FLEXIBILITY, SCALABILITY, AND PERFORMANCE

THE CASE FOR RETHINKING PAYMENT SYSTEMS

An NCR white paper

NCR

INTRODUCTION

When the public thinks about banking, it is the daily interactions between cards and cash on one hand and ATMs and POS devices on the other. Early adopters mentally add their mobile phone or a contactless token to their personal view of banking. But the essentials of payments and transactions remain the same.

Should the supporting systems go down, or ATMs become unavailable, they therefore become the most public display of customer service failure. So it is not surprising that traditional payment systems, whose architecture is designed to meet demand for high availability, retain their position in the banking IT estate. The Non-Stop™ platform from HP, for example, originally deployed to support ATM-led demand in the 1980s, has largely lived up to its name. It remains a proven and demonstrably safe, reliable and robust platform for payments and transaction services.

The idea that the risks of replacement outweigh the benefits has become strongly engrained at many levels. Understandably, the counter-arguments have struggled to find a receptive audience among executives facing constrained budgets and narrow margins.

However, the risk-reward calculation is changing – and fast. The arguments for new ways of approaching hardware deployment have an increasing body of evidence behind them, as we discuss in this paper.

TABLE OF CONTENTS

1 CHANGING BUSINESS DRIVERS

2 CHANGING TECHNOLOGY DEMANDS

3 RESHAPING THE TECHNOLOGY ESTATE

4 EXAMPLES OF HIGH-AVAILABILITY DEPLOYMENTS

5 SOFTWARE FEATURES

6 MITIGATING MIGRATION RISK

7 CONCLUSION

1. CHANGING BUSINESS DRIVERS

Most of these platforms were first deployed at a time when high availability was the primary consideration. However, changes in the industry mean that availability is now just one of many requirements for the majority of financial institutions: flexibility, scalability, extensibility and cloud-compatibility are now key considerations.

Financial institutions are now operating in a market disrupted by new types of payments, new channels, and new competitors. In this diverse and complex payments environment, customer demand has changed: no longer satisfied with a monthly statement or a simple list of transactions, they want more information about each payment. That, in turn, requires data to be fed into and analysed in the transaction payload.

Crossover, convergence and convenience have become defining concepts. Account-holders do not see the world as banking systems and even business units do. For them different payment types are not separate channels but part of a seamless service. In the pure digital environment, boundaries between mobile banking, mobile payments and mobile commerce, are blurring. In the branch environment, sophisticated ATMs support comprehensive omni-channel services that erase the distinctions between physical and digital.

New ways of delivering both traditional and innovative services – including new ways of thinking about IT hardware – are therefore attracting attention.

2. CHANGING TECHNOLOGY DEMANDS

In this changing environment, customer-centric, needs-based payments have become a priority. Fortunately, as business drivers are making the argument for thinking again about IT, technological advances are making the alternatives increasingly attractive.

First of all, the reliability of industry-standard hardware has greatly improved since the 1980s. The NonStop and Stratus platforms were undeniably in a class of their own when it came to supporting ATMs 30 years ago, but there are now many viable alternatives available.

What's more, the relative decrease in the price of hardware has reduced the investment risk significantly. We are past the point in the business cycle where organisations can simply 'throw' resources at new systems. But over capacity is no longer prohibitively expensive, and is much less a risk than under capacity.

Many of today's technologies, such as cloud, are not available with older operating systems and languages giving another pressure to adopt open standard operating environments. Once using these operating systems organisations can take advantage of the many tools, such as open source components, that are available to enhance productivity giving added benefit from making the change.

Changing standards are also demanding more of technology. Significant advances around message structure and formats, including the new ISO 20022 standard, replace a number of previous standards regarding card and electronic payments.

ISO 20022 is based on Extensible Mark-up Language (XML), to aid the exchange of intra-bank messages, as well as messages between a bank and its customers - with the aim of making payment processing more efficient for all market participants. Payment systems installed before ISO 20022 was even dreamed of, are not designed to generate and insert the new message formats into their workflow.

ISO 20022 is a significant change agent. But it also reflects a more general direction of travel towards object-oriented architecture, open standards, and the need to integrate distributed software components. Wider availability of Linux/ Unix systems and open databases, plus the use of APIs to integrate innovative solutions from independent FinTech firms are all indicators of where technology is headed.

Perhaps the biggest change of all is the acceptance of cloud deployments. While technologists have been talking up both private and public cloud as the future for compute-intensive systems – including payments – and frictionless workflow, reality has finally caught up with commentary. The advantages of cloud, the cost-effective scalability and flexibility, are achievable primarily through open systems and open platforms.

3. RESHAPING THE TECHNOLOGY ESTATE

Fortunately, financial institutions are not alone in demanding fault-tolerant deployment of mission-critical systems on commodity or standard hardware. Nor is retail banking the only industry with such stringent demands for extensibility, scalability, and 'five 9s availability'. Consequently, vendors have developed systems that can give financial institutions more choice when it comes to uncompromising, cost-effective performance, openness, flexibility and cloud-compatibility.

In modern technical topology, resilience and extensibility are achieved through three key elements:

- **Application clustering** to enable distributed processing and horizontal scalability
- **Database clustering** with solutions such as Oracle RAC
- **Replication** through technologies such as Oracle Data Guard and Golden Gate

The eventual configuration depends on the particular requirements and resources of the individual financial institution, and can substantially reduce both the operational risks of technology migration, and the business risks of being confined to non-competitive hardware.

4. EXAMPLES OF HIGH-AVAILABILITY DEPLOYMENTS

AUTHENTIC HIGH-AVAILABILITY DEPLOYMENT (ORACLE)

There are a number of options for achieving high availability in payment systems, as we show here.

- **Figure 1** shows a high-availability deployment of Authentic, NCR's transaction services hub, on Oracle servers. Here, Authentic 'nodes' are installed in two separate locations. Each consists of one or more database servers connected in an RAC cluster, plus a horizontally distributed cluster of application servers on which Authentic is executed. These servers can be physical or virtual machines from any vendor.

  Oracle Golden Gate technology is used to replicate data between the two nodes' database servers, while an external communications switch or intelligent router ensures the optimal direction of traffic to one or both nodes, switching between them as necessary. The switch distributes connectivity and if it detects a fail, will check the fault while continuing to direct traffic to the remaining servers.

In this model, Authentic can be deployed on a primary node, with the secondary node providing fail-over and extra capacity when traffic volume is high. Alternatively, Authentic, can be deployed in two active instances - depending on the nodes' proximity and ability to share data at low latency. Because the software is replicated across the two nodes, if one goes down or is operating at sub-optimal levels, the other can pick up the traffic with no loss of service.

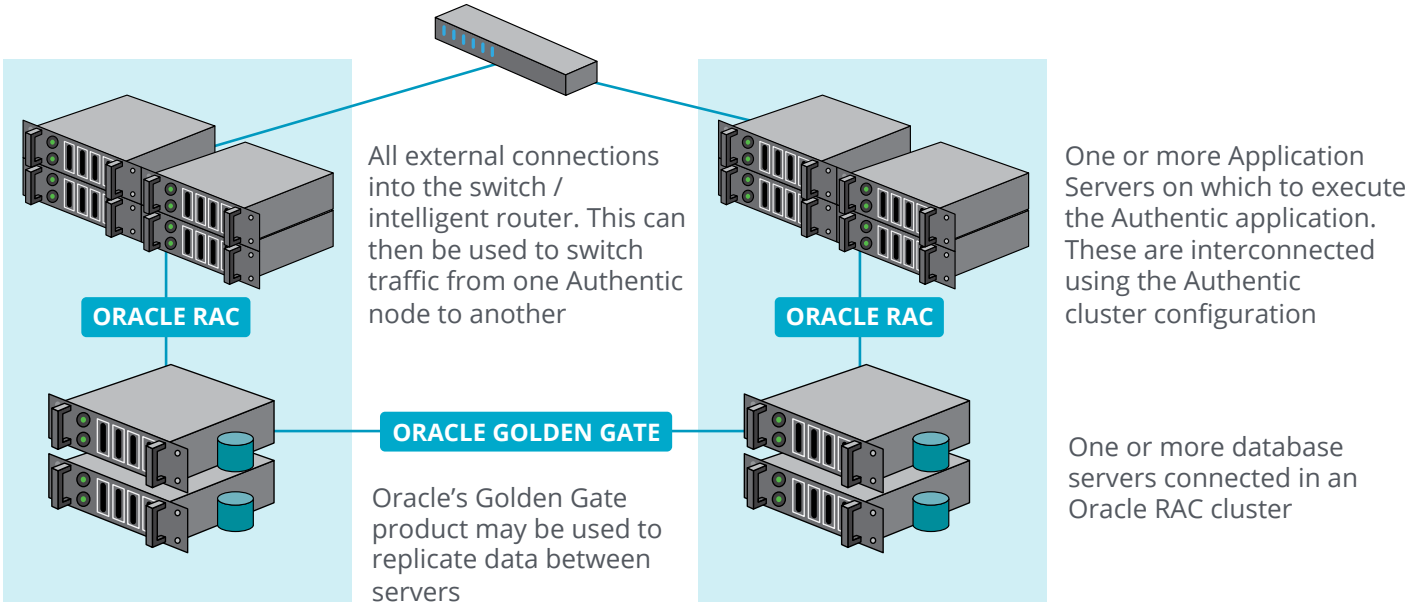


Figure 1

AUTHENTIC HIGH-AVAILABILITY DEPLOYMENT (ORACLE - FSFO)

- In **figure 2**, Authentic is deployed on an Oracle fast-start failover (FSFO) model. Here too database and application server clusters are deployed in two separate nodes, but it distinguishes between the primary node and a standby node, which is used only for failover.

  The network storage in the Data Guard technology provides replication and failover capabilities, and protects a database if the production site is lost. The external switch directs traffic, as before, but here the FSFO observer is responsible for initiating an FSFO failover and automatically reinstating a failed primary node as the new standby. This model is not limited to two sites or nodes. If necessary, financial institutions can deploy Authentic over multiple instances.

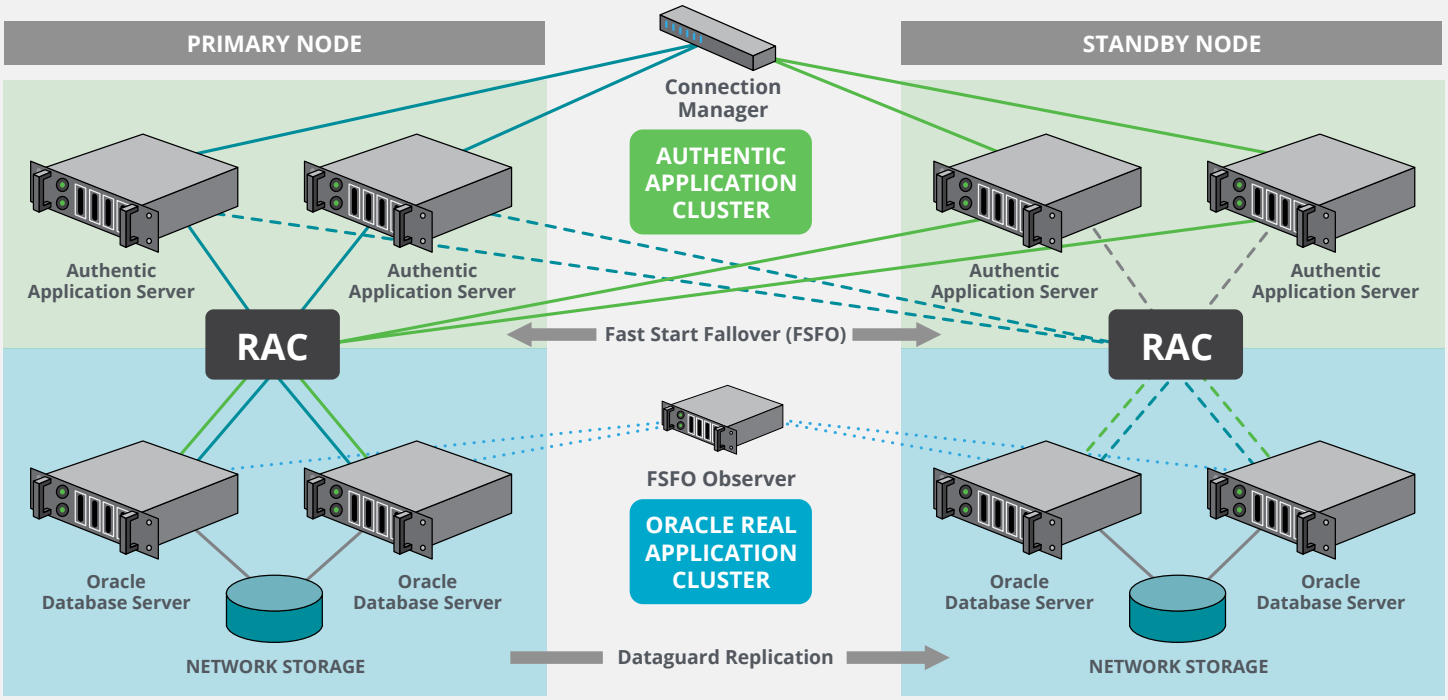


Figure 2

AUTHENTIC HIGH-AVAILABILITY DEPLOYMENT (SQL SERVER)

- **Figure 3** shows deployment on MS SQL servers. In this model, only one database server is required in each node with transaction replication providing near real-time updates to both nodes. One or more application servers can be used, and connected to the database server by standard JDBC connectivity. This model operates on a similar basis to the Oracle configuration in figure 1.
- Finally, there is the Stratus option, which can be deployed in the configurations seen in figures 1 and 3: two nodes of application and database clusters, connected with an external switch for directing traffic. The inherently fault-tolerant hardware provides the same resilience seen in these multiple-server configurations with only a single database server and a single application server in each node.

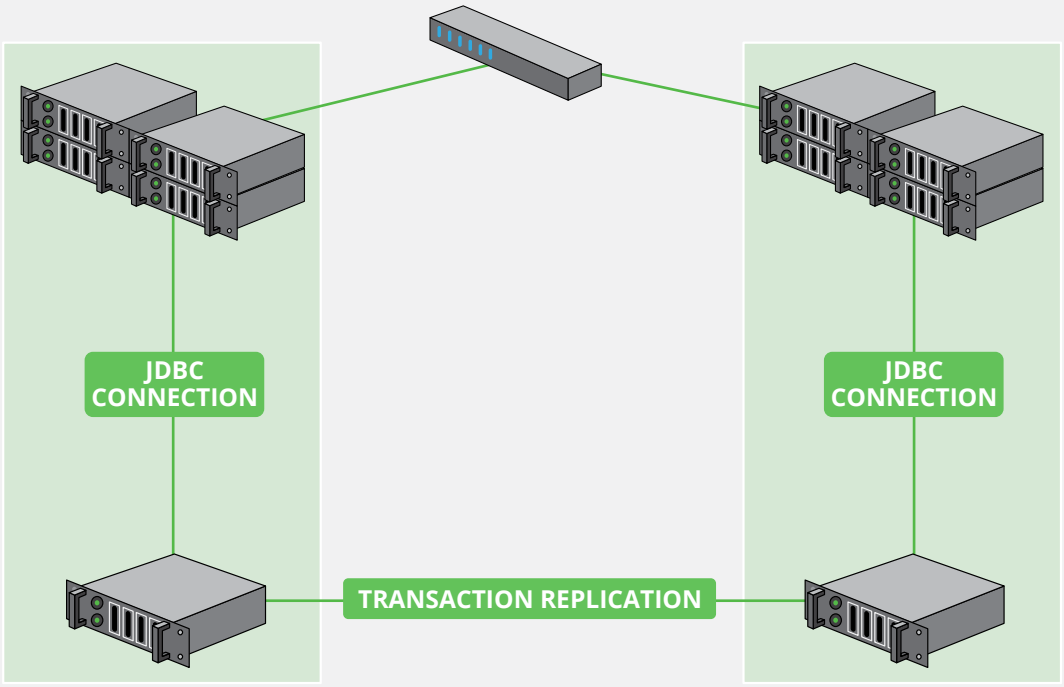


Figure 3

AUTHENTIC GLOBAL DEPLOYMENT (STRATUS ATR)

However, the Stratus Advanced Transaction Router (ATR) model of **figure 4** is a fundamentally different configuration, which associates services with connections. For example, should a server go down in Asia, the ATR looks for those services somewhere else around the world and redirects the transactions to the relevant node. The ATR model therefore allows for substantial geographical spread of server locations without losing performance in any.

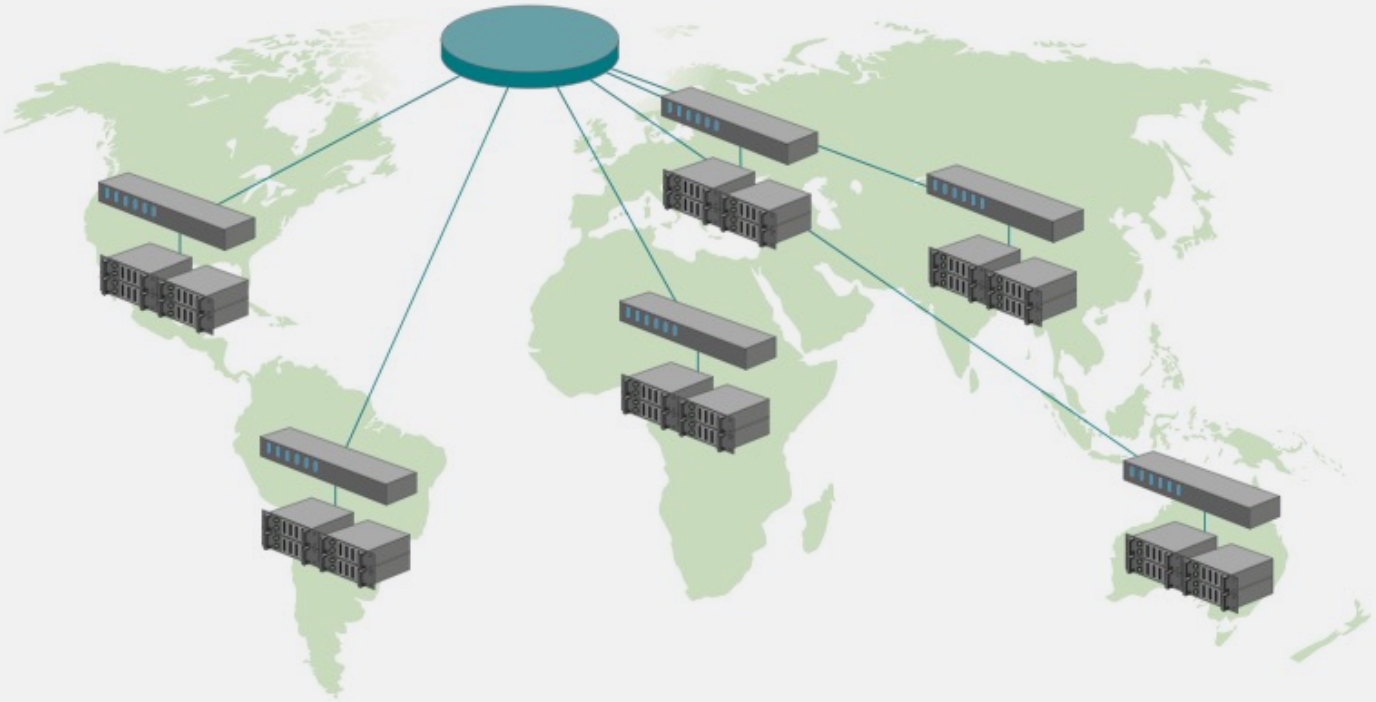


Figure 4

5. SOFTWARE FEATURES

The advantage of the distributed systems described above is that they no longer lock users into proprietary hardware and operating systems with accompanying maintenance costs. They are vendor-neutral, use standard components, and rely on common IT knowledge and skills, including Java and object-oriented design.

The success of these models also depends on deploying the right payments solution. For example, Authentic supports multiple databases and ensures that banks can still choose their preferred operating system and database in accordance with their own priorities.

Authentic is written totally in Java and its framework is built on open, industry-standard technologies and open communications standards. It also has self-monitoring capabilities that work in tandem with the redirection capabilities of the hardware to ensure optimum deployment across multiple sites. It is benchmarked to 10,000 TPS, scales without bottlenecks, is itself resilient both horizontally and vertically, and achieves close to 100 per cent availability.

6. MITIGATING MIGRATION RISK

As outlined previously, the right technology can reduce risks but migration is often still a major concern. There are five main steps to consider, which should be carried out in discrete phases to reduce risk. They are often tackled in the following sequence:

1. Establish external connections to interbank systems, such as card schemes or card networks
2. Establish connections to internal systems, such as core banking, card management or fraud detection systems
3. Establish connections to outsourced services, such as credit-card services
4. Migrate authentication and authorisation services
5. Migrate driving the ATM, POS and other devices

The actual order, timing, and sequencing will vary according to the connections and systems, resources available, and the preferences and priorities of the individual organisation. For example, an NCR customer in Europe found that the individual steps were further split into separate stages: steps 1-4 were completed in the first stage, while step 5 was part of the second stage of migration.

In all cases, common sense prevails. The work needed to add new device types or new connections to existing devices can be slotted into the above sequence, depending on how high a priority the new element is. For example, adding new devices forms part of step 5, while continuity of service is maintained by leaving older devices in the existing system until new ones are thoroughly tested and retiring devices are decommissioned. Alternatively, it may make sense to add new devices earlier in the process.

Financial institutions also need to keep their individual business case front of mind, as there could be a specific need that changes the typical sequence. The drive towards EMV adoption is one example. An NCR customer in Asia reversed the order given above and completed step 5 before embarking on steps 1-4 because it urgently needed to add EMV-card recognition to its ATM network. Although device driving (number 5 above) is almost always the final step, in this case it was an urgent priority and was carried out first.

Regardless of the sequence of activity, however, planning a migration will always include a temporary link between current systems and their replacements. It must also cover procedural items such as: where settlement data is obtained; how a migration step can be reversed out; and, where relevant, migration of card and account data.

Given the above, no two migrations will be identical. To develop a process that works best for their own circumstances, financial institutions should ask and answer the following questions:

1. What is the business imperative that is driving this migration? Is this so urgent that it must be handled first?

2. Will everything in the current system move to the new one? And are there functionalities that become obsolete in the face of strategic business changes?

3. What internal or external factors will affect the required functionality and the system?

    a. Will industry mandates for PCI compliance, EMV standards or others need to be incorporated at some point?

    b. Is the financial institution planning a new business model, platform, service, or new markets, which need to be considered?

4. How quickly does the migration need to take place?

    a. Are there business or technology imperatives that must be met within a given timeframe?

    b. What are the costs of running two systems in parallel during the migration, and how do these affect proposed timetables?

    c. Will a slower pace negatively affect the momentum needed to make the migration happen?

Banks therefore face a number of options during the migration process. But the resources and processes can be established to accelerate deployment, shorten time to success, and minimise the potential risks.

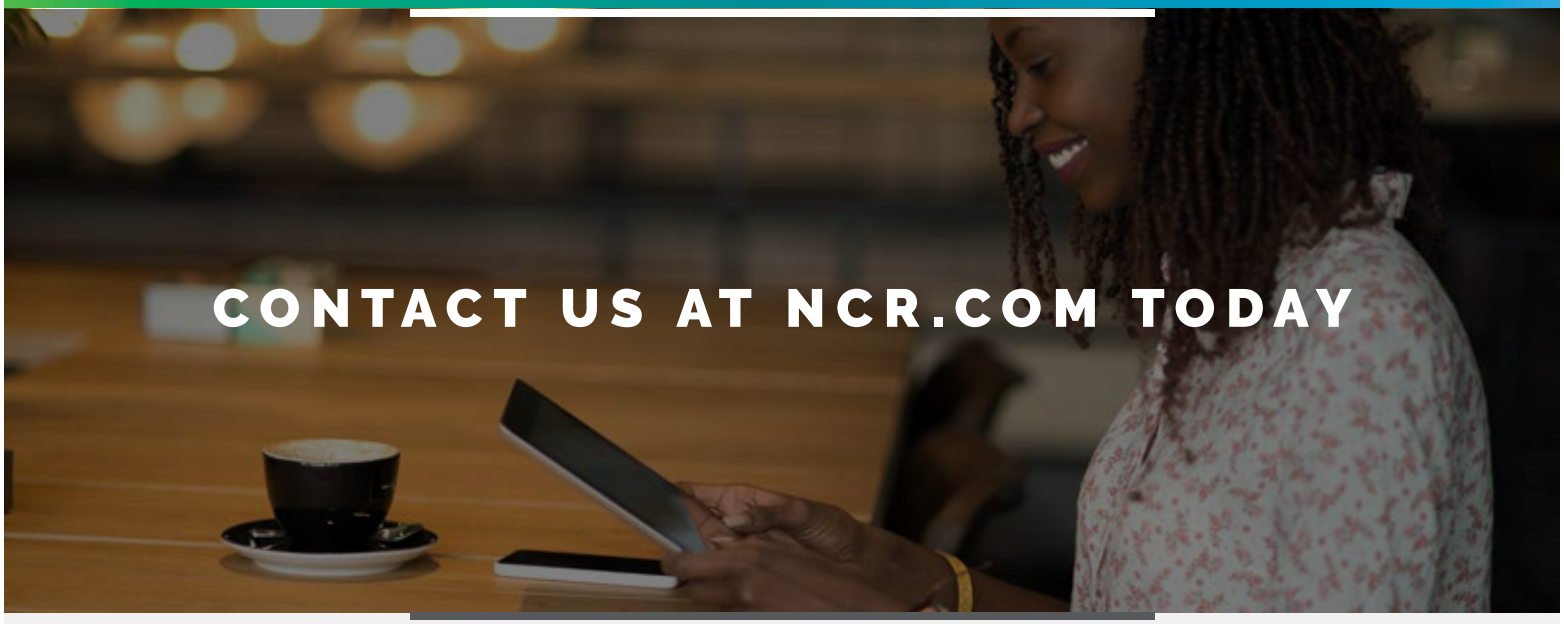
7. CONCLUSION

Many financial systems have reached the limit of what can be achieved by further customisations of existing platforms. In some cases, further adaptation may act as a barrier to the extensibility, flexibility, and performance required in today's markets. But the agile services that market disruptors build on more responsive and cheaper-to-run technology, and the utility-based, distributed cloud deployments seen in other business sectors, need not be out of reach for financial institutions.

To make sure that IT infrastructure is still delivering advantages, those financial institutions should:

- Develop an 'ideal state' for a technology-enabled payments and transactions service that works in a fast-changing business environment
- Identify where and how current platforms support this vision, and where they may hinder it
- Take a new look at how the right performance can be delivered with today's hardware
- Select a software platform that enables the promises of the hardware to be realised – and vice versa
- Consider a phased, agile migration rather than a big-bang deployment

Last, but not least, financial institutions should make sure they are clear about whether the risks of maintaining the status quo outweigh the risks of change.



CONTACT US AT NCR.COM TODAY

WHY NCR?

NCR Corporation (NYSE: NCR) is the global leader in consumer transaction technologies, turning everyday interactions with businesses into exceptional experiences. With its software, hardware, and portfolio of services, NCR enables more than 485 million transactions daily across retail, financial, travel, hospitality, telecom and technology, and small business. NCR solutions run the everyday transactions that make your life easier.

Authentic is an intelligent transaction-processing platform designed for today's fast-changing payments business. It has become the payments engine of choice for issuers, acquirers, payment service providers, ISOs and merchants around the world. Part of NCR's CxBanking software suite, Authentic unlocks amazing consumer experiences across physical and digital banking channels.

NCR is headquartered in Duluth, Georgia with approximately 29,000 employees and does business in 180 countries. NCR is a trademark of NCR Corporation in the United States and other countries.