



July 2020

BOI fined over €1.6 million in relation to cyber- fraud incidents

The Central Bank of Ireland (the “**CBI**”) has fined The Governor and Company of the Bank of Ireland (“**BOI**”) €1,660,000 for five regulatory breaches relating to two cyber-fraud incidents, and has also criticised it for failing to be open and transparent in a subsequent enforcement investigation into the matter.

The breaches were committed by BOI’s former subsidiary, Bank of Ireland Private Banking Limited (“**BOIPB**”) which was an independently regulated MiFID firm at the time when the frauds occurred, but is now a business unit within the Retail Division of BOI.

Background

The CBI’s investigation related to two separate payment instructions totalling €106,430 which were processed by BOIPB (the “**Incidents**”) and which were purportedly from a client, but were in fact from a cyber-fraudster who had hacked the client’s email account. The client notified BOIPB of the fraud when it received an email from BOIPB referring to recent communications between BOIPB and the client, of which the client was unaware. BOIPB immediately reimbursed the client.

The Findings

The CBI subsequently commenced an investigation into the Incidents and found that there had been five breaches of the European

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

Communities (Markets in Financial Instruments) Regulations 2007¹ and concluded that there were serious deficiencies in relation to BOIPB's third party payments processes.

The CBI found that BOIPB's Third Party Payments Procedure was "*wholly inadequate*" for the purpose of safeguarding client deposits when processing third party payments, as key procedural, security, and authorisation steps were not outlined in the document. The CBI also noted that in processing the fraudulent instructions BOIPB staff had breached BOIPB's internal policies and procedures, and it was also critical of BOIPB's failure to notify the Gardaí about the Incidents, until prompted to do so by the CBI.

Sanctioning Factors

In determining what sanction to impose, the CBI took into account the "ASP Sanctions Guidance" which it published in November 2019 (see link to previous article on this guidance [here](#)).

The CBI said there were two "aggravating" factors in the case. Firstly, it found that BOIPB's level of co-operation with its enforcement investigation was "*far below*" what it expected. It criticised BOIPB for failing to provide it with a copy of a draft internal report, which identified ongoing systemic control failings in the processing of third party payments, when the CBI requested records from BOIPB in the course of its investigation. The CBI acknowledged that the report was ultimately provided to it 19 months later as part of a specific statutory information request, however the CBI noted that in the intervening period BOIPB had strenuously denied the existence of any such failings to the CBI in response to the investigation. The CBI found that BOIPB's failure to be open and transparent had the effect of misleading the CBI in the course of the investigation.

Secondly the CBI was critical of the amount of time which it took BOIPB to fully remediate the deficiencies. It noted that remediation only took place 17 months after the Incidents, and then only following the CBI's intervention.

Comment

The CBI has issued several publications on IT and cybersecurity over the last number of years. The most recent is the industry letter which was sent to the asset management industry in March, setting out the CBI's findings from a thematic inspection into cybersecurity risk management practices in asset management firms. Firms should review the CBI's guidance as a failure to have adequate processes and procedures in place can lead to fines – this is the second time a firm has been fined following a cyber-fraud in just over two years (see article on the previous fine [here](#)).

The case also emphasises the CBI's expectation that firms will be open and co-operative with it during an investigation and shows that a failure to do so, can result in a higher fine.

¹These regulations have been repealed and replaced by the European Union (Markets in Financial Instruments) Regulations 2017.

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
July 2020

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.

DISCLAIMER:

This document is for information purposes only and does not purport to represent legal advice. If you have any queries or would like further information relating to any of the above matters, please refer to the contacts above or your usual contact in Dillon Eustace.

Copyright Notice:

© 2020 Dillon Eustace. All rights reserved.