



Banc Ceannais na hÉireann
Central Bank of Ireland

Eurosystem

**Settlement Agreement between the Central Bank of Ireland
and Ulster Bank Ireland Limited**

**Central Bank of Ireland imposes fine of €3,500,000 in respect of
IT governance failures by Ulster Bank Ireland Limited**

The Central Bank of Ireland (the “Central Bank”) has fined Ulster Bank Ireland Limited (the “Firm”) €3,500,000 and reprimanded it in relation to IT and governance failings by the Firm that resulted in approximately 600,000 customers being deprived of essential and basic banking services over a 28 day period during June and July 2012. The fine and reprimand are in addition to a redress scheme required and overseen by the Central Bank under which the Firm has paid approximately €59 million to affected customers.

The Central Bank found that the Firm failed to have robust governance arrangements in relation to its IT systems and controls and that, as a result, a major and prolonged IT failure occurred. Alongside causing widespread and significant loss and inconvenience to customers, the IT failure also threatened confidence in the operation of the retail banking sector as it effectively prevented the Firm from participating in the process used to settle payments among banks (“clearing”). These findings have been accepted by the Firm as part of the settlement agreement between the Central Bank and the Firm.

The Central Bank's Director of Enforcement, Derville Rowland, has commented as follows:

“The summer of 2012 saw an unprecedented disruption to banking services as a result of a failure that occurred on the IT systems that Ulster Bank Ireland Limited used to process daily banking transactions. The IT failure caused significant and unacceptable inconvenience to affected customers trying to carry out their everyday financial transactions. Over a prolonged period of time customers were unable to access cash through ATMs/cash and pay for goods and services and there was a delay in the processing of payments in and out of accounts. As the provision of financial services to customers represents the core business function of the Firm, the major breakdown in the Firm's provision of these services as a result of IT failings is completely unacceptable.

This enforcement action taken under our Administrative Sanctions Procedure is one of a number of measures that have been taken by the Central Bank in respect of the IT governance failings of the Firm. The €3,500,000 fine is the highest that has been imposed to date by the Central Bank and it reflects the seriousness with which the Central Bank views the failings of the Firm and the Central Bank's determination to ensure that customers have access to core banking services without disruption. In addition, the Central Bank required the Firm to put in place a comprehensive redress plan in response to the major inconvenience and disruption which has paid approximately €59 million to affected customers.

Firms are required to ensure that they maintain robust governance arrangements including, amongst other things, appropriate internal control mechanisms covering all aspects of their operations and infrastructure. IT systems critically underpin and support a firm's operations and accordingly it is essential that robust IT governance arrangements are in place to ensure continuity of service.

While the Central Bank recognises that IT outsourcing is a feature of modern banking business, outsourcing is no defence for regulatory failings. Ultimate accountability for compliance remains with firms and they must ensure that they maintain oversight of outsourced activities. Senior management must ensure that risks associated with outsourced activities are appropriately managed and must be aware that outsourcing arrangements can never result in the delegation of their responsibility to manage the risks associated with such activities. The obligations imposed upon firms and management applies equally to situations

where activity is outsourced on an intra-group basis or to a third party. Where firms and their management fail to ensure that robust governance arrangements are in place for in-house and outsourced IT systems, they should expect vigorous investigation and follow up by the Central Bank, and for the Central Bank to exercise its powers, including sanctioning powers where appropriate.

The Central Bank would like to acknowledge the cross-jurisdictional cooperation it received from the Financial Conduct Authority and the Prudential Regulation Authority in the UK.”

Background

The Firm is reliant on the Royal Bank of Scotland Group (“**RBSG**”) for the provision of IT services including IT risk oversight and management. The Firm entered into an outsourcing services agreement with RBSG for the provision of IT services in 2005.

During June 2012, software that RBSG used to process banking transactions across all of its businesses, including the Firm, failed. The immediate cause of the failure arose from difficulties with a software upgrade supplied by a third party that had been installed by RBSG a few days prior to the IT incident. As a result of the IT incident, the process of updating transactions and customer payments did not run for an extended period of time. This resulted in significant customer and market place disruption. Full account services for the Firm’s customers were not restored until 16 July, which was 28 days after the IT incident first occurred.

The impacts of the IT incident on the Firm’s customers included: late processing of payments in and payments out of accounts; inability to access ATMs/cash; late transfers of payments against customers’ credit card balances; incorrect credit and debit interest on accounts/cards; duplicative payments; customers’ inability to honour financial commitments (with impact on credit history); inability to pay for goods and services; inability to use online banking; inability of commercial customers to use the banking system and inability to view account balances. Additionally, customers of other financial services providers were also affected as they were unable to receive monies from the Firm’s customers and were accordingly unable to honour their own financial commitments.

The Firm took steps to accommodate affected customers during the period of the IT incident. These steps included extending branch and call centre opening times, extending credit limits, offering free cash advances to customers, using a third party bank to process key payments and reassuring customers that their credit history would not be permanently affected. While

the Firm provided updates to customers regarding the timelines for resolution of the IT incident based on information provided to it, due to a lack of understanding of the complexity of the manner in which its banking transactions were processed, these timelines proved inaccurate.

Central Bank Action

After the occurrence of the IT incident, the Central Bank immediately engaged with the Firm and RBSG, together with the then UK Financial Services Authority (“FSA”), with a view to resolving the disruption caused by the IT incident as quickly as possible. The Central Bank closely monitored the steps taken by the Firm and RBSG to resolve the IT incident and to mitigate its effects. The threat of widespread disruption to the clearing and settlement system posed by the IT incident was mitigated through cooperation between the Central Bank and the Irish Payments Services Organisation that involved the coordination of industry support in order to address and manage the threat. Industry support resulted in the re-routing of bulk electronic payments, including corporate payrolls and social welfare payments, through another clearing bank.

Following the resolution of the IT incident, the Central Bank required the Firm to implement a redress scheme and engaged extensively with the Firm regarding the development of the key principles of that scheme as well as the operational readiness of the Firm to implement the scheme. The Central Bank was concerned to ensure that all affected customers, where appropriate, could avail of redress and that full details of the scheme were made publicly available. The redress scheme commenced on 3 September 2012 and the Central Bank actively monitored the implementation of the scheme. To date the Firm has paid approximately €9 million in redress related to the IT incident.

The Central Bank also contributed to the scoping of an independent review ordered by the FSA, to establish the causes, consequences and management of the IT incident. The review identified a number of serious issues regarding the Firm’s governance arrangements. On foot of the review the Central Bank required the Firm to implement a programme of remediation to address these specific issues. The programme is currently being implemented by the Firm. The programme is scheduled to be fully implemented by March 2015.

As part of the programme the Firm is taking steps to ensure that it has effective oversight of the IT systems on which its business operates and that controls and testing processes are in place. The Firm has also enhanced its outsourcing framework. Enhancements include new service level agreements, service performance monitoring, risk oversight and the appointment of a dedicated outsourcing services team. The Firm's incident management framework has also been strengthened and detailed business contingency plans are in place including an extensive list of temporary business processes which can be deployed in the event of a core systems failure.

The implementation of the programme is being verified by the same independent third party that conducted the review in order to provide assurance that the work undertaken by the Firm as part of the programme will address the specific issues identified in the review. The Board of Directors of the Firm has undertaken to provide assurance to the Central Bank that the programme has been fully implemented after its completion.

Contravention

Regulation 16 of the European Communities (Licensing and Supervision of Credit Institutions) Regulations 1992 (the "**1992 Regulations**") required every credit institution to have robust governance arrangements, including effective processes to identify, manage, monitor and report the risks it was or might have been exposed to and to have adequate internal control mechanisms¹. The Firm breached Regulations 16(3), 16(3)(b) and 16(3)(c) of the 1992 Regulations by failing to have: (i) robust governance arrangements in relation to its IT systems and controls; (ii) effective processes to identify, manage, monitor and report the IT risks it was or might have been exposed to; and (iii) adequate internal control mechanisms in place to sufficiently manage the IT environment in which it operated.

The Central Bank has concluded that the Firm did not have adequate governance arrangements to ensure appropriate oversight of the IT services provided by RBSG and therefore did not comply with its obligations under Regulation 16 as a licensed credit institution. The Firm did not ensure that appropriate testing was conducted in relation to the software affecting the processing of banking

¹The 1992 Regulations were revoked by **Regulation 161** of the European Union (Capital Requirements) Regulations 2014 (the "**2014 Regulations**") with effect from 31 March 2014. The 2014 Regulations impose new obligations on credit institutions in respect of governance arrangements and systems and controls.

transactions which directly affected its ability to provide core banking services to its customers. The manner of processing banking transactions that was used by RBSG was not properly understood by the Firm. The Firm did not understand the potential impact of the related risks on its operations and customers and thus was not in a position to demonstrate that it satisfied its regulatory obligations in this regard. Furthermore it did not have the expertise or understanding to resolve the IT incident within an appropriate timeframe.

Penalty Decision Factors

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

- There were systemic weaknesses in the Firm's governance arrangements in relation to IT systems and controls and the outsourcing of those systems and controls. Accordingly the Firm did not have a proper understanding of the IT infrastructure on which its business operated, and did not understand the risks associated with that infrastructure and the software used to process its customers' banking transactions.
- There was no appropriate business continuity/contingency plan in place to enable the Firm to recover in a timely manner from an incident like the IT incident in June 2012;
- The extended duration of the IT incident;
- The significant loss and inconvenience caused to customers of banking services as a result of the IT incident;
- The potential impact of the contraventions on the orderliness of financial markets and public confidence in those markets due to the Firm's inability to participate in clearing and settlement;
- The risk mitigation programme that the Firm is in the process of implementing to remediate the deficiencies identified;
- The redress scheme implemented by the Firm;
- The previous compliance record of the Firm;
- The cooperation of the Firm during the investigation and in settling at an early stage in the Central Bank's Administrative Sanctions Procedure.

The Central Bank confirms that the matter is now closed.

- End -

Notes to Editors:

- (1) The fine imposed by the Central Bank represents the maximum amount that the Central Bank could impose in the circumstances, allowing for settlement discount in accordance with Central Bank policy. Prior to the commencement of the Central Bank (Supervision and Enforcement) Act 2013 (the “**2013 Act**”) the maximum penalty that the Central Bank could impose on a body corporate under section 33AQ of the Central Bank Act 1942 was €5,000,000. As the breaches at issue in this case occurred prior to the commencement of the 2013 Act the maximum penalty that the Central Bank could impose was €5,000,000. Since the commencement of the 2013 Act the Central Bank may impose a monetary penalty upon a body corporate or an unincorporated body of the greater of €1,000,000 or an amount equal to 10 per cent of the turnover of the body for its last complete financial year before a finding is made and a monetary penalty of €1,000,000 upon a natural person.
- (2) The fine imposed by the Central Bank is the highest fine imposed to date under the Administrative Sanctions Procedure. In July 2013, the Central Bank entered into a settlement agreement under the Administrative Sanctions Procedure with Quinn Insurance Limited (In Administration). The Bank levied a fine of €5,000,000 in that case. As noted in the press release announcing that settlement, however, the fine was waived given the wholly exceptional circumstances of that case ([http://www.centralbank.ie/press-area/press-releases/Pages/SettlementAgreementbetweentheCentralBankofIrelandandQuinnInsuranceLimited\(UnderAdministration\).aspx](http://www.centralbank.ie/press-area/press-releases/Pages/SettlementAgreementbetweentheCentralBankofIrelandandQuinnInsuranceLimited(UnderAdministration).aspx)).
- (3) As set out in the Central Bank’s “Outline of the Administrative Sanctions Procedure”, the Central Bank allows for a maximum percentage settlement discount of 30% to be applied to any monetary penalty that would otherwise be expected to be imposed on a regulated entity should a settlement agreement be reached during Stage 1 of the Administrative Sanctions Procedure and a maximum percentage discount of 10% to be applied should a settlement agreement be reached during Stage 2 of the procedure.
- (4) Firms should also ensure that their operations are consistent with guidelines issued by the Committee of European Banking Supervisors (“**CEBS**”) in December 2006 in respect of outsourcing. The European Banking Authority took over all of the responsibilities and tasks of CEBS with effect from 1 January 2011 and the guidelines remain effective. The guidelines set out, amongst other things, that the ultimate responsibility for the management of the risks associated with outsourced activities rests with the senior management of the outsourcing firm and that outsourcing arrangements can never result in the delegation of senior management’s responsibility. The European Banking Authority (“**EBA**”) is an independent EU Authority which works to ensure effective and consistent prudential regulation and supervision across the European banking sector. Its overall objectives are to maintain financial stability in the EU and to safeguard the integrity, efficiency and orderly functioning of the banking sector.
- (5) While the Central Bank will take the action as outlined above in respect of failures by firms to ensure that robust governance arrangements are in place when it is within its remit to do so, in certain instances the European Central Bank (“**ECB**”) and not the Central Bank will be the competent authority for the investigation and sanctioning of governance breaches amongst other breaches of financial services and regulatory law, since the introduction of the Single Supervisory Mechanism on 4 November 2014. There will also be other instances where the ECB may require the Central Bank to open proceedings with a view to taking action in order to ensure that appropriate penalties are imposed in respect of breaches of financial services and regulatory law. The Central Bank is committed to ensuring that governance breaches are investigated and pursued by the appropriate authority, be that the ECB or the Central Bank itself.
- (6) The Irish Payments Services Organisation (“**IPSO**”) was the industry body for payments services in Ireland at the material time. Since the IT incident the IPSO has integrated with the Irish Banking Federation to form the Banking and Payments Federation Ireland.
- (7) RBSG is now supervised by the Financial Conduct Authority (“**FCA**”) and the Prudential Regulation Authority (“**PRA**”). The FCA and the PRA were established, with effect from 1 April 2013, pursuant to the United Kingdom’s Financial Services Act 2012.
- (8) RBSG was directed to commission the review to establish the causes, consequences and management of the IT incident by the FSA pursuant to section 166 of the United Kingdom’s Financial Services and Markets Act 2000. The Central Bank provided input into the scope of the review.