June 2018

Four take-aways from the CBI's first cyber-fraud fine

Appian Asset Management Limited ("**Appian**") has been fined €443,000 for regulatory failures which, according to the Central Bank of Ireland (the "**CBI**"), left it exposed to cyber-fraud.

This is the first time that the CBI has issued a fine concerning a cyber fraud. Some lessons which can be learnt from the case are considered below.

Background

One of Appian's clients invested €1 million in two Appian managed sub-funds in March 2015. A fraudster hacked the client's web based email account and over a two month period impersonated him in email correspondence with an Appian employee. The fraudster induced Appian to instruct its depositary and transfer agent to liquidate €650,000 of the client's investments and ultimately to pay the funds to two third party corporate accounts, controlled by the fraudster, in the UK.

Key findings

The CBI found that the loss of the client funds which resulted from the fraud was caused by defective controls in three regulatory areas:

i. inadequate policies and procedures to monitor transactions, detect and report money laundering and to provide staff with appropriate training under the Criminal Justice (Money

For further information on any of the issues discussed in this article please contact:

Muireann Reedy
DD: +353 (0)1 674 1002
Muireann.reedy@dilloneustace.ie

Laundering and Terrorist Financing) Act 2010, as amended;

ii. failure to introduce adequate organisational arrangements to minimise the risk of loss of clients assets due to fraud under the CBI's Client Asset Requirements 2007; and

iii. failure to ensure that an employee performing a role that might expose Appian to financial, consumer or regulatory risk was fit for that role under the CBI's fitness and probity regime.

Take-aways

The failings identified in the CBI's detailed publicity statement should remind firms of the following:

- **check for red-flags when processing a "client's" redemption instructions:** e.g. do the instructions match the client's investment strategy; is a request being made to transfer monies into a bank account in a different jurisdiction to where the client resides; are there any other unusual elements to the request such as to split redemption proceeds into smaller amounts; do the instructing emails contain any grammatical or spelling errors? All of the above were referred to as "red flags" for fraud/anti-money laundering in the CBI's publicity statement;

- **follow your policies and procedures and ensure they are sufficiently detailed:** the CBI was critical of Appian's failure to follow its own policies and procedures which prohibited third party payments and required the MLRO to consider and approve all payments to third parties from Appian's client asset account. The CBI also found that Appian failed to fully implement a requirement for original signatures in respect of account mandates/changes.

  The CBI noted that while Appian recognised fraudulent misappropriation of client assets as an operational risk, its organisational arrangements were inadequate for various reasons. These included a failure to describe the circumstances in which Appian staff might verify unusual client instructions or the manner of verification, for example, call-backs. Interestingly, the CBI said that call-backs are best practice for firms without sophisticated verification processes;

- **ensure adequate AML training is given, including on how to identify suspicious transactions**: the CBI found that the one hour annual AML training session given to staff by Appian was insufficient to train them on how to identify suspicious activity. It also found that the scope of the training was not tailored to specific roles;

- **be satisfied that all employees meet the Fitness and Probity Standards:** the CBI found that Appian failed to satisfy itself that an employee complied with the CBI's Fitness and Probity Standards by ensuring he was competent and capable to perform the two controlled functions which had been assigned to him. The CBI said that Appian was required to monitor the relevant employee's competence and to educate him to the requisite standard or otherwise to remove him from his controlled functions if he failed to meet that standard.

Commentary

Cyber security has been a high priority area for the CBI in recent years with it issuing its "Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks" in 2016.

The CBI also announced in its 2017 Annual Performance Statement that a Central IT Risk Team came into effect this year with responsibility for conducting on-site inspections and supporting ongoing supervision in the areas of IT and cyber risk across all regulated sectors.

The Appian fine shows that the CBI's focus on cyber risk will not be going away any time soon.

Contact information

If you have any queries about the information contained in this article, please contact Muireann Reedy of our Regulatory Investigations Unit at Muireann.Reedy@dilloneustace.ie or at 01-674 1002.

Dillon Eustace
June 2018

DILLON EUSTACE

Dublin
33 Sir John Rogerson's Quay, Dublin 2, Ireland. Tel: +353 1 667 0022 Fax: +353 1 667 0042.

Cayman Islands
Landmark Square, West Bay Road, PO Box 775, Grand Cayman KY1-9006, Cayman Islands. Tel: +1 345 949 0022 Fax: +1 345 945 0042.

New York
245 Park Avenue, 39th Floor, New York, NY 10167, U.S.A. Tel: +1 212 792 4166 Fax: +1 212 792 4167.

Tokyo
12th Floor, Yurakucho Itocia Building, 2-7-1 Yurakucho, Chiyoda-ku, Tokyo 100-0006, Japan. Tel: +813 6860 4885 Fax: +813 6860 4501.