

## Money laundering: not just a game

---

10<sup>th</sup> April 2020

The virtual world is the latest frontier in the fight against money-laundering. The vastly popular videogame Counter-Strike: Global Offensive has been identified as a means by which cyber-criminals can launder and liquidate money. This is done through ‘loot boxes’ (containing gameplay items) which require keys to open – it is these keys, whose prices remain constant, that are swapped and used as currency. While loot boxes have long been identified as a form of gambling, this is the first instance where video games have been used to launder. It is unlikely to be the last.



The keys to the loot boxes are, indeed, key – they can be traded for real-life money through the CS:GO online store on service provider Steam. Keys are traded between bad actors and then exchanged for money: illegal money becomes legal. Steam’s parent company Valve have now removed the functionality to trade keys, but two precedents are clear: firstly, that this *can* be done (and is likely already being done on other, similar games), and that inventive evolutions in laundering are always being sought – with it being a struggle to keep on top. The model is moving further and further away from traditional bank-based means (although the biggest laundering frauds in history still originate from banks – think HSBC’s \$1.9bn USD fine for serving as a conduit for Mexican drug money) and into new channels. And while CS:GO’s makers will have lost no money, but a lot of reputation, other laundering is unlikely to be so kind in terms of compromising direct victims, instead of a giant, indirectly.

If there is any doubt about just how serious money laundering is, the figures speak for themselves: between 2% and 5% of global GDP believed to be laundered each year (per the UNODC), with £90bn impacting the UK alone, and record levels of laundering crime being reported – but investigations dropping dramatically (40 arrests across 28 cases for the UK last year). Such issues have never been more important, with a recent Solicitors Regulatory Authority study finding that one-fifth of UK law firms have inadequate protection against money laundering and growing fears that the UK is now the European destination of choice, particularly so as given that the impending departure from the European Union (at time of writing) means that the UK will not legally need to comply with the impending regulations that will impose greater control on the due diligence done on potential customers, nor participate in the mooted central AML authority under discussion by the EU Commission.

While the issue of 'golden visas' is in the public consciousness – most notably with the recent case involving the vast sums spent by the Hajiyev family in Harrods, and Chelsea owner Roman Abramovich's decampment to Israel following his refusal to explain the sources of his money – the UK is simultaneously opening its visa-shaped doors to those that donate around £2m GBP to the Treasury coffers. This, and the claimed intent to crack down on laundering, cannot surely both coexist.

Aside from purely financial institutions, property is an increasing tool of the launderers. One might for example sink liquid assets into a property owned by assorted shell companies to disguise its provenance, or deliberately under/overvalue a property, or buy and sell it so many times (again with cutouts) that verifying its ownerships becomes all but impossible. Or even, to establish one's own estate agency to handle a portfolio of laundered properties – not as uncommon as might be thought, given that just under half of the UK estate agents are not registered with an appropriate HMRC program.

Cryptocurrency is another development on the technological side that allows launderers to disguise their actions, which is appreciated for its relative anonymity, difficulty to prove, and ease of manipulation (existing only on the Internet and without tangible, identifiable evidence). With cryptocurrency being used as outright 'Initial Coin Offering' scams, to blackmail via bitcoin, to potential legitimised use in everyday transactions (supported by Apple), this opens doors to whole new areas of transaction laundering and further laundering in general.

With the UK lagging behind in this area, and worse to come, the lesson is clear: laundering is evolving, and unless AML keeps pace, this is a deathmatch that the 'good guys' may find it impossible to win.

### **KCS Group Europe - Strategic Intelligence & Corporate Security**

A leading provider of security and intelligence services, we operate discreetly in some of the world's most difficult environments on complex cases of fraud, theft, corruption, or market dynamics. We gather intelligence through the discreet use of human sources to level the playing field and help our clients to identify and deal with any risks, weaknesses and threats which could impact on their business financially or reputationally.

Our key areas of expertise include:

- Corporate Intelligence Services
- New market or sector entry research
- Know your customer screening

In addition, through our specialist team at KCS IS, we also offer a unique service in the areas of Cyber Security and Cyber Risk. This covers penetration testing, vulnerability assessments, intelligence gathering and cyber security audits, providing unparalleled, analysis, contingency planning, and implementation for our clients.

**To find out more or to arrange a meeting to discuss your business needs, please...  
email the team at [info@kcsgroup.com](mailto:info@kcsgroup.com) or call (00 44) 2072451191**

---