isn't set up to detect and report them, you are going to have an issue."

The renewed focus on SARs likely means that compliance examiners will request even more often every alert generated over a given period of time. "You will have to have an appropriate audit trail on those decisions as to why you did or didn't file a SAR," Daines said.

As for the investigations that could ultimately lead to a SAR, firms shouldn't be afraid to get creative. "We all have our systems, but always look for new ways to monitor," said Pamela Ziermann, senior vice president at Dougherty & Co., an investment bank and brokerage firm. One tactic she uses is to set Google news alerts on a person or entity when "there is something out there that you have no reason to file a SAR, but you have that sixth sense." Another trick: Map applications that feature street-level views can help verify that an office address is where it is purported to be.

Don't think that filing a lot of SARs will absolve you, as regulators will focus on content as much as they will on frequency. "To me, a SAR is a story, so focus on who, what, where, when," Ziermann said. "Somebody should be able to read it and know why you filed." She stressed continued training for staff on how to write SARs.

FinCEN's Influence

Upcoming FinCEN rules, intended to revise and formalize customer due diligence requirements under the Bank Secrecy Act, will also influence how firms should approach AML compliance and the examinations that assess those efforts. The proposed rule, issued last year, is expected to be complete by early 2016. It will apply to both large and small institutions, including banks, broker-dealers, mutual funds, futures commission merchants, and introducing brokers in commodities transactions.

> "A lot of folks think they don't have drug cartels or human traffickers, so they have no reason to file SARS, but there are a lot of things that can be reported and there are checkboxes for a lot of things that you might not otherwise think you need to report."
>
> Sarah Green, Senior Director of Enforcement, FINRA

A key amendment to FinCEN's current AML rules is a requirement that firms know and verify the identity of the "ultimate beneficial owners" of their customers, including individuals who own (directly or indirectly) 25 percent or more of the entity or exert significant control over it. Foreign regulators, as well as the International Monetary Fund in a recent report, have chided the United States for being a global laggard on beneficial ownership assessments.

The final rule will also expand obligations to identify and verify the identity of customers; understand the nature and purpose of the customer relationship for purposes of developing a customer risk profile; and require monitoring to maintain customer information and identify suspicious transactions. Many of these obligations are intended to be clarifications of existing FinCEN rules and its customer identification programs.

"This will be a real game changer for our industry and will mean big adjustments for firms," FINRA's Green says.

While many firms have already started identifying beneficial owners, the proposed rule adds a requirement to verify that information. "Firms will need to codify their approach and the tools they use, and draft policies and procedures to cover all this," Daines says.

The upshot for compliance officers: Training on all this will be crucial. "Particularly in larger firms, the function of on-boarding a client is typically not done by compliance," Daines explains. Compliance may have an oversight role, but the labor is typically the responsibility of operations staff. "Figuring out how to drill through to who the owners are at the bottom of that structure, the natural person, can be very difficult to do," he says.

The other FinCEN requirements should not be dismissed either. "Every firm is going to have to try to figure out what they want to capture to create a customer profile," Daines says. "While it seems straightforward—and certainly in the securities industry people have been risk ranking their customers to one degree or another over a long period of time—the concept of codifying it into a customer risk profile is a very different one that we are still trying to think through." ■