Banc Ceannais na hÉireann
Central Bank of Ireland
Eurosystem

ENFORCEMENT ACTION

Central Bank of Ireland

and

The Governor and Company of the Bank of Ireland

The Governor and Company of the Bank of Ireland fined €1,660,000 and reprimanded by the Central Bank of Ireland for regulatory breaches causing loss to a client and for misleading the Central Bank in the course of the investigation

On 27 July 2020, the Central Bank of Ireland (the **Central Bank**) reprimanded and fined The Governor and Company of the Bank of Ireland (**BOI**) for five breaches of the European Communities (Markets in Financial Instruments) Regulations 2007 (the **MiFID Regulations**) committed by its former subsidiary, Bank of Ireland Private Banking Limited (**BOIPB**). BOI has admitted the breaches, which vary in length from one to ten years.

In line with its published Sanctions Guidance, the Central Bank has determined the appropriate fine to be €2,370,000, which has been reduced by 30% in accordance with the settlement discount scheme provided for in the Central Bank's Administrative Sanctions Procedure.

The Central Bank's investigation arose from a cyber-fraud incident that occurred in September 2014 (the **Incident**). Acting on instructions from a fraudster impersonating a client, BOIPB made two payments to a third party account totalling €106,430: one from a client's personal current account, the other from BOIPB's own funds. BOIPB immediately reimbursed the client. During a Full Risk Assessment of BOIPB in 2015, the Central Bank discovered a reference to the Incident in an operational incident log.

BOIPB had not reported the cyber-fraud to An Garda Síochána, and only did so at the request of the Central Bank over one year after the Incident.

The Central Bank's investigation found serious deficiencies in respect of third party payments, including:

- Inadequate systems and controls to minimise the risk of loss from fraud
- Inadequate governance, oversight and ongoing review of the systems and control environment
- Lack of staff training and a culture in which fulfilling clients' instructions was given primacy over security and regulatory requirements
- Lack of compliance monitoring.

BOIPB's failure to be open and transparent had the effect of misleading the Central Bank in the course of the investigation. BOIPB failed for a period of 19 months to disclose to the Central Bank an internal report, commissioned following the Incident, which identified ongoing systemic control failings in the processing of third party payments. During that same period, BOIPB strenuously denied the existence of any such failings to the Central Bank in response to the investigation. BOIPB's conduct materially added to the time it took to investigate this case.

This is one of two aggravating factors in this case; the other being the excessive amount of time it took BOIPB to fully remediate the relevant deficiencies. Remediation in relation to third party payment processes took place in February 2016, 17 months after the Incident, and then only following the Central Bank's intervention. In August 2016, the Central Bank determined that a Risk Mitigation Programme (**RMP**) relating to third party payment processes was completed.

The Central Bank's Director of Enforcement and Anti-Money Laundering, Seána Cunningham, said:

"*The Central Bank has a clear expectation that firms are alert to the real and increasing risks from cyber-fraud to the security of their clients' deposits and confidentiality of their clients' financial information, and put in place appropriate safeguards to protect their clients accordingly.*

This is the second time the Central Bank has imposed a sanction on a firm where a client has suffered a loss from cyber-fraud as a direct result of the firm's regulatory failings. BOIPB's failure to put appropriate safeguards in place exposed BOIPB and its clients to the serious and avoidable risk of cyber-fraud. That risk crystallised twice. BOIPB then failed to report the cyber-fraud to An Garda Síochána, which is a serious matter. Reporting illegal activity is essential in the fight against financial crime.

This case should serve to highlight to all firms the importance of ongoing vigilance in the area of cyber security. The Central Bank expects all firms to consider, identify and manage operational and cyber

risks and ensure that their staff receive appropriate training tailored to the risks associated with their duties and responsibilities.

The Central Bank expects pro-active engagement from regulated entities – that extends from self-reporting through remediation and full cooperation with the investigation. The excessive time taken by BOIPB to remediate identified deficiencies and the failure to be fully transparent and open in the context of the Central Bank's investigation were aggravating features in this case."

BACKGROUND

Founded in 1989, BOIPB was first authorised as a "section 10 investment business firm" under the Investment Intermediaries Act, 1995 (the **1995 Act**) on 26 May 2000. This authorisation was subsequently transferred to an authorisation under the MiFID Regulations on 1 November 2007.

At the time of the cyber-fraud, BOIPB was an independently regulated MiFID firm and its primary activity was to provide investment services to high net worth individuals who had investable assets in excess of €1,000,000. In addition, BOIPB provided a full range of banking services to its clients (lending, deposit taking and day-to-day current account banking) as a deposit agent of BOI.

Since 1 September 2017, BOIPB is no longer a MiFID firm and is now a business unit within the Retail Division of BOI. The unit retains the name Bank of Ireland Private Banking as a trading name of the Governor and Company of the Bank of Ireland. Its services are authorised by the Central Bank of Ireland under the licence of BOI, a regulated financial service provider for the purposes of the Central Bank Act 1942. BOIPB's audited financial statements for the year ended 31 December 2016, the last year it existed as a separate entity, reported operating income of €19,867,000.

THE CYBER-FRAUD

Third party payment instructions were processed by BOIPB with particular reference to a procedure called the Third Party Payments Procedure (the **TPPP**), which outlined steps to be followed to verify a client's identity before processing a third party payment instruction.

BOIPB processed two separate payment instructions received in September 2014, purportedly from a client (the **Client**), which in fact were sent by a cyber-fraudster (the **Fraudster**) who had hacked the Client's e-mail account. This led to two transfers totalling €106,430 to be transmitted to a corporate bank account at a UK bank. The first transfer was drawn from the Client's current account, and the second transfer was drawn, at the instigation and

authorisation of BOIPB, from BOIPB's suspense account because the payment from the Client's deposit account was rejected due to insufficient funds.

The Client made contact with BOIPB and notified it of the fraud on 30 September 2014, on receipt of an e-mail from BOIPB indicating recent communications (which were unfamiliar to the Client). The Client was immediately reimbursed by BOIPB.

To facilitate the instructions received from the Fraudster, BOIPB staff, in breach of BOIPB's policies and procedures:

- Released confidential account details to the Fraudster in response to an email request
- Did not ask security questions of the Fraudster when taking transfer instructions and responding to requests for account balances over the telephone
- Did not use the telephone number held for the Client on BOIPB's database, instead speaking to the Fraudster on a telephone number provided in a fraudulent e-mail instruction
- Did not have a second staff member complete a call-back to verify the request.

The Fraudster used the following tactics:

- "*Email hijacking*": hacking the Client's e-mail account and re-directing e-mails coming from BOIPB to a mirror image e-mail account secretly set up by the Fraudster to intercept communications coming from BOIPB in relation to the fraudulent payment requests
- "*Social engineering*": in communications with BOIPB staff, making reference to the purchase of a property, the name of the Client's solicitor, and similar terminology to that used by the Client in other emails.

BOIPB did not identify certain flags which could have been indicative of fraud.

- The Fraudster used the expression "*Ireland Account*" when referring to the Client's current account
- One email sent by the Fraudster from the Client's email account to BOIPB staff was signed off with an entirely different name than the name of the Client. The name used was that of an unrelated client of BOIPB. The BOIPB recipient of the email did not pick up this discrepancy, or if he did, did not query it
- The fraudulent instructions were suspicious in nature. They included: incorrect telephone details; the request for a second substantial transfer within two days of an initial substantial transfer in an amount greater than the balance on the Client's account;

and the remittance of funds to a jurisdiction other than the jurisdiction in which the Client resided.

PRESCRIBED CONTRAVENTIONS

The Central Bank investigation identified the following contraventions:

Contravention 1

BOIPB breached Regulation 33(1)(f)(i) of the MiFID Regulations between 1 November 2007 and August 2016 by failing to implement sound administrative procedures and internal control mechanisms in respect of third party payments.

The Central Bank's investigation found that the TPPP was wholly inadequate for the purposes of safeguarding client deposits when processing third party payments. In particular, key procedural, security and authorisation steps were not outlined in the document. Staff did not receive adequate training on the processing of third party payments to ensure they were fully aware of how to safely process these payments.

Contravention 2

BOIPB breached Regulation 160(2)(f) of the MiFID Regulations between 1 November 2007 and August 2016 by failing to introduce adequate organisational arrangements around third party payments to minimise the risk of loss of client assets as a result of fraud.

The serious weaknesses in the process around third party payments, which had existed for some time, should have been known to management through proper governance, oversight and monitoring. There was no monitoring of third party payments by the first or second lines of defence. Furthermore, the recommendations of the first internal report commissioned by BOIPB in relation to this matter, dated December 2014, were not acted on. Similar weaknesses were identified in a second internal report in January 2016. Remediation of the issues identified in both reports did not take place until February 2016.

Contravention 3

BOIPB breached Regulation 34(3)(a) of the MiFID Regulations between 1 November 2007 and 2 January 2018 by failing to establish, implement and maintain systems and procedures adequate to safeguard the security, integrity and confidentiality of client bank account details.

The investigation found that for the purposes of customer service, BOIPB staff frequently engaged with private clients through e-mail. E-mail communication, because it is more

vulnerable to infiltration by fraudsters than other forms of communication, needs to incorporate additional checks before being acted upon. By failing to identify and provide for this, BOIPB failed to safeguard the security, integrity and confidentiality of information relating to client bank accounts.

Contravention 4

BOIPB breached Regulation 34(1)(c) of the MiFID Regulations between 30 September 2014 and 16 December 2015 by failing to establish, implement and maintain adequate internal control mechanisms designed to secure compliance with its reporting obligations pursuant to Section 19 of the Criminal Justice Act 2011.

BOIPB reported the Incident to its Group Financial Crime Unit (**GFCU**) on 1 October 2014. GFCU, on behalf of BOIPB, did not report the Incident to An Garda Síochána until December 2015, on the instigation of the Central Bank.

Contravention 5

BOIPB breached Regulation 35(2)(c) of the MiFID Regulations by failing to comply with Regulation 34(4) between November 2013 and December 2016 because, for that period, BOIPB's Compliance function failed to monitor, and on a regular basis to assess the adequacy and effectiveness of the measures and procedures put in place and the actions taken to address any deficiencies in respect of third party payments.

The TPPP included a requirement that ad-hoc monitoring of third party payments be carried out by the Compliance function. The investigation found that throughout the period November 2013 to May 2016, no ad-hoc monitoring of third party payments was in fact carried out.

This failure persisted despite two internal reports highlighting the absence of monitoring and the systemic non-adherence to the TPPP.

BOIPB'S RESPONSE TO THE CYBER-FRAUD AND REMEDIATION

The Central Bank expects firms to promptly remediate known deficiencies in their procedures and internal control mechanisms. BOIPB failed to do so.

Following the Incident, BOI Group Internal Audit function (**GIA**) investigated how it had occurred. GIA produced their findings in a report in December 2014, which pointed to systemic failings in the processing of third party payments. GIA strongly recommended that BOIPB carry out sampling to verify the authenticity of other "*high-value interpays*". BOIPB failed to do this. GIA further recommended, that, at a minimum, the procedure in place relating to third party

payments should be enhanced to clarify roles and responsibilities for authenticating and approving third party payments. Again, BOIPB failed to do this. The procedure remained unchanged until February 2016.

In March 2015, BOIPB commissioned a further internal review, this time by BOI Retail Business Assurance (**RBA**) centred on BOIPB's procedures for processing third party payments.

Separately, following the Full Risk Assessment (the **FRA**) conducted in 2015, the Central Bank informed BOIPB that improvements in relation to third party payment processes would be part of the subsequent RMP arising from the FRA as the process in place was "*not robust enough*". The RMP was issued in February 2016, which set out the Central Bank's expectations in relation to the actions needed to improve the third party payment process.

RBA issued its findings in draft to BOIPB in January 2016 (the **RBA Report**). Following an assessment of a sample of third party payment records, RBA concluded that the same issues identified in December 2014 persisted, namely that client identification questions were not consistently being asked of clients as well as other deficiencies in the third party payment process.

BOIPB updated and revised the TPPP in February 2016. The RBA Report was signed-off in June 2016. In August 2016, the Central Bank determined that the full RMP was completed.

BOIPB'S COOPERATION WITH THE CENTRAL BANK

The Central Bank expects regulated entities to cooperate in an open manner at all times and to respond to requests promptly, effectively and accurately.

When the Central Bank's investigation commenced in February 2016, BOIPB possessed the RBA Report which contained highly critical findings in relation to the processing of third party payments. As such, it was highly probative to the Central Bank's investigation.

The Central Bank issued a request for records in February 2016. BOIPB should have provided a copy of the RBA Report when it responded to this request in April 2016. BOIPB failed to do so, instead it included one vague narrative reference to a risk assessment of banking activities (making no reference to a "report" or the fact that it related to third party payments specifically) within a document accompanying the records it supplied in response to the Central Bank's request.

BOIPB disclosed the RBA Report to the Central Bank 19 months after the commencement of its investigation in response to a Central Bank statutory request explicitly requiring production of

the record BOIPB had described as a "*risk assessment*". It was only when the document was disclosed and reviewed that its true nature and content became apparent to the Central Bank.

The Central Bank conducted lengthy enquiries as to the circumstances around BOIPB's failure to promptly disclose the RBA Report and the following arose:

- BOIPB held the RBA Report back as it was in "*draft format*"
- BOIPB decided not to proactively provide the RBA Report to the Central Bank following its signing-off in June 2016. Instead, it would provide the signed-off report to the Central Bank only if specifically requested to do so
- Notwithstanding BOIPB's acceptance of the recommendations of the RBA Report, in the course of the Central Bank's investigation:
    - BOIPB made no reference to the existence of the RBA Report or its highly critical findings until after it was provided to the Central Bank in September 2017; and
    - Until May 2018, BOIPB denied that there were any deficiencies whatsoever in its third party payment processes, despite the manifestly contrary findings of the RBA Report, available since January 2016.

SANCTIONING FACTORS

In deciding the appropriate penalty to impose, the Central Bank considered the ASP Sanctions Guidance issued in November 2019. The following particular factors are highlighted in this case.

The Nature, Seriousness and Impact of the Contravention

- The contraventions revealed serious weaknesses of the management systems and internal controls relating to the processing of third party payments. The Central Bank, at a minimum, expects that firms ensure that there are comprehensive written procedures and robust internal controls, with effective and appropriate oversight and governance afforded to these. BOIPB had a responsibility to have adequate controls in place to protect its clients' deposits, and those controls were not sound
- There was an actual loss of client deposits and the continued exposure of those deposits to potential loss
- The breaches spanned the lengthy period from November 2007 to January 2018.

The Conduct of the Regulated Entity after the Contravention

Aggravating

- BOIPB's level of cooperation was far below what is expected. BOIPB failed to provide complete and timely information and documentation in response to the Central Bank's investigation letter and statutory request. It also provided information to the Central Bank that was imprecise and vague. The cumulative effect was that the Central Bank's investigation was frustrated and prolonged.
- BOIPB did not take remedial action in a timely manner to address the contraventions despite knowledge of the severity of the deficiencies and the attendant risk of further loss to client deposits.

Other Considerations

- The financial position of BOIPB (prior to being merged into BOI on 1 September 2017) and the need to impose a proportionate level of penalty.

The Central Bank confirms that the investigation is now closed.

NOTES

1. The fine imposed by the Central Bank was imposed under Section 33AQ of the Central Bank Act 1942. The maximum penalty under Section 33AQ is €10,000,000, or an amount equal to 10% of the annual turnover of a regulated financial service provider, whichever is the greater.

2. This is the Central Bank's 137th settlement since 2006 under its Administrative Sanctions Procedure, bringing the total fines imposed by the Central Bank to over €105 million.

3. Funds collected from penalties are included in the Central Bank's Surplus Income, which is payable directly to the Exchequer, following approval of the Statement of Accounts. The penalties are not included in general Central Bank revenue.

4. The fine reflects the application of an early settlement discount of 30%, as per the discount scheme set out in the Central Bank's Outline of the Administrative Sanctions Procedure 2018 which is here: link.

5. A copy of the ASP Sanctions Guidance November 2019 is available here: link This guidance provides further information on the application of the sanctioning factors set out in the Outline of the Administrative Sanctions Procedure (see link above) and the Inquiry Guidelines prescribed pursuant to section 33BD of the Central Bank Act 1942 (a copy of which is here: link. These documents should be read together.

6. The European Communities (Markets in Financial Instruments) Regulations 2007 (S.I. No. 60 of 2007) were repealed and replaced by the European Union (Markets in Financial Instruments) Regulations 2017 (S.I. No. 375 of 2017) which are available link and the European Union (Markets in Financial Instruments) (Amendment) Regulations 2017 (S.I. No 614 of 2017) which are available here: link

7. Bank of Ireland Private Banking Limited merged into The Governor and Company of the Bank of Ireland on 1 September 2017.

8. 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: link On 13 September 2016, the Central Bank issued

cross-industry guidance in respect of IT and cybersecurity risks that is available for download here: link

9. On 10 March 2020, the Central Bank issued an industry letter for the attention for the attention of all Board members and Senior Management of asset management firms and published findings of a Thematic Inspection into the cybersecurity risk management practices in Asset Management firms: link