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 €24,500,000 and reprimanded by the Central Bank of Ireland for breaches pertaining to its IT service continuity framework and related internal controls failings

On 30 November 2021, the Central Bank of Ireland (the **Central Bank**) reprimanded and fined The Governor and Company of the Bank of Ireland (the **Firm** or **BOI**) €24,500,000 pursuant to its Administrative Sanctions Procedure (**ASP**) for failures to have a robust framework in place to ensure continuity of service for the Firm and its customers in the event of a significant IT disruption. These IT service continuity deficiencies were repeatedly identified from 2008 onwards but due to internal control failings only started to be appropriately recognised and addressed in 2015. The steps taken by the Firm to address the deficiencies were completed by 2019.

The Central Bank has determined the appropriate fine to be €35,000,000, which has been reduced by 30% to €24,500,000 in accordance with the settlement discount scheme provided for in the Central Bank's ASP.

The Firm has admitted five contraventions[1] occurring between 2008 and 2019 including:

- The failure to demonstrate an ability to ensure continuity of service in the event of significant IT disruption;

[1] Breaches of the European Communities (Licensing & Supervision of Credit Institutions) Regulations 1992 (S.I. No. 395 of 1992) (as amended)) and the European Union (Capital Requirements) Regulations 2014 (S.I. No. 158 of 2014).

- The failure to have effective internal controls to identify deficiencies in the IT service continuity framework and ensure they were escalated to the senior management committees and ultimately the Board; and
- The failure to properly engage and oversee the management of third party IT service providers with respect to IT service continuity.

Firms and their boards are responsible for having an effective IT service continuity framework and associated internal controls. These are core parts of a firm's operational resilience and will continue to be an area of focus as part of the Central Bank's and the European Central Bank's supervisory strategy.

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

"Today's banks and financial services firms are wholly dependent on effective, reliable and resilient IT systems. It is vital that firms have a framework in place so that they can ensure continuity of critical IT services and minimise the impact of any significant disruption.

Without an effective IT service continuity framework, significant IT disruptions, particularly if they were to happen in a bank, could have a very serious impact on millions of customers who rely on ready access to their funds and services to keep their everyday lives and businesses moving.

From 2008 until 2019, BOI was in breach of key regulatory provisions regarding IT service continuity, arising from deficiencies that were repeatedly identified between 2008 and 2015 in third party reports. However, steps to address these deficiencies only commenced in 2015.

The extent and duration of these breaches were particularly serious given the 'always on' nature of the services BOI provides and how pivotal IT is to the entirety of its business operations. The impact of these breaches meant that had a severe disruption event occurred, BOI may not have been able to ensure continuity of critical services, such as payment services. Had BOI's critical services been disrupted, this could have led to adverse effects on customers and the financial system.

This case is an example of robust enforcement action where failures expose consumers and the financial system to serious potential risk. The Central Bank expects boards and senior management of firms to implement and operate robust risk and control frameworks which recognise and address risk issues in a timely way as part of an effective risk culture. This is a core element of operational resilience designed to protect consumers and ensure financial stability."

BACKGROUND

BOI is authorised to carry on banking business in Ireland as a credit institution under Section 9 of the Central Bank Act 1971. BOI is one of the largest banks in Ireland with 169 branches and over 2 million customers. Its principal activities consist of retail and commercial banking. BOI reported total operating income (net of insurance claims) for the year ended 31 December 2020 of €2,645 million.

The European Central Bank (the **ECB**) is the prudential supervisor of BOI and works closely with the Central Bank as part of the Single Supervisory Mechanism (**SSM**).[2]

Under the SSM, the ECB has the power to ask national banking regulators to investigate issues that it has identified, and to take enforcement action where this is merited.

In 2015, BOI's Internal Audit raised concerns about deficiencies in BOI's IT service continuity framework. In 2016, BOI commissioned an internal investigation into how the IT service continuity deficiencies had persisted from 2008 to 2015. The resulting report (completed in October 2017), which was provided to the ECB, identified a number of risk management and internal control failings in respect of BOI's IT service continuity. In addition, the report identified failings relating to BOI's management and oversight of its third party IT vendors and failings relating to its management body having access to information regarding the deficiencies in BOI's IT service continuity framework.

Following consideration of the report, the ECB determined that these issues merited further investigation. The Central Bank's investigation commenced following a referral[3] by the ECB in August 2018.

From 2008, BOI's internal controls in relation to IT service continuity employed a three lines of defence model, whereby:

- the first line of defence owns and manages the risks;
- the second line of defence is responsible for oversight and challenge of the first line of defence and risk oversight; and
- the third line of defence provides independent assurance.

The Central Bank's investigation found that there were failings in each line of defence (as detailed further below). The failures in each line of defence culminated in an overall failure of

[2] The Firm became subject to direct supervision in prudential matters by the European Central Bank as of 4 November 2014.
[3] Pursuant to Articles 4(1) and 18(5) of the SSM Regulation (Council Regulation (EU) No 1024/2013).

this model in relation to the Firm's IT service continuity framework. This is most clearly demonstrated in circumstances where IT service continuity deficiencies were not addressed, despite being repeatedly identified in third party reports, between 2008 and 2015.

The Central Bank's investigation found that BOI had in place second and third lines of defence which were meant to challenge and oversee the first line business unit responsible for IT service continuity. However, both the second and third lines of defence failed to ensure that the first line business unit was acting on the adverse findings of reports prepared by third parties, which had reviewed BOI's IT service continuity framework. In addition, the second and third lines of defence failed, independently, to address and escalate the IT service continuity risks to which BOI was exposed.

Ultimately, these internal control failings resulted in deficiencies in the Firm's IT service continuity framework persisting for a prolonged period. This is particularly serious as the Firm's reliance on IT was significantly increasing year on year, in common with the sector.

In 2015 the Firm initiated steps to address the deficiencies in both its IT service continuity framework and associated internal controls. The Central Bank acknowledges that the steps taken by the Firm have resulted in an overall improvement in its IT service continuity framework and internal controls. Firms and their boards must have in place robust internal controls to ensure that their IT service continuity frameworks are maintained to a necessary standard. This enforcement outcome highlights the actions the Central Bank will take where firms cannot demonstrate that they are maintaining effective IT service continuity frameworks.

PRESCRIBED CONTRAVENTIONS

The Central Bank's investigation identified five breaches relating to the European Communities (Licensing & Supervision of Credit Institutions) Regulations 1992 (S.I. No. 395 of 1992) (as amended) (the **1992 Regulations**) and European Union (Capital Requirements) Regulations 2014 (S.I. No. 158 of 2014) (the **Capital Requirements Regulations**) as set out below.

Contravention 1 – Failure to have in place contingency and business continuity plans in relation to IT service continuity.

From June 2008 to April 2019, the Firm breached Regulation 16(4)(b) of the 1992 Regulations and Regulation 73(3) of the Capital Requirements Regulations by failing to have in place contingency and business continuity plans with regard to IT service continuity to ensure the

Firm's ability to operate on an ongoing basis and limit losses in the event of severe business disruption. In particular:

- The Firm failed to define its critical services[4] or put in place IT runbooks.[5]
- It was unlikely that the Firm would have been able to successfully failover[6] a critical service to a secondary site (in the event a serious incident occurring) within an acceptable timeframe.
- The Firm did not undertake adequate full end-to-end IT service continuity testing.[7]

Contravention 2 – Failure to have in place and maintain robust governance arrangements, including effective processes to identify, manage, monitor and report the risks that the Firm was exposed to and failure to have adequate internal control mechanisms.

From June 2008 to April 2019 the Firm breached Regulation 16(3) (b) and (c) of the 1992 Regulations and Regulation 61(1) (b) and (c) of the Capital Requirements Regulations by failing to have in place and maintain robust governance arrangements including:

- effective processes to identify, manage, monitor and report IT service continuity risks the Firm was exposed to; and
- adequate internal control mechanisms concerning IT service continuity.

These governance failings led to the Firm's failure to address the IT service continuity deficiencies as set out in Contravention 1.

The Firm failed to have in place and maintain effective governance arrangements through its three lines of defence model regarding IT service continuity. As a result, deficiencies in the Firm's IT service continuity framework were identified by third party reports prepared for the Firm but were not managed, escalated and appropriately dealt with by the Firm. This demonstrates a recurring failure that is indicative of poor internal controls and demonstrates

[4] Critical services are business services that provide a substantial banking or operational activity and are of such importance that any weakness or failure in the provision of these activities could have a significant impact on BOI's ability to meet its regulatory and legal obligations and/or control over, or continuity of, its services and activities. They could also adversely impact on BOI's ability to manage risks related to these activities.
[5] A runbook describes how the Firm would continue to provide a service should an incident arise. A runbook would also contain procedures to begin, stop, supervise, test and restart a service/system.
[6] Failover is a procedure by which a system automatically transfers control to a duplicate system when it detects a fault or failure.
[7] End-to-end testing refers to a software testing method that involves testing an application's workflow from beginning to end.

an overall failure of the Firm's three lines of defence model with regard to its IT service continuity framework, which arose due to the following:

First Line of Defence

The first line of defence (the Firm's central IT unit responsible for IT service continuity) failed to (i) have in place effective risk management practices and processes, (ii) have in place an effective risk register, and (iii) manage and escalate findings from third party reports.

Second Line of Defence

The second line of defence failed to provide robust oversight and challenge of the first line of defence. The second line of defence failed to ensure that the first line of defence was adequately identifying, managing and escalating risks. Furthermore, the second line of defence failed to independently (of the first line) manage or monitor IT service continuity risks to which the Firm was exposed.

Third Line of Defence

The third line of defence failed to understand the gravity of the key IT service continuity risks within the Firm from 2008 to 2015. Additionally the third line of defence failed to provide robust oversight and challenge of the Firm's first and second lines of defence in relation to the risk management of IT service continuity.

Contravention 3 – Failure to have in place and maintain robust governance arrangements, including a clear organisational structure with well-defined, transparent and consistent lines of responsibility.

From June 2008 to April 2019 the Firm breached Regulation 16(3)(a) of the 1992 Regulations and Regulation 61(1)(a) of the Capital Requirements Regulations by failing to have in place a clear organisational structure with well-defined, transparent and consistent lines of responsibility in relation to IT service continuity.

In this case, the first line business units were siloed, which resulted in an uncoordinated approach to IT service continuity with no consistent processes or procedures in place for managing and reporting IT service continuity requirements and risks. In addition, there was no well-defined, transparent and consistent second line function with responsibility for overseeing and challenging IT service continuity requirements and risks across the Firm to ensure that they were being adequately managed.

The first line unit responsible for IT service continuity was identifying risks, however, due to the siloed nature of this unit, stakeholders within the Firm had limited or no visibility of these IT service continuity risks. This had the effect of excluding key stakeholders in the Firm from involvement in the assessment of prioritisation decisions regarding IT service continuity, which is a key area of operational risk.

Contravention 4 – Failure to adequately develop a clear understanding of the roles, responsibilities, accountabilities and clear interdependencies between third party IT service providers.

From June 2008 to December 2019 the Firm breached Regulation 16(4)(a) of the 1992 Regulations and Regulation 61(3)(a) of the Capital Requirements Regulations by failing to adequately develop a clear understanding of the roles, responsibilities, accountabilities and interdependencies between different third party IT service providers.

Contravention 5 – Failure to ensure that the Firm's management body had adequate access to information on the Firm's risk situation.

The Firm breached Regulation 64(13) of the Capital Requirements Regulations, from 31 March 2014 (when the requirement was introduced) until Q4 2015, by its failure to ensure that the Firm's management body had adequate access to information on the Firm's risk situation in respect of IT service continuity, which was a key area of operational risk. Specifically, the findings of third party reports which identified deficiencies with IT service continuity were not made available to the Firm's management body.

SANCTIONING FACTORS

In deciding the appropriate penalty to impose, the Central Bank had regard to the Outline of the Administrative Sanctions Procedure 2018 and the ASP Sanctions Guidance November 2019. It considered the need to impose a level of penalty proportionate to the nature, seriousness and impact of the contraventions and the size of the Firm's operations. The Central Bank also had regard to the need for deterrence. The following particular factors are highlighted in this case:

The Nature, Seriousness and Impact of the Contravention

Duration and frequency of the contravention

- The Firm failed to have an adequate IT service continuity framework and associated internal controls in place over a sustained period from 2008 to 2019, despite the repeated

reporting of these IT service continuity framework deficiencies by third parties from 2008 to 2015.

Serious or systemic weakness of the management systems or internal controls relating to all or part of the business

- The investigation found serious weaknesses in: IT service continuity plans; internal controls; organisational structures and consistent lines of responsibility; appropriate management of the Firm's third party IT vendors concerning IT service continuity; and reporting to management body of IT service continuity risks.

The impact or potential impact of the contraventions

- IT underpins the delivery of services across the entirety of the Firm's business operations. In the event of a significant IT disruption, the Firm could potentially have been exposed to significant risk and potentially have been unable to continue to provide critical services, such as payments. This could have caused serious financial and reputational damage to both the Firm and the wider financial system.

The loss or detriment or risk of loss or detriment caused to consumers or other market users

- While no detriment arose in this case, had a significant IT failure or prolonged outage occurred, given the increasing dependence on online banking, this could have had a very serious impact and could have resulted in customers being denied access to the basic banking services they needed on a day to day basis.

The extent to which the contravention departs from the required standard

- The contraventions represented a serious departure from the required standards expected of the Firm to ensure that in the event of a significant IT incident the Firm could ensure continuity of critical services.

The Conduct of the Regulated Entity after the Contravention

Mitigating:

The following two mitigating factors, indicative of exemplary co-operation and self-reporting on behalf of the Firm, applied in this case:

- *the regulated entity proactively and voluntarily provides the Central Bank with the output of any pre-existing internal investigation and/or third party review;*

- *there has been identification of other contraventions by the regulated entity.*

The investigation found that, following concerns that had been raised by its Internal Audit in 2015 about deficiencies in BOI's IT service continuity framework, BOI commissioned an internal investigation in 2016 (completed in 2017) into how the IT service continuity deficiencies had persisted from 2008 to 2015. The resulting report:

a) was proactively and voluntarily provided to the ECB;

b) identified a number of risk management and internal control failings in respect of BOI's IT service continuity; and

c) identified a number of additional contraventions relating to BOI's management and oversight of its third party IT vendors and failings relating to its management body having access to information regarding the deficiencies in BOI's IT service continuity framework.

This assisted the Central Bank's investigation, facilitated the review of documentation, and reduced the time and resources required to complete the investigation.

The Previous Record of the Regulated Entity

Aggravating:

- The Firm has been the subject of four prior enforcement actions.

Other Considerations

- The need to have an appropriate deterrent impact on the Firm and other regulated entities.

This enforcement action against the Firm is now concluded.

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 145th settlement under its Administrative Sanctions Procedure, bringing the total fines imposed by the Central Bank to over €191 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 2018 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. In accordance with the SSM, the Firm became subject to direct supervision in prudential matters by the ECB as of 4 November 2014.

7. The European Communities (Licensing & Supervision of Credit Institutions) Regulations 1992 (S.I. No. 395 of 1992) (as amended) were in force between 1 January 1993 to 31 March 2014; a copy can be found here: link. These were repealed and replaced by the European Union (Capital Requirements) Regulations 2014 (S.I. No. 158 of 2014) which are here: link.

8. 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. The Firm has been the subject of four previous settlement agreements with the Central Bank, as follows:

- 2012: Breaches of the Assets Covered Securities Act 2001 and Regulation 16 of the European Communities (Licensing & Supervision of Credit Institutions) Regulations 1992.
- 2016: Breaches of the Consumer Protection Code 2012.
- 2017: Breaches for non-compliance with the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010.
- 2020: Breaches of European Communities (Markets in Financial Instruments) Regulations 2007.