COMPLIANCE WEEK
THE LEADING INFORMATION SERVICE ON CORPORATE GOVERNANCE, RISK AND COMPLIANCE

The Fine Art of Knowing Your Customer

Carole Switzer April 30, 2013

Who knew that the art of anti-money laundering (AML) compliance had so much in common with the science of spotting fake paintings? Art forgery, which the FBI has estimated generates more than $6 billion annually, represents a big and decidedly criminal business.
This is the case despite the fact that fine arts sleuths can borrow tools from medical labs and deploy state-of-the-art software to detect telltale thread patterns on canvasses. Governance, risk management, and compliance (GRC) professionals responsible for sniffing out potential AML-related fraud have less sophisticated tools to deploy—even though these criminal proceeds amount to $1.6 trillion each year, according to a United Nations Office on Drugs and Crime study.

But it's not much of a stretch to suggest that those responsible for developing an effective customer risk assessment program—a capability commonly referred to as Know Your Customer (KYC)—can learn a thing or two from experts who spot fake paintings. And just like the art expert, the AML expert running an effective customer risk assessment program can't depend solely on sophisticated tools and gadgets but must employ good, old-fashioned due diligence and ongoing monitoring.

Accounts of some of the world's most notable painting forgeries feature many of our most famous artists: Botticelli, Vermeer, and da Vinci each inspired forgeries. The way the vast majority of these fakes were exposed involved methods much less technical than thread-count software and decidedly less glamorous than the dashing portrayals of art forgery capers in popular movies like The Thomas Crowne Affair.

In fact, the most effective ways to avoid buying a phony are basic enough that they have been posted to the online how-to guidance site eHow; some of these steps include:

- Deal only with reputable art dealers;
- Learn as much as possible about the artist whose painting you plan to invest in;
- Visit museums and galleries where the artist's works are displayed;
- Look at the painting from as many angles as possible; and
- Hire an independent expert trained in conducting investigations to confirm authenticity.

Each of these steps has a KYC parallel activity, and for good reason. That's because leading customer risk assessment programs function as if a company is patiently composing a portrait of a customer. These programs call for gradually intensifying levels of due diligence that are designed to produce an accurate picture of the customer.

Unlike paintings, however, customers change over time. That's why the best customer risk assessment programs deploy ongoing monitoring. When monitoring detects problematic activities, such as highly questionable transactions, the company takes a closer look at the transactions and the customer.

Some of Hollywood's most clever movie forgeries, as the Thomas Crowne Affair gleefully depicts, feature fakes painted over original portraits. This ruse also has a KYC corollary: sometimes, due diligence activities require risk managers to strip away layers of false or questionable information to reach an authentic vision of a customer's AML risk profile.

The best customer risk assessment programs deliver—and sustain—an accurate portrait of customers by operating in a highly integrated and comprehensive manner; specifically, these programs:

1. Pull customer information from a wide variety of sources;
2. Synthesize this information regardless of where it is collected and where within the organization it is stored; and
3. Organize, analyze, and deliver the information on a timely and continual basis.

Supporting technology helps, of course, but it need not be as exotic or expensive. These three steps not only help companies know their customers better, they also can deliver a capability that, for financial services companies, represents a key enabler of principled performance.

Truly knowing your customer requires companies to keep their eyes wide open regarding who they are serving at all times. In an era of global business where some customers can employ extremely innovative methods to disguise their true characters, performing in a principled manner requires companies to do much more than simply take their blinders off when assessing new customers.

Instead, they should devise an effective and efficient approach to putting customers under the microscope via a methodical and repeatable approach to good, old-fashioned due diligence.

Know Your Customer: An OCEG Roundtable

Switzer: It seems extremely difficult to really know your customer today, when one can create dummy businesses and identities that look and feel completely real. How do you go about determining that the customer is who they say they are?

Mara: Each jurisdiction has its own standards as to the documentation required as a part of a Customer Identification Program (“CIP”), mostly based on certain types of government issued materials (e.g. a driver's license). A strong CIP program uses a combination of these documents and various public and private information sources to cross-validate information provided by a customer. Additionally, strong customer on-boarding training enables these personnel to recognize “red flags” that may indicate altered or falsified documents. These, in combination with ongoing due diligence, for example comparing customer activity against peer profiles or anticipated behavior builds a body of evidence that a customer is who they say they are.

Yuille: As part of the Know Your Customer process regulators will mandate screening for sanctioned entities and may have some minimum requirements in areas such as ID and address verification. Running checks against adverse media and external risk intelligence can help verify that a client really is who they claim to be and highlight unseen risks.

Devlin: We have found two areas in particular that many financial institutions seem to struggle with. One is really drilling down into corporate ownership and control – identifying the ultimate beneficial owner (“UBO”) behind a series of linked companies takes persistence and too many firms in our experience are content to be fobbed off with assurances from the customer which, when examined, don't truly answer the question of who the UBO is. A second problem area is the level of due diligence undertaken on very high risk customers. These are customers who may display a complex risk profile—perhaps they're nationals of sanctioned countries, or politically exposed persons (“PEPs”) based in countries known to have significant corruption problems. Many firms have a fairly rigid approach to the onboarding of customers based on their perception of the customer's risk profile, but very high risk customers may need more tailored forms of Enhanced Due Diligence (“EDD”) such as in-depth vetting or investigatory work before an institution can feel that it truly understands their risk profile.

Switzer: What customer behaviors, both within and outside of your relationship, raise suspicion of involvement in money laundering, and how do you monitor those behaviors?

Mara: Mostly, suspicion is raised when customer behavior either fits a pattern of activity that is indicative of increased money laundering risk (e.g. structuring) or when it is not aligned with either the behavior of similar customers or anticipated behavior for that customer. Most commonly, some form of automated transaction monitoring is used to identify these activities for review. Behavior outside of the relationship is harder to identify but negative news searches, link analyses, and data analytics, among other methods, can be used to draw inferences and refine your perception of risk. For example, transfers of funds to a single external account from a number of customer accounts may indicate a relationship between the customer accounts that was not previously evident. If the external account holder then shows up in a negative news search as a criminal, then it should cause you to take a closer look at your customers.

Devlin: For many years financial institutions have thought of money laundering as comprising solely or mainly of the process of washing tainted funds deriving from predicate criminality until they appear clean. It is only recently that people have begun to recognize that a bank can be exposed to money laundering risk not only by washing tainted funds but also through facilitating the predicate criminality itself that produces those tainted funds, and by enabling the ownership of assets bought with tainted funds (commonly via a series of structures).

Yuille: Financial services relationships tend to be for the long term. Within the term of that relationship people's lives change - marriage, divorce, job changes, new families, wider social unrest etc all these can create financial or social pressures that in turn lead to suspicious or illegal behavior. Routine review and updating of onboarding information including, updated ID documents, screening against databases of heightened risk entities and negative media scanning can all help identify an adverse change in circumstances. Environmental factors such as a change in geo-political risk may also be the trigger for a more immediate review of a group of accounts. Ongoing monitoring and analytics across accounts helps to identify abnormal behavior that warrants additional investigation. Typically a single client will have multiple accounts/products with an institution, sometimes as the result of acquisitions, so information may exist in multiple systems and process. Developing ‘golden client records' can also provide useful insights and highlight a relationship that warrants closer monitoring. Understanding wider family relationships and related business accounts can help identify behavior worthy of careful investigation, and may also highlight commercial opportunities.

Switzer: What is more important in this Process—training your people to recognize suspicious behavior and report it, or using data analytics to find and assess suspicious transactions?

Devlin: While sophisticated data analytics are undoubtedly important, there is no substitute for trained and experienced staff tasked with sifting the wheat from the chaff. Hiring staff with sufficient experience, particularly of esoteric areas, can be expensive, but it is money well spent. There is no point in having a first class alarm system if the person responding to it can't distinguish a break-in from a false alert and theoretical training can only take you so far down that road. What is perhaps equally important is a regular and rigorous process of internal and external audits of the system and its alert handlers. Without a fresh perspective some teams find that they get stuck in a groove and normalize or do not investigate transactional behavior which an outsider might find startling.

Mara: I don't think this process can be successful in most institutions without effort devoted to both of these areas. Data analytics are hugely important when handling large volumes of data and in identifying relationships between accounts to detecting potential suspicious behavior. This enables an institution to sift through millions of transactions and identify red flags much more efficiently. However, red flags do not always mean that a set of activity is actually suspicious. Patterns of activity are suspicious only in context and analysts must be trained to evaluate the information. For example, large cash deposits might be suspicious for an individual but not for a business. However, an internet-based business would probably not have large cash deposits so the context is obviously important. Modern approaches combining traditional data analytics with visual analytics take this to the next level and strongly enhance this overall process.

Yuille: Both are important. The volume of transactions mandate the use of technology, people can often see connections that technology can't. To identify abnormal behavior it is necessary to first establish normal behavior, for individuals and also for groupings of similar accounts—white collar, blue collar, self employed, etc. People can pick-up the investigation and make connections that technology can't and also understand the wider context.

Switzer: What are some of the biggest challenges in monitoring customer risk and what is your one piece of advice for doing it well?

Mara: From a business perspective, one of the biggest challenges is to balance between collecting enough information to adequately evaluate risk while not collecting so much information that the customer experience with your firm is damaged. From an operational perspective, the sheer volume of information generated by the rapid pace of business activity represents an ongoing challenge. I don't think that it's possible to be effective and efficient without combining input from the business, operational, technology, and compliance areas of a firm with responsibility and accountability for managing risk. Working together to find the best solution tailored to each firm's risk profile and tolerance is a necessity. Working separately is a good way to find a solution with which no one is happy.

Devlin: By all means put effort into maintaining a good rapport with your valued customers, but don't compromise your ethical standards. In many parts of the world with steep authority gradients and powerful social hierarchies institutions and individuals within institutions are wary of asking tough questions of local PEPs because they fear causing offense, damaging the relationship, or upsetting more senior colleagues in other divisions of their firm. While in many instances no bad will come of this, those customers who are engaged in criminal activity— the giving and receiving of bribes, for example—will exploit any deference which they detect by being less forthcoming than they should. Treat your customers consistently and you will gain in the long run.

Yuille: I'll keep it short. Mine transaction data for indications of suspicious behaviour.

OCEG ROUNDTABLE PANELISTS

Carole Switzer,
Moderator
President,
OCEG

Tom Devlin,
Stephen Platt & Associates

Rob Mara,
Executive Director,
Ernst & Young

Andrew Yuille,
VP, Business
Segment Marketing,
Thomson Reuters

Source: OCEG