When overnight processing failed, could the numbers still be trusted?

Royal Bank of Scotland, NatWest and Ulster Bank | United Kingdom | June 2012

ACTUAL CAUSE	CUSTOMERS AFFECTED	REGULATORY PENALTIES	CUSTOMER REDRESS
Software incompatibility after back-out S01	**At least 6.5 million in the UK** S01	**£42m FCA + £14m PRA** S02 | S03	**Approximately £70.3m in the UK** S01

DOCUMENTED EVENT

In June 2012, Technology Services - the banks' centralised group IT function - backed out an upgrade to batch-scheduler software. The upgraded and previous versions were incompatible. The FCA identified the compatibility issue as the actual cause and inadequate IT-risk systems and controls as the underlying cause. [S01]

The incident disrupted processing across RBS, NatWest and Ulster Bank. Some channels remained available while showing out-of-date balances or incomplete transaction histories. Incorrect interest was applied, statements were inaccurate or duplicated, payments were delayed and full participation in clearing was affected. [S01][S03]

At least 6.5 million UK customers were affected. The FCA imposed a £42 million penalty, the PRA imposed £14 million, and the FCA Final Notice records approximately £70.3 million of redress to UK customers. [S01][S02][S03]

NFRISK SCENARIO ADAPTATION - NOT A REGULATOR FINDING

Imagine that an overnight scheduler is backed out after a change. Channels remain partly available, but account updates are incomplete. Customers see stale balances, interest is applied incorrectly, payments queue behind and different systems recover at different speeds. How quickly would the institution know which numbers can still be relied upon?

STRESS-TEST QUESTIONS

01 Would change and back-out testing expose compatibility and downstream data effects before production?

02 Can monitoring distinguish late completion from incomplete, duplicated or misordered processing?

03 Who can declare balances trustworthy after recovery, and what evidence must support that decision?

04 Are important services tested through customer and clearing outcomes, rather than platform availability alone?

CONNECTED RISK

Technology & Change | Operational Resilience | Data & Control Integrity | Payments

RETROSPECTIVE REGULATOR-LINKED RELEVANCE

UK operational resilience
The FCA later used the incident as an example in CP19/32. This establishes retrospective relevance; it does not mean the later regime applied to the 2012 event. [S04]

NFRISK ANALYTICAL MAPPING

Basel event-type lens
Primary: Business disruption and system failures. Secondary: Execution, delivery and process management. This is not a regulator determination. [S05]

NFRISK PRACTITIONER INTERPRETATION

Availability is not the same as integrity. The key question is whether balances, interest, statements and payment positions remain complete, current and trustworthy after change, back-out and recovery. Recovery evidence should prove data integrity and business-service outcomes, not merely technical availability.

PRIMARY-SOURCE REGISTER

S01 FCA Final Notice (2014)
S02 FCA penalty announcement (2014)
S03 PRA penalty announcement (2014)
S04 FCA CP19/32 (2019)
S05 Basel Sound Practices (2003)

EVIDENCE BOUNDARY Official findings above are separated from the institutional scenario, framework interpretation and NFRisk practitioner view.