KCS Group Europe

Cyberlaundering: A Bad Deal

18th June 2018

Picture the scene. A particular table at a particular casino, strangely not part of the action. A gentleman comes to the table and plays one single game of baccarat. The stake – ten million dollars. He loses, pays his debt and leaves without a word. But while this may sound like the stuff of spy fiction, it is in fact a well-established method of money laundering: one that, like so much else, has been supplanted by the adoption of new cyber techniques to solve an age-old problem.

The trick of the game played out in the casino was to move the money from one side to another in a way that seemed legitimate but which could conceal illicit movement of funds: classic laundering. The advent of technology has of course improved the means and opportunities of those needing to wash their money. Not only can you run it through shell companies and offshore accounts with much greater ease, and ensuring that everything remains centrally controlled (thus increasing the challenge for AML), but one can employ even more diversionary tactics to conceal the fact that there is even laundering going on.

Recently for instance, saw reports that the wonderful world of Internet shopping was being used to leverage the power of anonymity for money laundering. Listings on Amazon and eBay, fake rooms for rent, even specially-designed cryptocurrencies – all are used to provide nominal excuses for why large amounts of money are going to specific accounts, and gain the protection of the international banking system (and the comparatively small amounts each time) to stay under the radar of law enforcement. Moreover, these are for the most part not carried out through the Dark Web or transactional sites known to be frequented by hackers and scammers – these are genuine e-commerce sites, among the biggest in the world, where perhaps one just does not simply assume that there can be extensive problems.

One might see a book being sold for thousands of dollars, or currency being transferred to other countries in a totally new coin, or even taxi fares being paid for journeys that never happened. The principle is the same: move the money and move it in a way which seems legitimate.

So how can this be countered? The problem falls in two parts. Firstly in terms of stopping the money laundering directly, there clearly needs to be a much greater degree of scrutiny applied to these big commerce sites and the products which are being sold – and stopping the washing from taking place. This is a large grey area where the law is concerned, given the constantly evolving nature of the methodology, lack of clarity about how one can be sure something is cyberlaundering, and the lack of firm support given to date. Just as traditional AML has been strengthened by international bodies and treaties, so too must focus now shift to AML in the online arena: better tracking of transactions and IP/internet registries, better verification that the products and transactions are genuine, and better protections in place to immediately freeze/halt transactions that are considered to be overly suspicious.

The second problem is to identify individuals involved in the money laundering (whether for purposes of legal action, or a hunt for risks/weaknesses/threats) - using new methods such as these will likely mean it is harder (although not impossible) to track them and prove their involvement in laundering. But this is not something that can be ignored. Criminals may get smarted, but so too must the investigative aspect keep pace and be prepared to tackle this rising threat – not to do so is too big a gamble to take.