Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

Settlement Agreement between the Central Bank of Ireland

and

Appian Asset Management Limited

The Central Bank of Ireland imposes a fine of €443,000 on Appian Asset Management Limited for regulatory breaches causing the loss of client funds

On 13 June 2018, the Central Bank of Ireland (the "Central Bank") fined Appian Asset Management ("Appian" or the "Firm") €443,000 and reprimanded it for significant breaches across three regulatory regimes: client asset, anti-money laundering, and fitness and probity. The breaches have been admitted by the Firm.

The Firm's historic regulatory failures left it exposed to a cyber-fraud by a third party where, acting on the instructions of a fraudster impersonating a client, it facilitated a series of transactions resulting in the loss of €650,000 of a client's funds. The client was fully reimbursed.

The Central Bank had regard to section 33AS(1) of the Central Bank Act 1942, and had it not been for the financial position of the Firm, the Central Bank would have imposed a financial penalty of €825,000.

The Central Bank's enforcement investigation identified that the loss of client funds was caused by Appian's failures in the following areas:

(i) it had defective controls to protect client assets against fraud;

(ii) it had inadequate policies and procedures to monitor transactions, detect and report money laundering and provide its staff with appropriate training; and

(iii) it failed to ensure that an employee, performing a role that might expose the Firm to financial, consumer or regulatory risk, was fit for that role.

Seána Cunningham, the Central Bank's Director of Enforcement and Anti Money Laundering, has commented as follows:

"*This is the first time the Central Bank has imposed a sanction on a firm where there has been a loss of client funds from cyber-fraud as a direct result of the firm's significant regulatory breaches and failures.*

Appian's failures in this case demonstrated serious deficiencies in its governance arrangements, risk management, compliance oversight, and systems of internal control. These failings, combined with a culture in which clients' instructions were given primacy over security and regulatory concerns, rendered the Firm exposed to the cyber-fraud that occurred. It placed client assets at heightened risk and that risk crystallised. The Central Bank views such fundamental failings as completely unacceptable.

The Central Bank expects the Board and senior management of all firms permitted to hold client assets to take active measures to ensure they hold such assets safely and securely.

It is imperative that the people who run firms are vigilant as to their vulnerabilities around cybercrime and should ensure that all appropriate regulatory safeguards are in place to protect their clients' assets.

The level of fine reflects the seriousness of Appian's governance, operational, compliance and risk failures. It also reflects the importance the Central Bank places on investor protection. Regulatory failures of this nature, especially where the failures result in financial losses to clients, will result in vigorous investigation and action by the Central Bank."

BACKGROUND

Appian is authorised as an Alternative Investment Fund Manager ("**AIFM**") under the European Union (Alternative Investment Fund Managers) Regulations 2013 (the "**AIFM Regulations 2013**") on 6 January 2014. Appian was previously authorised under the Investment Intermediary Act 1995 from 14 March 2003. That authorisation was transferred to a MIFID authorisation from 1 November 2007 until the Firm became authorised under the AIFM Regulations 2013.

Appian is authorised, amongst other things, to provide portfolio management functions, and to engage in the following activities in accordance with Regulation 7(4) of the AIFM Regulations 2013:

- manage portfolios of investments; and
- provision of non-core services comprising investment advice and reception and transmission of orders in relation to financial instruments.

Appian manages one Central Bank authorised umbrella fund called the Appian Unit Trust (the "**Fund**") comprising five sub-funds (the "**Sub Funds**").

During the relevant period, Appian was subject to the Central Bank's Client Asset Requirements 2007 (the "**CAR 2007**") because:

- compliance with the CAR 2007 was imposed as a condition of the Firm's authorisation on 6 January 2014; and
- the AIFM Regulations 2013 requires an AIFM which provides individual portfolio management services referred to in Regulation 7(4) to comply with CAR.

THE CYBER-FRAUD

The cyber-fraud was a process which unfolded over a two month period during which no one at Appian formed fraud, money laundering or terrorist financing ("**ML/TF**") suspicions or submitted fraud reports to the Gardaí or suspicious transaction reports to the Gardaí and the Revenue Commissioners.

In March 2015, an experienced businessperson ("**Real Client**") invested €1 million in two Appian managed sub-funds. In April 2015, a cyber-fraudster ("**Fake Client**") having hacked Real Client's web based email account, impersonated him in a protracted series of email correspondence with a particular employee (the "**Employee**"). Fake Client induced Appian to instruct its depositary and transfer agent (the "**Depositary**") to liquidate €650,000 of Real Client's investments in two Sub Funds and pay the proceeds in four tranches to Appian's client asset account. Appian split those proceeds into six smaller amounts that it paid to two third party corporate accounts at UK banks controlled by Fake Client.

Appian processed the redemptions and paid the proceeds to Fake Client's accounts despite Fake Client's instructions including the following red flags for fraud and/or money laundering:

- Real Client was a new client to the Firm and had indicated that his strategy was to hold his investment for the long term. Fake Client's redemption requests came less than two months after Real Client had invested in the Sub Funds;
- Further inconsistencies between Fake Client's instructions and Real Client's profile and financial disclosure including:
    - Redemption to multiple third party corporate accounts outside of Ireland (where Real Client resides);
    - The signatures on the two account mandates for the third party corporate accounts bear questionable resemblance to Real Client's signature which the Firm had on file;
    - The general communication skills, including grammatical and spelling errors, in Fake Client's emails were not consistent with Real Client's profile, that of an articulate businessperson;
    - Fake Client "baited" Appian into believing he would invest €2 million following the sale of a purported Swiss property. Real Client did not own Swiss property. Appian continued to release funds to Fake Client even after the passing of the purported sale completion date without considering why he still needed funds; and
    - Fake Client explained the naming of one of the corporate accounts as having reference to the name of his son. Real Client did not have a son with the name referenced by Fake Client.
- Fake Client's UK bank returned one tranche of funds on three occasions to Appian because Fake Client had given Appian the incorrect account names twice and SWIFT details once.
- Fake Client requested that the payments be split into smaller amounts with the intent of avoiding UK banking controls, and the Firm complied without raising any question.
- Fake Client changed his own (fake) profile during his engagements with Appian. For example, he initially said proceeds would be paid into his personal UK account but later provided details of two corporate accounts instead.

On two occasions, Fake Client used "*spoofing*". He set up a fake account with an address similar to Employee's email address. When Real Client queried redemption notifications, Fake Client intercepted his email and sent responses purportedly from Employee that assuaged Real Client's doubts.

APPIAN'S CLIENT ASSET REGIME BREACHES

On 6 January 2014, the Central Bank authorised Appian as an AIFM. Regulation 7(6A) AIFM Regulations 2013, which came into effect on 27 May 2014, requires AIFMs that provide individual portfolio management services to comply with the CAR 2007.

Appian breached Section 3.1.2(f) of the CAR 2007 by failing to introduce adequate organisational arrangements to minimise the risk of loss of client assets as a result of fraud. Particular failings in this regard are as follows:

(i) The Firm marketed its services to Real Client with reference to asset security and represented that there would be no redemption to third party accounts. Real Client relied on this representation which turned out to be incorrect;

(ii) To facilitate Fake Client's instructions, the Firm circumvented the Depositary's policies and procedures, the prospectus rules for its Sub Funds and the Firm's own policies and procedures by redeeming Real Client's funds into the Firm's own client asset account to facilitate the transfers to the third party accounts; and

(iii) The Firm registered Real Client's assets in the name of the Firm without his consent.

The investigation found that Appian recognised fraudulent misappropriation of client assets as an operational risk but its organisational arrangements were inadequate in the following ways:

- Appian failed to describe or otherwise address fraud risk, including describing red flags for fraud.
- Appian failed to describe the circumstances in which Appian staff might verify unusual client instructions or the manner of verification, for example, callbacks to confirm client identity. Although not a specific requirement under the CAR 2007, callbacks are best practice for firms without sophisticated verification processes.
- Appian failed to implement its own procedures that incorporated redemption rules in a fund prospectus implicitly prohibiting redemptions to third party accounts and clients simultaneously holding more than one account.
- Appian failed to develop its own organisational arrangements to govern redemptions including describing and limiting the circumstances in which it would instruct the Depositary to pay redemption proceeds to its client asset account and how such instructions would be verified and approved.
- The Firm's procedures required director approval of third party payments from its client asset account but did not describe when or how a director should approve payments or the information and supporting documents on which the director should rely.

- Appian failed to fully implement a requirement for original signatures in respect of account mandates/changes. Appian paid to an account with a name that was different from that on the signed mandate in its possession.
- Appian failed to provide client asset training to all client-facing staff or circulate its client asset procedures to them.
- The Firm's organisational arrangements demonstrated a poor approach to client asset risk that treated unusual instructions from high net worth clients as beyond question and placed following client instructions above regulatory and compliance considerations.

APPIAN'S AML/CFT REGIME BREACHES

Appian committed four prescribed contraventions of the AML/CFT regime imposed by the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010, as amended by the Criminal Justice Act 2013 (the "**CJA 2010**").

(i) Failure to monitor and scrutinise client transactions

For the period between 27 April 2015 and 18 June 2015, Appian failed to monitor its dealings with the client and scrutinise transactions to the extent reasonably warranted by the risk of money laundering or terrorist financing, and failed to consider its knowledge of Real Client when acting on Fake Client's instructions, in breach of section 35(3)(a) CJA 2010.

While Appian was in fact acting on the instructions of Fake Client, it thought that Real Client was issuing the instructions, in circumstances where there were reasonable grounds to form money laundering suspicions as a result of the Firm's knowledge of its client and in respect of a series of increasingly suspicious transactions.

The Firm processed the redemptions and paid the proceeds to Fake Client's third party accounts despite Fake Client's instructions including the red flags for money laundering listed earlier at pages 3 and 4 above.

(ii) Failure to adopt policies and procedures to prevent and detect the commission of money laundering and terrorist financing.

Between 15 July 2010 and 3 December 2012, Appian breached sections 54(1) and (2)(a) CJA 2010 by failing to adopt adequate policies and procedures to prevent and detect the commission of money laundering and terrorist financing including adopting policies and procedures to be followed by its staff specifying its CJA 2010 obligations.

Between 3 December 2012 and October 2015, Appian failed to circulate its AML/CFT policies and procedures to frontline staff who needed them, thereby failing to implement them.

In further breach of section 54(2)(a) of the CJA 2010, Appian failed, between 15 July 2010 and October 2015 to adequately assess customer and product risk including generic and firm-specific AML/CFT risks.

Appian's policies did not recognise early redemption as posing a potential ML/TF risk. The Firm's written procedures did recognise third party payments as such a risk and explicitly prohibited the activity. Those procedures also required MLRO consideration and approval of all payments to third parties from Appian's client asset account. Crucially, Appian did not follow these procedures in respect of the fraudulent transactions.

(iii) Failure to report suspicious transactions

Appian breached section 42(1) CJA 2010 from 27 April 2015 to 18 June 2015 by failing, when the Firm have admitted that there were reasonable grounds to suspect a person may have been engaging in money laundering, to report the relevant transactions to Gardaí and the Revenue Commissioners.

While Appian failed to employ an adequate mechanism for the detection money laundering by way of red flag system alerts, it further failed to have the necessary mechanism in place for the escalation and reporting of the unusual nature of the fraudulent activity, internally and to the relevant criminal authorities.

(iv) Failure to ensure staff were instructed on AML/CFT-related law and provided with ongoing training.

From 15 July 2010 to 10 September 2012, Appian breached section 54(6) CJA 2010 because it failed to train anyone involved in the conduct of its business in AML/CFT law or provide on-going instruction on identifying suspicious activity.

From 10 September 2012 to around October 2015 Appian held one hour annual AML/CFT training sessions for staff. The training was sufficient to introduce staff to AML/CFT law but in further breach of section 54(6), it was insufficient to train them to identify suspicious activity. In addition, the scope of the training was not tailored to specific roles, including the Firm's MLRO.

APPIAN'S FITNESS AND PROBITY REGIME BREACHES

Section 21 of the Central Bank Reform Act 2010 (the "**2010 Act**") requires firms to satisfy themselves that employees performing controlled functions (functions that might expose a firm to financial, consumer or regulatory risk) are fit and proper to occupy those roles.

From 2014, when Employee joined Appian, to 2015 when he left, the Firm breached section 21(a) of the 2010 Act by permitting him to perform two controlled functions without satisfying itself Employee complied with the Fitness and Probity Standards 2014 (the "**Central Bank's F&P Standards**"). It breached section 21(b) of the 2010 Act by permitting him to perform those functions without securing his agreement to abide by the Central Bank's F&P Standards when it hired him or thereafter.

Senior Management of Appian should have satisfied itself on reasonable grounds he was competent and capable to perform the two controlled functions it assigned him, CF3 (giving customers advice) and CF4 (arranging financial services), pursuant to section 2.2(a) of the Central Bank's F&P Standards. This necessitated monitoring his competence and educating him to the requisite standard or removing him from his controlled functions if he failed to meet that standard. The Firm did neither.

REMEDIATION

On discovering the fraud, Appian reported it to the Central Bank, An Garda Síochána and the Financial Intelligence Unit. Real Client was fully reimbursed. The Firm did not benefit from the cyber-fraud.

The Firm remediated its failings, and complied with the Risk Mitigation Programme issued by the Central Bank following the fraud. They introduced new client asset and AML/CFT policies and procedures. In relation to client assets, Appian implemented new controls, including additional checks around validation such as independent callback verification of all redemption requests. This, along with other remediation efforts, served to strengthen the Firm's client asset arrangements. The Firm was also required to commission a review of its risk management framework with such review required to extend at a minimum to Board oversight, management capability, risk management processes, compliance function and the risk management culture.

The Firm cooperated with the Central Bank's enforcement investigation and availed of the settlement discount scheme.

PENALTY DECISION FACTORS

In deciding the appropriate penalty to impose, the Central Bank considered the following matters:

- The seriousness of the breaches:
    - The serious nature of Appian's failings – across three regulatory regimes
    - The serious impact - leading to the loss of significant client assets.
    - Appian circumvented its own and the Depository's processes as well as the prospectus rules of its Sub Funds to facilitate the transfer of funds.
    - Appian facilitated the circumvention of UK clearing bank controls by splitting funds into smaller amounts for payment to Fake Client.
- The long duration of the breaches (varying in length between one year and five years).
- The need to impose an effective and dissuasive sanction on regulated entities.
- The co-operation of the Firm during the investigation and in settling at an early stage in the Central Bank's Administrative Sanction Procedure.

The Central Bank's investigation into Appian in respect of this matter is now closed.

NOTES FOR EDITORS

1. On 22 September 2015, the Central Bank sent a Dear CEO letter following its review of the management of operational risk around cyber-security within the investment firm and funds industry that is here. On 13 September 2016, the Central Bank issued cross-industry guidance in respect of IT and cybersecurity risks that is available for download here.

2. The Central Bank's March 2012 "Review of the Regulatory Regime for the Safeguarding of Client Assets" is available for download here. The Client Asset Requirements 2007[1] were replaced on 1 October 2015 by the Client Asset Regulations (the **"CAR 2015**") which are available for download here. The CAR 2015 were revised during 2017 and the Client Asset Requirements now sit in Part 6 of the Central Bank (Supervision and Enforcement) Act 2013 (Section 48(1)) (Investment Firms) Regulations 2017 (S.I. No. 604 of 2017) (the **"CAR 2017**"), which are available for download here. The CAR 2017 does not include a provision equivalent to that contained in Section 3.1.2(f) of the CAR 2007.

3. The Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 is available here. The Department of Finance CJA 2010 Guidelines on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (DoF AML/CFT Guidelines) are here.

4. The Central Bank's F&P Standards are here. The current guidance on its F&P Standards is here.

5. The fine imposed by the Central Bank was imposed under Section 33AQ Central Bank Act 1942. The maximum penalty available under that Act is €10,000,000, or an amount equal to 10% of the annual turnover of a regulated financial service provider, whichever is the greater. The Central Bank had regard to section 33AS(1) of the Central Bank Act, 1942. This states: *"if the Bank decides to impose a monetary penalty on a regulated financial service provider under Section 33AQ or 33AR, it may not impose an amount that would be likely to cause the financial service provider to cease business"*.

[1] Client Asset Requirements issued under S.I. No. 60 of 2007 European Communities (Markets in Financial Instruments) Regulations 2007.

6. The fine that the Central Bank would have been imposed but for Section 33AS(1) reflects the application of the maximum percentage settlement discount of 30%, as per the Early Discount Scheme set out in the Central Bank's "Outline of the Administrative Sanctions Procedure" which is here.

7. The Central Bank has published advice on how to avoid scams and unauthorised activity which is here. There is also guidance available from An Garda Síochána with guidance about how to identify and avoid being a victim of fraud, which is here.

8. This is the Central Bank's 119th settlement since 2006 under its Administrative Sanctions Procedure, bringing total fines imposed by the Central Bank to over €62 million.