

the **Availability Digest**

www.availabilitydigest.com
[@availabilitydig](https://twitter.com/availabilitydig)

Banks Worldwide Suffer from IT Legacy

February 2014

Banks around the world seem to be experiencing outages at an ever increasing rate. Lloyd's Banking Group appears to be the latest casualty.



The Lloyds Banking Group Outage

On the afternoon of January 26, 2014, customers of the banks comprising Lloyds Banking Group could not use their debit cards nor could they withdraw money from ATMs. The Lloyds Banking Group banks include Lloyds, TSB, and Halifax. Hundreds of thousands of customers were left at checkout counters or gas stations unable to pay for their purchases. The outage lasted from 3 PM to 7:30 PM. Once service was restored, there were additional delays as the backlog of transactions was cleared.

About one-quarter of card payments were affected, and half of all ATMs were down. Online and telephone banking services were not affected.

According to sources, there was no maintenance or update activity going on at the time of the failure. Rather, the failure was caused by two of seven servers that process debit-card transactions. Conjecture is that one of the servers was a production server and the other was its backup. It appears that the bank lost a server and then suffered a failover fault.

The bank's IT systems are a patchwork of dated systems cobbled together through acquisitions over the recent years. Its core system is a Unisys system dating from the 1980s.

As a cost-cutting measure, Lloyds has cut IT staff and outsourced much of its IT support to India. Lloyds made it clear that outsourcing was not an issue in the failure.

Following similar failures at other U.K. banks, the Financial Conduct Authority (the U.K. banking regulatory body) has asked banks to name their IT leaders who can be held accountable in the event of their systems failing

Royal Bank of Scotland

The Royal Bank of Scotland (RBS) suffered a much more serious outage on Cyber Monday, December 2, 2013, the busiest online shopping day of the year.¹ Millions of customers could not access cash via ATMs. They could not use their credit cards or debit cards. They could not access their accounts via the Web or via their mobile apps. The outage affected all of the subsidiary banks of RBS – not only the Royal Bank of Scotland but NatWest and the Ulster bank as well.

¹ [Royal Bank of Scotland Suffers Multiple Outages, Availability Digest; December 2013.](http://www.availabilitydigest.com/public_articles/0812/RBS_system_neglect.pdf)
http://www.availabilitydigest.com/public_articles/0812/RBS_system_neglect.pdf

No specific reason for the outage was given by RBS. However, a statement by its CEO indicated that the outage was the result of mergers and acquisitions. The RBS IT environment had become a patchwork of systems that was becoming more and more difficult to maintain. For years, RBS had made little investment in their IT systems, preferring instead to struggle with their aging infrastructure.

This has led to a series of outages over the prior several months. In March of 2013, RBS, NatWest, and Ulster Bank mobile applications went down for six hours. Customers could not access their accounts via their mobile phone apps. Earlier in the year, ATMs and all online access were down.

The granddaddy of all outages hit RBS in June of 2012. It caused weeks of havoc. The outage was caused by an upgrade gone massively wrong. The bank had decided to upgrade its CA 7 batch facility to a new version. It found a problem with the new version and backed it out, returning to its current version. However, in the process, the IT staff accidentally deleted a key control file that prevented the overnight batch job from completing.

It took a week to pinpoint the cause of failure and to resume the batch run. However, during this time, scheduled bills could not be paid, employers could not pay their employees, and pensioners could not get their pension payments. Interbank transfers could not be made, which spread the problem to other banks.

It took more than two additional weeks to work through the backlog of transactions that had accumulated during the outage and to resolve all of the problems so that the systems could be returned to normal operations.

Australia's Painful Banking Outages

There have been a series of major outages at Australia's four largest banks over the last two years.² The National Australia Bank (NAB), Commonwealth Bank, the Australia and New Zealand Bank (ANZ), and Westpac have all had their shares of outages affecting ATMs, retailers' POS devices, and online banking. The outages have occurred as these historic banks engage in multi-year replacements of their aging core legacy systems, some dating back to the 1980s. Apparently, these systems have become quite fragile in their old age.

National Australian Bank (NAB)

November, 2010

NAB clears payments for many other banks in Australia by conducting nightly batch runs on behalf of its partner banks. A transaction-history file showing all payment activity for each bank is generated and is sent to that bank by the end of day.

Early on the morning of Wednesday, November 24, 2010, NAB's partner banks went on high alert when they did not receive their transaction files. Without these files, the banks had no record of the previous day's transactions that affected their customer accounts. Payroll deposits could not be made. Credit-card payments were frozen. Direct debits for bill paying went into limbo. Interbank payments ceased. The NAB ATMs were down, as were its online banking services. Retailer point-of-sale terminals managed by NAB were useless. Centrelink welfare payments could not be made to the neediest families in the country.

It was reported that someone from NAB's IT department inadvertently uploaded an erroneous file that "corrupted" the system. The conjecture is that the file contained the instructions for managing the batch-processing cycle. It apparently caused many transactions to be duplicated and the batch run to fail.

² [Australia's Painful Banking Outages](http://www.availabilitydigest.com/public_articles/0703/australian_bank_outages.pdf), *Availability Digest*, March 2012.
http://www.availabilitydigest.com/public_articles/0703/australian_bank_outages.pdf
[Commonwealth Bank of Australia – a Correction](http://www.availabilitydigest.com/public_articles/0704/commonwealth_bank_correction.pdf), *Availability Digest*, April 2012.
http://www.availabilitydigest.com/public_articles/0704/commonwealth_bank_correction.pdf

The problem did not last for hours. It lasted for days as customer accounts were reconciled. Some problems carried over almost two weeks after the incident.

January, 2011

A glitch in NAB's secure login system took down telephone banking at 9 am on January 31, 2011. Fortunately, security was not breached; and telephone banking was restored seven hours later.

April, 2011

Déjà vu. Just five months after its November, 2010, batch processing meltdown, NAB suffered a similar outage. A problem in its overnight batch settlement system caused transaction files not to be delivered to its partner banks. The problem took several hours to fix. Days passed before the bank could catch up on the resulting backlog and reconcile its customer accounts.

February, 2012

In February, 2012, NAB's online banking services suddenly disappeared at 8:20 pm. NAB's eight-million customers nationwide were left without access to ATMs, Internet banking, telephone banking, and credit-card services. Bills could not be paid online. Customers could not withdraw cash from their accounts. Services were not restored until the next afternoon, eighteen hours later.

Westpac

March, 2011

On March 3, 2011, some customers found that they could not log on to Westpac's online banking services. The problems were intermittent and seemed to move from customer to customer. Affected customers could not transfer funds, use their credit cards, or get cash from some ATMs.

The problem was evidently due to server overload. Westpac reported that its servers were running at 80% of capacity during this time. Presumably, random customer attempts to use its online services were timing out.

Then, just two weeks later, on March 15, 2011, Westpac suffered another outage. None of its customers could log on to its online banking services. Online banking was down for an hour before services were restored.

May, 2011

On the morning of May 3, 2011, one of Westpac's data-center air conditioning units failed, and apparently there was not enough spare capacity to carry the data center. Servers had to be shut down as temperatures rose in the data center, causing a prolonged outage of the bank's online banking services and affecting all of its twelve-million customers. ATMs, credit/debit card use, and online banking services disappeared for several hours until they were restored by late morning. Online banking took additional time to restore.

February, 2012

On February 21, 2012, Westpac was once again hit by a severe outage of its online services. Customers could not get cash from ATMs and in some cases not even from the bank's branches. Services were down for several hours. The bank explained that it was in the process of upgrading its IT infrastructure and that the problem was due to a "home page" issue.

Commonwealth Bank

December, 2010

On December 14, 2010, Commonwealth Bank customers experienced intermittent outages in their online banking and ATM transactions. Commonwealth stated that the problems were due to an “overdue running of a computer file.” It was those customer accounts that required data from the late running file that had difficulty accessing cash through ATMs or transferring funds via online banking.

March, 2011

Again, Commonwealth Bank customers found on March 1, 2011, that they could not transfer funds or pay bills online. Retail POS machines were affected, and scheduled payments were delayed.

However, this time, cash from the bank’s ATMs was plentiful – too plentiful for some. The technical problem forced Commonwealth to disconnect the transaction switch connecting some of its core systems to its ATMs. Its ATMs could still dispense cash, logging the transactions locally in the ATM. Since there was no check of a customer’s account balance, customers found that they could withdraw any amount by simply visiting several of the bank’s ATMs. Word of this bonanza quickly spread, and there were reports of people queuing up at the bank’s ATMs to take advantage of the situation.

June, 2011

Commonwealth again lost its Internet banking on June 16, 2011, for most of the afternoon. Customers were unable to complete bill payments, transfer funds, and initiate international money orders. However, telephone banking remained operational, as did the bank’s mobile web site.

Australia and New Zealand Bank (ANZ)

June, 2010

On June 16, 2010, both Internet banking and telephone banking were interrupted due to a disk error.

Once again, ANZ left 1.8 million customers without banking services on June 22, 2010. EFTPOS and online banking were down for two hours. Only limited cash withdrawals could be made from the bank’s ATMs.

August, 2010

ANZ’s third failure in as many months occurred on August 24, 2010. Credit/debit cards could not be used at retail stores for a period of three hours. However, ATMs and the bank’s branches continued in operation.

May, 2011

Online services were unavailable for over an hour during the middle of the day. Restoration of services required the rebooting of servers.

Other Recent Banking Outages

China

In just one weekend in June, 2013, three Chinese banks suffered outages.

- A money transfer system at the Bank of China (BOC) failed, and customers could not transfer money.
- Customers of Bank of Nanjing could not transfer money.
- A nationwide outage of ATMs and point-of-sale (POS) devices occurred at China's biggest bank, the Industrial and Commercial Bank of China (ICBC).

All three banks said that the outages were due to technical problems.

Singapore

Singapore's largest banking network, comprising the DBS and POSB banks, lost most of its IT functions in July, 2010.³ Gone were its online banking, its ATMs, its payment-card services, and its back-office systems.

The problem was caused by an IBM employee who directed operations staff to use an outdated procedure to perform maintenance on a disk-storage system. The correct procedure had yet to be documented. IBM took full blame for the outage.

The bank compounded the problem by waiting too long to dust off its business continuity plan. By the time the bank convened its disaster recovery team, the crisis was almost over.

U.S. Banks

Bank of America

In February, 2013, customers of Bank of America were unable to access their online banking accounts, mobile payments systems, or even the bank's telephone call centers. Even Bank of America's employees were not able to see customer accounts for several hours. The bank attributed the outage to internal technical problems.

J.P. Morgan Chase

Millions of customers lost access to their online accounts for more than a day in September, 2010, due to a website server failure. It was reported that the problem was a software bug. It took most of the day for the bank to find and fix the problem.

The Financial-Transaction Network Infrastructure

The banking outages that are most noticeable are those that affect payment-card authorizations and ATMs. Most of the outages described above are of this nature. However, it should be noted that there are two systems involved in these exchanges. One is the banking IT infrastructure, which has proven to be anything but reliable. The other is the financial-transaction switches that interconnect the ATMs and POS terminals with the banks.

If one of these switches should go down, it would affect many banks. These switches have proven to be highly reliable. They rely on modern technology and generally are fully redundant. They are provided by such products as ACI's BASE24-eps, Opsol's OmniPayments, AJB's RTS. ElectraCard Services' electraSWITCH, FIS' Connex, and Lusion's Tango. The majority of these switches run on HP fault-tolerant NonStop (originally Tandem) servers, which accounts for their high availabilities.

³ Singapore Bank Downed by IBM Error, *Availability Digest*, August 2010.
http://www.availabilitydigest.com/public_articles/0508/singapore_bank_outage.pdf

What Is Going On?

Banks are saddled with decades-old legacy systems designed for batch processing. They are reluctant to replace complex systems built in the 1960s and 1970s that have been working fine for years. These systems are difficult to maintain since the developers have long since retired or died. Furthermore, they tend to be written in COBOL and PL1, and qualified programmers in these languages are becoming few and far between.

Compounding this challenge is that today's systems tend to be a patchwork of dated systems cobbled together as a result of mergers and acquisitions over recent years.

However, the banks have to meet the growing demand for customer-facing applications such as online banking and mobile services. They are building new systems to handle these tasks and are interfacing them to their legacy systems with middleware. Consequently, the systems are becoming more and more complex. At the same time, they are cutting IT staff and are outsourcing more and more of their IT support overseas.

Jean-Louis Bravard, former CIO of J.P. Morgan Chase has described the situation as follows:

"Retail banks rely on obsolete legacy IT surrounded by an ever-increasing plethora of newer systems to give consumers the impression that the banking systems are fit for purpose in our internet and smartphone world."

The CEO of RBS admits that for years, RBS had made little investment in their IT systems, preferring instead to struggle with their aging infrastructure. RBS is now making a massive investment to upgrade their systems to modern architectures.

Summary

Many banks are struggling with modernizing their systems. Some regulatory agencies have joined the fray.

Australia's finance industry regulator, the Australian Prudential Regulation Authority (APRA), has expressed its lack of tolerance for service outages of Australia's banks due to neglected legacy systems. It understands that it is necessary for the banks to continue to replace aging systems; but APRA will not accept outages due to institutions running outdated, unsupported operating systems, hardware, or software. Nor will it stand for outages caused by running critical systems with single points of failure or by losing critical skills. It warned against cutting IT budgets.

In today's high-technology world, there is an expectation of high availability and high resilience for critical services such as banking. Institutions today cannot cover up IT failures. There is no place to hide from Twitter and Facebook. However, banking customers for the next decade can expect regular outages of key banking systems. Banks will continue to struggle with system outages as they work to replace their aging, decades-old legacy banking systems.

Acknowledgements

In addition to the references previously made, material for this article was taken from the following sources:

[Outage at J.P. Morgan Cuts Web Access](#), *Wall Street Journal*; September 14, 2010.

[NatWest IT glitch continues to cause headaches for customers](#), *V3*; June 26, 2012.

[Bank of America Suffers Widespread Outages: Hacking Is Not Suspected](#), *NY Times*; February 1, 2013.

[China Bank outages trigger consumer cash worries](#), *Reuters*; June 25, 2013.

FCA investigation into RBS crash last year not complete as new IT crisis hits, *Computer Weekly*; December 6, 2013.

TSB, Lloyds, and Halifax customers complain as cards won't work, *Telegraph*; January 26, 2014.

Lloyds Banking Group outage caused by double server failure, *V3*; January 27, 2014.

HP server failure takes blame for Lloyds Banking Group's tech woes, *IT Pro*; January 27, 2014.

Lloyds blames HP server for crippling its ATMs, *Contractor UK*; January 27, 2014.

TSB chief uses Twitter to blame HP server for IT meltdown, *Finextra*; January 27, 2014.

Lloyds is the latest bank to experience major IT outage, *Computer Weekly*; January 27, 2014.

HP Server Blamed in ATM Outage at Lloyds Banking Group, *CruxialCIO*; January 30, 2014.

Lloyds Group probes server crash behind ATM, cash card outage, *The Register*; January 2014.