INSIGHTS, THOUGHTS AND OBSERVATIONS

ODD Blog: Protecting your reputation – April 2022

"It takes 20 years to build a reputation and five minutes to ruin it," said Warren Buffett, "If you think about that you'll do things differently."

He was right. Just consider, as an example, travellers' tales told in hotel bars across the globe. Inevitably these include descriptions of horrendous journeys, be they by rail, sea, or air, and almost inevitably conclude with, "and I'm never travelling with them again."

If you, the listener, are unwise enough to ask for more details, you will probably find this blanket statement stemmed from one poor experience: lost luggage, a cancellation or, perhaps, a rude fellow passenger, but now the narrator not only avoids that travel brand, but is intent on advising everyone within earshot to do the same.

A problem afflicting an individual is one thing, but what of the reputational impact of an event which impacts hundreds or thousands of people. British Airways cancellation of all short-haul flights from Heathrow because of computer problems in February this year, for example?

Reflecting Buffett's admonition, one of the things many investors and investment managers are doing differently these days is to commission reputational risk reviews, a key part of robust ODD. These reviews check that an investment they plan to make, or perhaps a service provider they are considering using, will not damage their reputation or financial wellbeing.

One task of such reviews, as conducted by perfORM, is to undertake a deep dive into the contents of a portfolio or corporate structure to ensure there are no skeletons in the closet. In the current investment climate, for example, it would be embarrassing, and probably costly, to be discovered investing with a manager with substantial holdings in sanctioned Russian shares.

F1 champion Lewis Hamilton had an equivalent problem late last year when he had quickly to distance himself from his Mercedes-AMG-Petronas team's sponsorship deal with Kingspan Group, a publicly listed insulation manufacturer, which the press reported was linked directly to the June 2017 Grenfell Tower disaster.

Interestingly, perfORM has recently worked with a leading sports team to carry out ODD on a sponsorship partner in the digital asset space to make sure they are comfortable with being associated with this service provider. Who you get into bed with matters.

Reviews of reputational risk are also actively concerned with the durability of a firm's IT systems, and how safe they are from cyber-attacks.

Examples of failures here are commonplace from the issues experienced by TSB customers in March this year resulting in duplicated debit card payments, to the huge data leak admitted by the online US share-trading platform Robinhood in November 2021. According to the company's statement, an "unauthorised party obtained a list of email addresses for approximately five million people, as well as full names for a different group of approximately two million people…several thousand entries in the list contain phone numbers, and the list also contains other text entries."

perfORM's ODD reviews are not designed to block corporate issues or failures of the type described, but they are critical to ensuring that those who have a fiduciary duty to investors – for example, family offices, funds of funds, pension funds, endowments – are able to exercise that duty responsibly and in-depth.

As Warren Buffett also said, “Risk comes from not knowing what you are doing.”

Digital Asset Custody Risk – February 2022

We have considered the risk of self-custody of digital assets by Investment Managers (IM), i.e. where the IM custodies their own keys in a wallet, and the risk of custody by a qualified custodian, or a custody IT solution. The use of the latter two reduces the IT security risk faced by investors; the cost of such solutions incorporates enhanced and tested IT security. The IM is effectively relocating this risk to a third party, which we would expect to have a controls report, such as a SOC report or ISO certification, which the IM is unlikely to have. The risk of loss due to error or hacking is somewhat reduced.

The use of a qualified custodian or custody IT solution does not, however, mitigate the risk of fraud by authorised keyholders, any more than a self-custody solution. Regardless of how strong the controls in place are, the IM is responsible for setting up the protocols which allow assets to be withdrawn, such as the number and nature of the authorisers, and the whitelisted IP addresses or wallets to which assets can be transferred. Often the IMs are small and have few employees, meaning that the number of signatories is also small and the risk of collusion heightened. In our experience, this is a scenario unique to digital asset funds and is due to the nascent nature of the asset class. In a traditional hedge fund set-up, trades take place in the Fund’s name between registered executing brokers and are given up to regulated prime brokers or custodians; there is limited scope for assets to move outside the regulated environment.

What we learnt about ODD in 2021 that will help inform reviews in 2022 – January 2022

The debate around self-custody versus using a third-party custodian (sometimes classified as ‘qualified’) for investment managers looking to custody digital assets will continue. That debate no longer exists in traditional asset investing, as very few would now consider self-custody a feasible and sensible option. And yet, for digital assets, self-custody is an option, and is often supported by dedicated third-party technology firms. Factors we think that will inform the debate include:

- Increasing involvement of institutional investors and, by default, a bias towards third-party custodians in line with their other assets
- Greater transparency provided by investment managers into their internal controls around self-custody technology solutions, including policies and procedures
- Service, choice and operational track record of custodians will continue to mature. This will improve the breadth of service options that enable investment managers to use a third-party custodian, such as staking
- Consideration of native crypto-custodians’ balance sheets, which continue to improve but still significantly lag traditional assets, raising questions around their safety and security (think $billions instead of $trillions). This may change in 2022, with continued adoption across traditional banking sectors
- Continued improvement in choice and adoption of automatic trade and settlement systems that reduce the need for manual processing
- (Hopefully) an increased number of investment managers and crypto exchanges that are licenced to operate in populous, highly regulated jurisdictions

Tips to those who are targets of ODD in order to be prepared / ready

- Have all your documents – DDQ, presentation, staff organisation chart, etc. – dated within the last three months
- Ensure your firm’s LinkedIn profile is consistent with your documents, including name, randing and employee job titles
- Ensure your internal documents are in line with legal documents, e.g. fund redemption terms in the DDQ match terms in the prospectus

- Be prepared to discuss your approach to cyber security and business continuity in detail; this is a key focus area where we continue to find risk consideration to be lacking for all types of firms
- Ensure your controls for payments out of the fund to third parties are robust; many operational issues arise as a result of wire fraud and as a result this continues to be a key focus for ODD
- Be prepared to explain the level of involvement independent directors have in the oversight of the fund