

Spy vs. Spy

Both sides are innovating to stay ahead in the war on criminal money.

Who is winning the war on criminal money? Jersey has made a valiant assault, employing regulatory reform, better practices and innovative technology. Money launderers and financiers of terrorism, our formidable opponents, have themselves been developing techniques and technology, not only to build defences but also to launch counter-assaults. The stakes are high, with criminal money estimated at between two and five percent of worldwide GDP.

Regulation and compliance practices in Jersey have continued to meet international best practice. The risk based approach to customer due diligence, made mandatory by the Money Laundering (Jersey) Order 2008, has enabled businesses to be more intelligent in their allocation of resources, offering relief for low risk relationships but necessitating extra care and attention where risk is high.

Two new challenges emerge in the implementation of the risk based approach. The first is that determining a client's risk rating is no longer just a matter of consulting an objectively defined list, such as a list of politically exposed or sanctioned people. Rather, a subjective judgement is required, considering the kind of product being offered to the client, the nature of the introduction and history of the relationship, factors specific to the firm, and factors associated with the countries and entities involved.

The second challenge is how enhanced customer due diligence (EDD) can be undertaken effectively. A full assessment requires that clients' associates and business interests not just be identified, but also investigated. Commercially available data is typically limited to listings of associates, and it is difficult to dig deeper in order to gain the necessary understanding. Some organisations have found Google to be an important tool at this point, trading privacy for the flexibility of being able to investigate without limit.

New technology has helped to address both of these challenges. Tools like KYC360^o, developed locally, provide information without regard for objective definitions of heightened risk, so the Richard Bransons of the world can be investigated as easily as the Tony Blairs. This has become feasible due to the development of software algorithms that can automatically analyse vast catalogues of information. By reducing the dependence on human researchers, information on more entities is available, and the need to objectively define who should be included slips away.

The same algorithms permit deeper investigation. Where a relationship is discovered between Mr X and Ms Y, the same analysis can be automatically applied to Ms Y even if Ms Y was hitherto unknown. When that analysis links Ms Y to Prime Minister Z, the value of the approach becomes clear.

These tools, and others that support the risk based approach, have enabled industry and government to not only conform to the new standards, but to be more effective and efficient at the same time. Nobody likes new rules, but the pain of their implementation can be mitigated and even benefits realised if the right tools are at hand.

While we are busy improving our ability to detect risk and criminal activity, criminals and their accomplices are finding clever uses of technology to avoid being spied upon. Creating clean autobiographical entries on Wikipedia is no longer the state of the art.

Search engine optimisation (SEO), a technique that has been around as long as internet search engines, has found an increasingly nefarious range of uses. The original use of SEO was as a marketing aid. If you start a company selling diamonds, chances are that searching for “diamonds” on the web will show no trace of your website in the first hundred pages of results. Hardly good for business. Search engines like Google increase your “page rank” if other websites link to yours, using popularity as a proxy measure for quality. One SEO technique involves automatically creating thousands of blogs or web pages that link to your website, improving your prominence in searches. By charging fees for this service, SEO has become an industry of its own.

That same technique has now been applied with the opposite aim – to reduce the prominence of websites that contain unfavourable news. Corporations or individuals can now engage in “profile cleansing” by creating thousands of blogs or web pages that refer to the subject in a positive light. The intention is to push negative information to a distant page of search results, in the hope that it remains undiscovered. Profile cleansing is now available as an online service.

The extent to which this is occurring is as yet immeasurable, but since the fees are small in comparison to the benefit of keeping a low profile, its prevalence can only increase. Yet another factor to consider when conducting customer due diligence.

As usual, the best way to address this technological counter-attack is with yet more technology. Google adjusts its ranking mechanisms continuously in an ongoing battle with the SEO industry, but these adjustments aim to neutralise marketing attempts (where sites are artificially promoted), quite the opposite of obfuscation. Tools like KYC360^o RiskScreen that conduct automatic filtering and highlight adverse results can help see through these diversionary tactics.

Criminals have now taken to conducting investigations of their own, aiming to counter successful compliance research with textbook extortion. These grim scenarios typically involve a client who, fully aware that their proposed transaction is likely to trigger a suspicious transaction report, conducts some background checks on the financial services professionals that can effect the transaction. The threat to release that information is then used in the hope that due diligence on the transaction might be overlooked. Adverse information on even one person can provide sufficient leverage, and criminals have no moral hesitation in using innovative services like Facebook or more traditional spying methods to achieve their goals.

Set within the ongoing war on criminal money is a technological arms race, with both sides becoming smarter and better armed. Regulated businesses will demand more specialised tools and services, looking to achieve cost savings despite the increasing regulatory burden, and innovative providers will meet that need. Compliance successes drive criminals to innovate, so new typologies will continue to emerge.

Who will win? We can hope for a Hollywood ending, but this is set to be a very long film indeed.

Karl Anderson is Managing Director of KYC360^o, the online money laundering community. The community offers free resources and tools to members, and industry-leading premium tools by subscription. KYC360^o is used by banks, trust & corporate services providers, law firms, regulators and law enforcement globally.