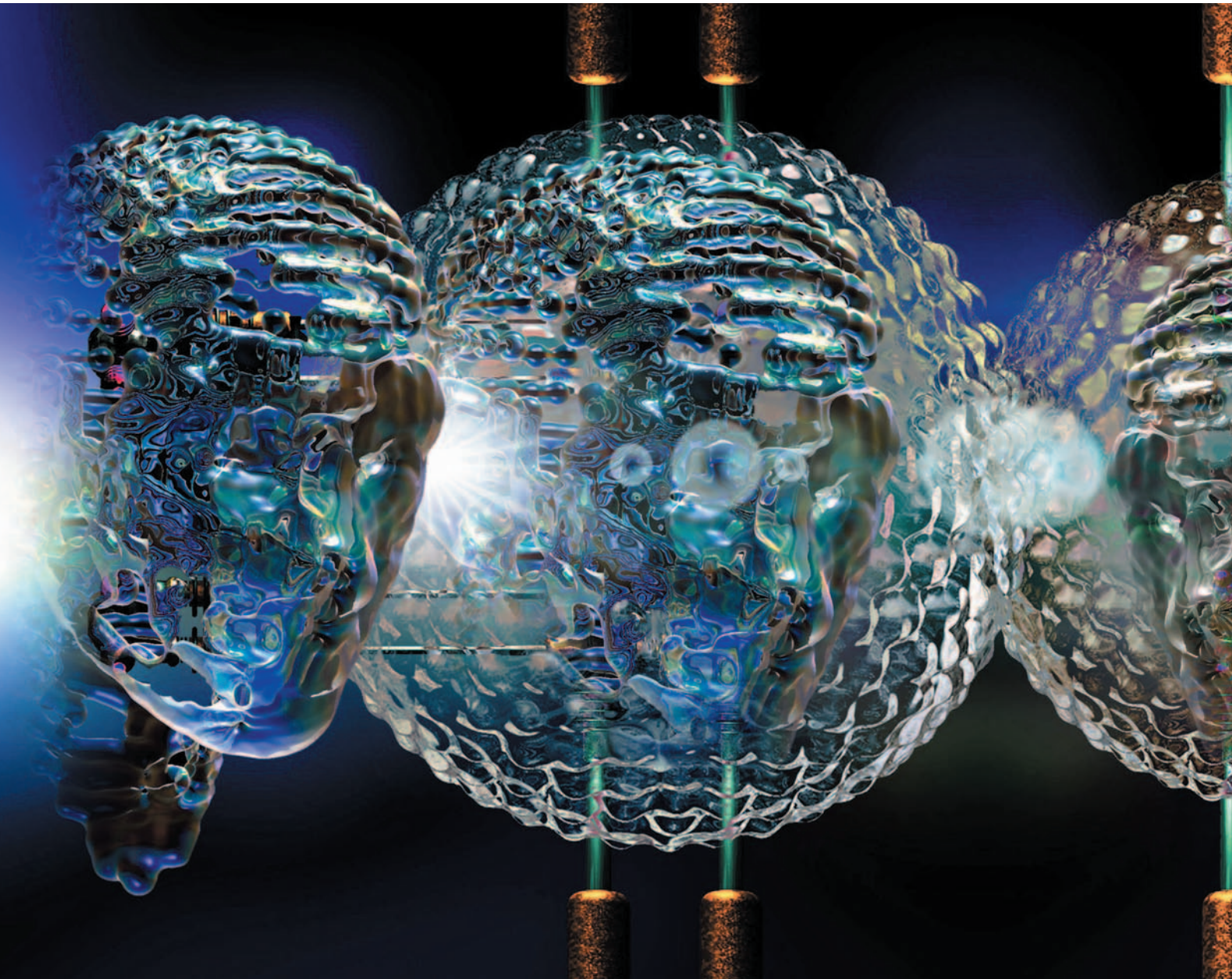


The new face of compliance



Elise Coroneos uncovers the world of watchlists, anti-money laundering software and Web-based platforms designed to help hedge funds comply with “know your customer” regulations

Once upon a time, financial institutions dealing with a customer of known disrepute risked little more than a slap on the wrist and a regulatory fine. Some compliance specialists still talk of the old days when their clients preferred to swallow a fine rather than pay for a more expensive option: implementing a robust culture of customer compliance.

Compliance was something that happened in the back office. Nobody saw it, and few people talked about it.

No longer. The regulatory environment has changed dramatically in the past two years, leaving many hedge funds unequipped to meet more rigorous standards. Whereas traditional financial institutions have multiple departments to conduct due diligence, minimize risk, investigate customers and meet compliance requirements, hedge funds often have little infrastructure in place for these purposes.

"The challenge is bigger for hedge funds because they have to meet the same requirements in many cases as the banks do, without the resources that the banks have," says John Auerbach, the director of anti-money laundering services at Kroll Inc, an independent risk consulting company. "That is what makes the life of the compliance officer at a hedge fund so much more difficult."

Kroll helps its clients comply with regulatory requirements by designing compliance policies and procedures, training programs, and customer and employee screening; providing intelligence on organized crime and terrorism; conducting forensic investigations of suspected or alleged money laundering incidents; and coordinating with law enforcement agencies.

Hedge funds are most at risk of facilitating money laundering or dealing with unsavory entities at the investment stage, when a new investor is brought on board, and at the redemption stage, when the investor cashes out, says Auerbach.

At the investment stage, the fund runs the risk of accepting money from a person or entity that has been gained through illegal means such as drug trafficking, official corruption or embezzlement. "Because hedge funds attract people of high net worth, it makes them attractive to money launderers who like

to be able to find ways to move large amounts of money," says Auerbach.

Even if a fund has no reason to be suspicious of a particular investor, says Auerbach, it can run off the track at the redemption stage if it agrees to wire the proceeds of an investment to a third party it has not properly vetted.

"It is important to always identify all relevant parties because money launderers work through networks of agents and front companies," says Auerbach. "They try to hide the nature of the funds by passing them through a lot of hands."

It used to be that a hedge fund could safely accept and redeem investments to persons who did not appear on the sanction list of the US Department of the Treasury's Office of Foreign Assets Control, known as the OFAC list. These days, however, sophisticated operations that facilitate money laundering are not so easy to identify.

"Checking OFAC is simply not enough," says Auerbach. "Anyone on this list has already been convicted of a major crime, so it is very unlikely that they are going to be opening accounts under their own name." Furthermore, he says, hedge funds with international client bases have compliance requirements that extend beyond the US and therefore beyond the reach of OFAC.

The mother of all databases

At the forefront of providing hedge funds with a credible solution are a new breed of databases that extend across borders. Known as "watchlist" databases, these use spidering technology to combine all sanction lists worldwide with information that is available on the Internet and other electronic sources.

Activities of individuals and organizations found on these databases run the gamut: known money launderers, fraudsters, organized criminals, narcotics dealers, arms dealers and war criminals. These names are aggregated into a centralized database that subsequently allows financial institutions to very easily screen their customers.

Consider the watchlist provided by Choicepoint/Bridger in Bozeman, Montana. Its Bridger Tracker software was first developed in 1989 as a custom design to help a large corporation comply with OFAC requirements, according to Michelle Thiel, data and compliance manager at Choicepoint/Bridger.

Today, Bridger Tracker is available in three mediums: a network-ready Windows-based product, an online product that is accessible via a Web browser and an Internet connection, and Developers Solution, which can be integrated into a third-party system. According to Thiel, 80% of all US banks have their data checked by Bridger Tracker software.

Another database provider is World-Check, which is headquartered in London. It was created in October 2000 to meet the specific requirements of several Swiss financial institutions, with its first version going live in late January 2001. Today World-Check's watchlist includes the names of more than 200,000 individuals, businesses and organizations that are known to be high risk. To put this number in perspective, you need only consider that the 5,000 to 10,000 new profiles World-Check adds to its watchlist every month is two to three times the size of the entire OFAC list. It is updated twice daily.

World-Check gathers data from over 100,000 sources, including public information available electronically via government-related sanction lists, policing organizations from around the world such as Interpol, SEC violators or debarred directors from different countries, and watchdog groups that cover various issues related to financial risk.

But World-Check goes far beyond these electronic sources. In March 2003, the firm formed a partnership with Kroll through which it augments the intelligence obtained from its database services with on-the-ground, subject-specific due diligence conducted by Kroll's global network of investigators.

"If something is showing up in the newspaper in China, it may not be picked up by electronic sources," says Auerbach. "But Kroll has people on the ground in China, so if you really need to know about a customer, we have people who know that market and can tell you what is not hitting the news and watchlists."

Kroll, in turn, recommends that its clients screen their customers against World-Check's database.

This all-encompassing approach, means that hedge funds are much more likely to catch out suspicious persons or entities operating beneath the radar of the conventional enforcement sources, says Brendan Cohen of World-Check.

Identifying suspicious persons by conventional methods, says Cohen, is about as likely as a ship hitting an iceberg that projects above the water.

“Of course a ship is likely to avoid hitting an iceberg if it can see it, but it is the iceberg below the water that poses the most risk,” he says.

At your fingertips

For smaller hedge funds, the best way to access one of these watchlists is by using its online service, which doesn't require any setup or download. Besides Web access and a user login, a fund need only type in a customer name to see if it is in the database.

Access to watchlists is usually sold as an annual subscription, the cost of which largely depends on the number of user IDs a firm requires. At World-Check, a fund requiring only a couple of IDs will pay between \$1,000 and \$2,000 for each ID, says Cohen.

If the name is not in the database, the fund can simply hit a button to print out a report documenting that it has conducted a search, complete with a date stamp and a user ID stamp. This report can then be put in the file to serve as an audit trail.

“In a matter of minutes, you checked every sanction list, policing organizations, media and the like, and it took no technical skills and no concrete due diligence skills,” says Cohen.

This process is entirely confidential, as World-Check keeps no physical records of who is logging on or the names they are searching. Furthermore, World-Check allows a subscriber to anonymously submit the name of a potential investor it believes is suspicious, but does not appear on the database. World-Check will then scour the public domain to try and verify whether that suspicion is valid. If so, the name will be added to the database.

“So not only does the hedge fund have an online service that allows them to check sanction lists worldwide, but they also have access to a full, qualified due diligence team,” says Cohen.

Added autonomy

So far so good, but what happens if there is a “hit” and a potential customer's name turns up on a watchlist. Hedge funds, says Cohen, must be aware that doing a search on a watchlist is akin to doing one on Google.

“The point is that there may be some very valuable information presented, but you won't know it unless you go through every document that comes up as a potential hit, which is just not time efficient,” says Cohen. As a result, the watchlist itself is of little value without a time-efficient way to verify the identity of each and every hit.”

This could be a very time-consuming process when you consider that in the US, 80% of the population has the same 500 last names, leaving only 1.2 million unique last names, says John Keane of Norkom, an international software company headquartered in Dublin.

Norkom offers a solution to this problem known as name-matching, or filtering, software. This enables a fund to check whether a client's name as it appears on a watchlist actually represents the same person with the same name, sitting across the table at the time of investment.

“When you get a hit, we give you a profile that helps you to quickly identify whether it is the same person,” says Keane. “So we're not just simply saying, Congratulations, you have a hit.”

Norkom's synopsis on the individual can include hyperlinks to original document sources provided by external agencies and other individuals/entities in its database with whom this person might be associated. “This is a huge value added, because money laundering often happens through relationships,” says Keane.

Choicepoint/Bridger also provides identity verification services, including the option of buying access to two other services on a transaction basis,

one provided by Choicepoint and the other by eFunds. This verification technology can be used to verify that a social security number is in fact a true social security number.

“So you are basically taking steps against the appropriate files for your internal and maybe external regulators to make sure you know who that customer is,” says Thiel.

Finding a time-efficient manner in which to conduct customer due diligence is especially important because funds have to verify not only new and redeeming clients, but also all existing clients to ensure they have not suddenly turned up on a watchlist.

World-Check allows clients of its name matching software both to check against its database and to download the entire database. The software then automatically checks clients' list of customers against the database. One benefit of the software is that once a match is found, it helps the compliance officer work through to a conclusion by providing decision screens.

Furthermore, the system is able to remember the decisions a user makes so the user will not be forced to make the same decision for the same matches every time the entire client list is checked. This benefit is not available to online-only subscribers.

Cohen says that the World-Check database and name matching software combined will typically cost around \$30,000 for the first year, for a smaller institution with minimum login requirements. □

