

## Letter from the CEO



Welcome to the summer issue of Level Four news. In this issue, we report on the findings of our recent survey which has shown that combating network downtime continues to top banks' list of ATM priorities for the second year running and looks set to do so through 2010.

Also on the agenda is ATM testing. This newsletter will discuss best practice testing strategy with a focus on developing and implementing a holistic methodology for integrated testing. Finally, we will discuss the ATM landscape in the Middle East with a focus on the recent move to EMV adoption.

Ian Kerr, CEO, Level Four  
*Please email your comments to [enquiries@levelfour.com](mailto:enquiries@levelfour.com)*

## Middle East focus



Banks in the Middle East have been, so far, less affected by fraud when compared with Europe as strict national laws have acted as efficient deterrents. However, in recent years, the oil-rich states have seen an influx of people arriving from abroad, either for business or leisure; with these, fraudulent transactions have increased too. Although Gulf banks have enjoyed a privileged position for a long time, since 2008 we have seen a marked change with a dramatic rise in magnetic card fraud. The issue seems to have escalated further towards the end of 2008 and in the recent

months with reports of an increased number of ATMs plagued by transactions executed with unauthentic cards. Compliance with the Europay MasterCard Visa (EMV) standards is the key to a safer environment, but how is this going to affect the ATM channel? We analyse the impact of this change in the lead article of this issue over the next pages.

Issa Keshek, Regional Director, Middle East, Level Four

## Reducing downtime remains top ATM priority for banks



Following a delegate survey at ATMIA European ATMs show, Level Four have found that combating network downtime continues to top banks' list of ATM priorities for the next 12-18 months. The issue also topped the list in Level Four's survey at the same event in April 2008, highlighting the ongoing challenge banks face to maintain their ATMs. By reducing downtime, banks can maximise the quality of service, brand value and revenue potential of this frequent customer touchpoint.

The majority of respondents (61%) said that tighter control of budgets was the biggest change in priorities since the onset of the financial crisis. Banks must now balance the need to maximise their budgets against the requirement for a complete end-to-end testing strategy that tackles the true complexity of the ATM.

This focus on addressing the fundamentals of the ATM is reflected in a comparison of the results year-on-year, which shows a marked shift in where banks are placing their efforts. Rolling out new services at the ATM was the second most cited priority last year but appeared bottom of the list this year. Instead, integrating the ATM channel with other banking channels moved to second place.

## What's inside

The New Middle Eastern ATM Challenge.....	2/3
Upcoming Events.....	3
Best Practice in ATM Testing .....	4

## The New Middle Eastern ATM Challenge

One of the causes of the recent growth in fraud in the Middle East region is the use of magnetic stripe cards as opposed to Chip and PIN. To date, the roll out of Europay MasterCard Visa standards (EMV) in Middle Eastern states has been spearheaded by Saudi Arabia and is being either seriously discussed or being adopted elsewhere in the region. However, roll-out has been patchy and even non-existent in some countries. When compared to Europe, the oil rich states' card security is relatively easy to crack and consequently the region is becoming increasingly attractive to fraudsters. In light of this, banks must now consider how they can restore the level of security they have become accustomed to for so long.

So far, there has been a mixed response to the situation, possibly born out of confusion around how best to address the issue.



In particular, several banks have taken drastic, yet short-term, measures to contain the crisis. Some institutions lowered ATM withdrawal limits while others prevented customers from accessing their accounts from abroad. As a result, customers are growing increasingly concerned about the safety of their savings.

What is clear is that banks must ensure their ATM networks are secure in the long term. With the UK leading the way, with 92 per cent of the country's total cards EMV-enabled by August 2008, other markets are strengthening their protection against fraud through EMV. Traditional magnetic cards will need to be replaced with the more advanced EMV-compliant Chip and PIN cards in the Middle East too. The effectiveness of EMV-compliant cards is clearly demonstrated by the experience of more mature markets. Referring back to the UK example, the introduction of the EMV standard in 2004 reduced card fraud by 25% within two years. This resulted in a marked difference in customer attitudes towards banks as fraud levels at the ATM declined following the roll out.

By being on a later wave of EMV roll-out, the Middle East can benefit from the lessons learnt from earlier implementations. As previously mentioned, the UK has experienced significant reductions in fraud following roll out of Chip and PIN. More recently, Canada has implemented an EMV migration timeline and appears to be on track to complete EMV migration in 2010 whilst Latin America has committed to EMV and has implemented a pan-regional liability shift for issuers who fail to migrate. As the world gradually migrates to EMV, it is important that the Middle East learns from these models and implements a successful EMV strategy to ensure that the region does not get left behind.

Decisive action towards EMV now appears to be on the cards as the UAE central bank has recently stated that it will adopt Chip and PIN technology on debit cards. While no deadline for migration has yet been set, this is a clear message to financial institutions within the region that investment in EMV technology is a priority. The UAE's statement follows a review of the UAESWITCH cash machine network which links all the country's ATM networks, enabling customers to use any ATM in the UAE and the Gulf countries. This call to action is a significant step towards full regional migration. Similar initiatives are being considered in other countries around the Gulf.

In Europe, EMV was rolled out with governmental support. Governments introduced the concept of 'liability shift', so that responsibility for fraud losses falls on the non-EMV-compliant party. This might be needed in the Middle East in order to provide an incentive for compliance among banks and retailers and ensure migration occurs sooner rather than later. While migration to EMV has begun due to the cost of fraud, it appears that a mandated timeline should be the next step in the Middle East region in order to secure a full EMV roll-out. With EMV now firmly on the agenda, it is perhaps only a matter of time before this is introduced.



While costly to implement, EMV Chip and PIN provides significant benefits to banks and retailers. Fraudsters are deterred from copying the chip since it is expensive, time intensive and requires resources out of proportion to the likely reward. As the chip is a computer device it can interact with the accepting device, such as an ATM or payment terminal, and process data.

From a technology standpoint, EMV mandates are more complex than the traditional approach. With the use of magnetic stripe cards, Gulf banks have seen very little change in their ATM network testing routines and certification requirements. In contrast, EMV standards change more frequently and therefore require more rigorous and frequent testing. The latter is around ten times more labour intensive than traditional testing procedures, which could lead to considerable productivity issues. While there are clearly some investments to be made in order to comply with EMV mandates, the risk of fraud

means that banks are no longer in the position to procrastinate on the issue. Therefore, to navigate a smooth path to compliance, banks need to ensure they have the expertise, resources and technology to make the right decisions quickly during the migration process and the ongoing maintenance of their ATMs networks.

With key industry players such as Visa and MasterCard discussing the possibility of setting penalties for non-compliant institutions, banks must act quickly. Once the migration is complete, banks must ensure any faults are swiftly addressed and that uptime across their ATMs networks is achieved. To address this, they must put in place measures to automate the ongoing testing and monitoring of their networks. This will enable banks to benefit from a tangible return on investment as automated procedures are more time and cost-effective than a manual approach.

The ATM remains a bank's most frequent customer touchpoint. With the risk of fraud and the impact of regulatory compliance issues, banks must ensure they do not overlook this critical channel. While magnetic stripe card fraud is, without any doubt, a big challenge for banks, EMV mandates offer to financial institutions the opportunity to demonstrate to customers a strong approach to security and, as such, to re-establish their trust.



## Upcoming events



### Retail Delivery 2009, Boston, MA 3rd – 5th November 2009

BAI Retail Delivery began as an ATM conference with 200 attendees and is now the largest retail financial services event in the world, bringing together nearly 6,000 participants annually. Interact with and learn from more than 250 solutions providers from around the world in the BAI Retail Delivery Expo. Many of the most valuable education and networking opportunities are right in the expo this year, they include:

- General Session presentations
- BAI Retail Delivery Community discussion groups organized by areas of interest
- Solutions theatres
- A far-reaching industry whitepaper library
- A full line-up of live podcast interviews unveiling the latest industry research findings

## Best Practice in ATM Testing

### What you need to test...

The first step towards an effective testing strategy is to understand the full scope of what is to be tested. At its most basic level, testing involves the testing of the ATM application against the host system. When it comes to deploying automation tools, the business benefits are only realised if a bank is able to meet the requirements from a single system. Typically, end-to-end testing must encompass the ATM, relevant card types, the host that drives the ATM, as well as the external switching and authorisation networks that are involved in the transaction chain.

There are numerous points along this chain that could fail and that need isolating in order to resolve an issue. Once this is appreciated and looked at as a whole, an effective testing strategy can be developed. The key different areas impacting the overall test strategy can be broken down as follows:

**Operating system** — Most banks have now migrated to use the Windows operating system, with XP the clear current favourite. While Windows has advantages over OS/2, there are risks introduced by security updates and bug fixes issued by Microsoft, which occur on a very frequent basis. A change to the operating system requires a complete retest of the system each time a change occurs. However, most banks are not in a position to spend the time and money on a full system regression test and will take a risk-based view with their supplier on what, if any, testing is carried out. This is a suboptimal situation based on the reality of the fact that updates occur frequently, but a regression test cycle would take potentially several man-months using a manual testing regime. Clearly this problem could be eliminated if a comprehensive test automation strategy was employed.

**Other applications** — In today's multi-vendor environment third parties often install additional software on to the ATM hardware. A typical ATM application stack may include the Windows operating system, the ATM application, a monitoring agent, anti-virus and firewall software, software distribution client etc. With the challenge of misaligned release cycles for each of these applications, banks need to be able to conduct frequent and rapid re-testing of the network if they are to avoid introducing unnecessary risk into their systems.

**New devices** — New XFS devices such as those to support cheque, coin and note deposits are being introduced into ATM networks, making systems increasingly complex. As the scale of the overall functionality increases so does the potential for device and software errors in processing these critical transactions, and the test requirements increase significantly.

**Card testing** — With the widespread adoption of smart card technology, banks need to test and certify each card type in their ATM systems to ensure the correct transaction routing and service presentation. To test a typical EMV card requires hundreds of



different test scripts, which, when multiplied by the number of different card types, results in an extensive testing universe.

**Card scheme certification testing** — One of the larger overheads involved in testing systems is planning and executing the certification of the ATM system against the host systems of the major card schemes, both domestic and international. The increased use of card scheme simulators, plus an effective method of automation of the ATM transactions, can simplify the certification process for all parties and reduce third-party dependencies.

**Host message testing** — Host message testing encompasses the link between the bank and the terminal driving system routing and authorising the financial messages. As outlined above, there are several points along the transmission of messages within the ATM network that must be isolated and tested accordingly.

**To download your copy of Level Four's "Best Practice in ATM Testing" guide, please visit [www.levelfour.com](http://www.levelfour.com)**