# Chip migration in the USA: How near is the **end** of **Skimming**?


Von Lachlan Gunn

**Aus Sicht europäischer Kartenemittenten sind die USA einer der gefährlichsten Orte weltweit, so Lachlan Gunn – nach den Ankündigungen von Visa und Mastercard mehr denn je. Denn die Zeitpläne für die Umstellung auf den Chip sind weit gefasst, und bis das Zeitfenster sich schließt, werden Kriminelle versuchen, aus den bestehenden Sicherheitslücken so viel Profit wie möglich herauszuholen. Dass die Visa-Pläne Geldautomaten nicht mit einbeziehen, kommt erschwerend hinzu. Als Fazit bleibt: Die bisherigen Pläne sind ein Schritt in die richtige Richtung. An Sicherheitsstrategien wie Geo-Blocking führt aber auch weiterhin kaum ein Weg vorbei. Red.**

On 9th August 2011 Visa announced plans to accelerate the migration to EMV (Chip and PIN) contact and contactless chip technology in the United States. These plans, which will encourage the U.S. adoption of dynamic chip authentication technology, enable U.S. merchants and processors to start to take action, confident that they are following a clear roadmap. The Visa plans include the following three initiatives:

Expand the Technology Innovation Program (TIP) to Merchants in the U.S. effective 1st October 2012. To qualify, terminals must be enabled to support both contact and contactless chip acceptance, including mobile contactless payments based on NFC technology.

- Build Processing Infrastructure for Chip Acceptance. By 1st April 2013 Visa will require U.S. acquirer processors and sub-processor service providers to be able to support merchant acceptance of chip transactions.

- Establish a Counterfeit Fraud Liability Shift. Effective 1st October 2015 Visa intends to institute a U.S. liability shift for domestic and cross-border counterfeit card-present point-of-sale (POS) transactions. Fuel-selling merchants will have an additional two years, until 1st October 2017, before a liability shift takes effect for transactions generated from automated fuel dispensers. With the liability shift, if a contact chip card is presented to a merchant that has not adopted contact chip terminals, liability for counterfeit fraud may shift to the merchant's acquirer. The U.S. is the only country in the world that has not committed to either a domestic or cross-border liability shift associated with chip payments.

**Lachlan Gunn, Director and Coordinator, European ATM Security Team, Edinburgh.**

### Mastercard follows with Maestro ATM transactions

Then on 1st September 2011, Mastercard followed with an announcement that it will extend its existing EMV liability shift programme for inter-regional Maestro ATM transactions, as part of an effort to align technology efforts to prevent and manage fraud.

The liability shift will cover both the United States and Asia-Pacific regions and will be effective on 19th April 2013, with the exception of Australia and New Zealand, where the liability shift will become effective on 31st December 2015. South Asia (Bangladesh, Bhutan, India, Maldives, Nepal and Sri Lanka) will continue to be excluded from the inter-regional ATM EMV liability shift programme. It should be noted that liability shift already applies for Europe, Canada and the Middle East and

Africa and will be completed for Latin America by end of October 2012.

In an interview with the Credit Union Times Mastercard Worldwide spokesperson Seth Eisen clarified that "U.S.-based ATMs will have to take EMV cards as of April 19, 2013."

What does this mean for European card issuers battling against card fraud? Europe began to migrate towards EMV nearly a decade ago and, over the past few years has seen an impressive overall drop in skimming related losses, although the situation can and does fluctuate from country to country, with some countries still fighting increasing losses.

EAST recently published a chart which shows the impact on ATM related skimming losses of the roll-out of EMV at European ATMs. Domestic issuer losses (losses committed inside national borders by criminals using stolen card details) fell by 63 percent when comparing figures for the first six months of 2006, with those of the second six months of 2010.

Even when nearly all ATMs (97 percent+) are fully EMV compliant in EU-Sepa countries, fraudulent withdrawals can still take place because of the usage of "mag stripe only" cards from non EMV card issuers, or because EMV card issuers authorize 'mag stripe fall back' transactions.

A big spike in international losses (losses committed outside national borders by criminals using stolen card details) occurred in 2007 when such losses increased by 201 percent from the previous reporting period. In such cases counterfeit EU payment cards are used to make cash withdrawals in countries where all or some of the ATMs are not yet EMV compliant. As long as mag stripes are present on EMV cards, the cards are vulnerable to skimming. International losses during the second half of 2010 were down by 64 percent from the highpoint in 2007.

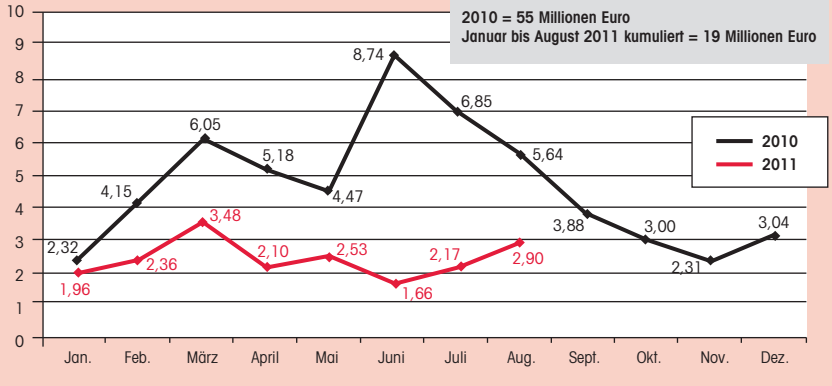
In addition to the impact of the EMV roll out, this fall in international losses can also be attributed to the effectiveness of anti-skimming devices, where they have been deployed, to improvements in the detection and monitoring of fraudulent transactions, and to regional card blocking for "card present" transactions.

**80 percent of fraud against EU payment cards is committed in the United States**

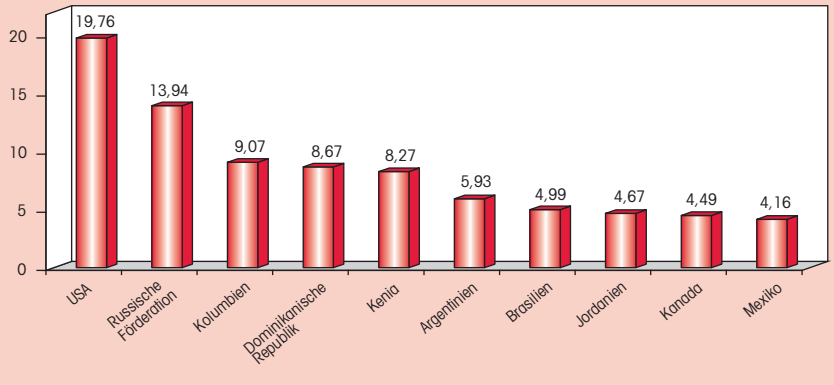
Also of concern to European card issuers, however, is the hacking of mag stripe data. This hacked data can be used to create counterfeit payment cards, although the fraudsters do not have PIN information – a difference when compared to counterfeit cards made from skimmed data. In the U.S. a PIN is not currently required in the face-to-face environment, and therefore counterfeit cards made from hacked data can be used to make fraudulent signature-based and key entry transactions.

This brings us back to the U.S. and the recent announcements: Many EU countries are now reporting that losses in the U.S. make up the largest percentage of international losses. This is in line with the latest Organised Crime Threat Assessment published by Europol which states that around 80 percent of non-EU fraud against EU payment cards is committed in the United States. Up until the Visa announcement no plans had been published for EMV migration in the U.S. In

**Bruttoschaden mit Dubletten in Millionen Euro nach Eingangsdatum**




**Einsatzländer für Kartenfälschungen Januar bis Juni 2011** (in Prozent)




Quelle: Euro Kartensysteme

this context, the announcements from both Visa and MasterCard are to be applauded.

**Three key concerns remain for European issuers**

But three key concerns remain for European card issuers.

- While the Mastercard announcement means that member bank ATMs must become EMV compliant, ATMs are not covered by the Visa plans.

- Signature-based mag stripe and key entry transactions will still be allowed.

- The timescale for the Visa announcement – 1st October 2015 is still a long way off.

Firstly Visa's announcement only covers merchants. EMV implementation at merchant terminals will reduce the risk of skimming at such terminals, and the proposed liability shift will be a good incentive for acquirers to take action. This may reduce skimming incidents at such terminals, and may also make the fraudulent use of skimmed EMV cards more difficult. Unfortunately the European experience indicates that ATMs are the preferred channel for financial fraudsters to obtain cash from counterfeit cards. Mastercard has flagged the route towards ATM EMV compliance and Visa must now follow it.

**Geo-Blocking works**

Until the entire U.S. ATM estate becomes EMV compliant, European card issuers will still continue to suffer counterfeit losses there, unless some form of geo-blocking is implemented. Banks in Belgium, Germany and Norway have already introduced geo-blocking for payment cards; in order to use their cards outside Europe card holders have to contact their banks in advance of any trip. It works!

Another solution would be Chip only debit cards for use within Sepa or at any EMV compliant terminal worldwide. Such cards would need a visible mag stripe to allow the card to be inserted into motorised card readers, but it would not contain customer data.

Secondly Visa states that globally they will: continue to support a range of cardholder verification methods including signature, PIN and no-signature for low-value, low-risk transactions. In the longer term, it is expected that the use of static verification methods such as signature and PIN will be reduced or eliminated entirely as new and dynamic forms of cardholder verification are implemented. This is too vague and does not seek to eradicate signature based key entry or mag stripe transactions by a defined date. Once again geo-blocking can help to minimise this risk for European card issuers in areas without a liability shift, where signature-based magnetic stripe or key entry transactions are the only option for cardholders.

**Losses are likely to spike**

Lastly, while the Mastercard deadline of 19th April 2013 is probably as tight as is feasible, the Visa deadline of 1st October 2015 is still a long way off. If the U.S. follows a similar pattern to Europe, losses are likely to spike as criminals become aware that their window of opportunity is drawing to a close.

This happened for European ATM related skimming losses in 2007. As life becomes more difficult for them in Europe and other EMV compliant areas, organised criminals are likely to continue to maximise their opportunities in the U.S. market; and it won't just be a magnet for fraudsters with European cards!

By 2015 China Union Pay has stated that all Chinese cards will be EMV cards. Counterfeits of these cards may also be taken to the U.S. for cash withdrawal purposes.

**The plans announced do not go far enough**

In summary, the plans announced by both Visa and Mastercard are welcomed by EAST members as an important step forward for the U.S. market, but as they stand they do not go far enough.

How near is the end for skimming? As long as payment cards have mag stripes that can be copied, skimming will continue. The long term goal must be for the whole world to move towards EMV contact and contactless technology. Card issuers can, and will, continue to find ways to mitigate skimming risk, such as the introduction of geo blocking, but only the removal of mag stripes will finally remove the skimming problem.

From a European card issuer's perspective, the U.S. is now one of the riskiest places on the planet; from a criminal perspective it must surely be now one of the most lucrative places to operate. What will continue to drive change in the U.S.? Apart from significantly increasing domestic card fraud related losses, the other key driver will be an increased dissatisfaction among U.S. cardholders, unable to use their mag stripe only cards at an increasing number of chip only payment terminals across the world. In August 2011 Citi announced the launch of the Citi Corporate Chip and PIN card, an EMV compliant smart card designed for U.S. corporate cardholders travelling abroad, and a claimed first by any U.S. commercial card issuer.

It seems that U.S. card issuers are caught in a pincer between the rising cost of fraud, and rising cardholder dissatisfaction. European card issuers can only hope that this will drive further and faster progress along the paths that both Mastercard and Visa have now set out for the U.S. market.