EPC Newsletter Issue 7 - July 2010

SEPA FOR CARDS

EPC Card Fraud Prevention Forum

Agreement on new measures to fight card fraud

19.07.10 BY CÉDRIC SARAZIN

SUMMARY

In June 2010, more than 100 delegates convened in Paris for the two-day EPC Card Fraud Prevention Forum to debate the current trends in card fraud, identify appropriate countermeasures and assess necessary investments in the field of card security. The EPC Forum was sponsored by the Féderation Bancaire Française (FBF) and the Groupement Cartes Bancaires (CB). Thirty speakers from twelve countries and nine international organisations, including the European Commission and the European Central Bank (ECB), carried out an exhaustive review of current challenges and actions required by the EPC, the industry and / or regulators in response to these challenges. Participants included EPC members, merchants, vendors, law enforcement and other public authorities, processors and card schemes. This Forum and its ensuing resolutions demonstrate that the EPC is more than ever at the forefront of card fraud prevention in SEPA.

***

A changing environment for card fraud

Card fraud prevention represents an opportunity to save more than 1.5 billion euro annually for the European card payment industry. This figure does not include all the direct and indirect costs resulting from managing fraud-related issues nor does it reflect the negative impact on the image of the banks.

Elemér Terták, Director Financial Institutions at the European Commission's Directorate-General Internal Market & Services, reminded the participants in his keynote speech that "security is key to maintain users' confidence" and that it is also "important to involve all stakeholders" in processes such as card standardisation and fraud prevention.

Since the inception of its card program, the EPC has identified card fraud prevention as one of its top priorities together with the SEPA card standardisation program. The latter, amongst others, aims to establish high levels of security in the area of card payments. The EPC is therefore working together with the other stakeholders on card standardisation in the Cards Stakeholders Group (CSG) created in 2009. The CSG is mandated to progress the SEPA Cards Standardisation Volume - Book of Requirements (see link below).

The EPC Card Fraud Prevention Task Force was established in 2003, and from the very beginning included non-bank stakeholders. It was also at that time that the EPC committed to migrate all SEPA cards and terminals to chip and PIN based on global EMV standards by the end of 2010[1]. Nearing the completion of this migration, the European market will soon be in a mature chip and PIN environment. Challenges, however, still remain: for example, card fraud using the old magnetic stripe technology outside of SEPA has to be addressed and security in the area of e-commerce needs to be improved.

In light of these facts, the EPC is currently working on a new Resolution "*Preventing Card Fraud in a Mature CHIP environment*" and so decided to organise the Forum in Paris to have in-depth discussions between experts on the subject.

In his welcome address as host of the Forum, Bernard Dutreuil, Director of Means of Payments at the Féderation Bancaire Française, said: "Together with Groupement Cartes Bancaires CB, the FBF is particularly proud to actively contribute to the reduction of card fraud in SEPA and to improve SEPA card standardisation. In line with the French National SEPA Committee conclusions, we underline the importance of the involvement of the Eurosystem in the newly created SEPA Council on the card fraud prevention matters".

A wide review of the fraud trends and investments in security

The first day of the Card Fraud Prevention Forum was dedicated to the sharing of information about card fraud in SEPA based on the identification of the latest fraud trends and a review of the current investments in security oriented programs.

With regard to observed trends in card fraud the Forum participants shared the following conclusions:

- Card fraud prevention as such represents a major cost saving opportunity for banks.
- The situation is considered to be under control when the card is present and the chip can be used (in face-to-face payments and cash

withdrawals).

- Fraud is migrating rapidly to points of least resistance, i.e. non-chip countries outside SEPA based on the fraudulent use of magnetic stripes on cards which have been previously "skimmed" (i.e. copied) by fraudsters.
- Instances of card-not-present fraud (i.e. card payments in e-commerce or by telephone or mail order) are increasing and represent up to 70% of the total fraud in some systems.

A review of the different investments necessary to secure card transactions highlighted the following:

- Six months before the target date of end 2010, the European experts agree that the results of migration to chip and PIN in SEPA are very good.
- Migration to chip and PIN is even extending to other regions of the world. For example, countries such as Turkey, Morocco, Brazil, and Malaysia are also well advanced. The experts regretted, however, that the USA still remains a significant exception as regards this trend. Claude Brun, Vice Chairman of the EPC, applauded the strategic decision of the largest US retail group to accept and issue EMV chip cards in the US. He also urged the European members of the global schemes to put in place liability shifts[2] favouring EMV through bilateral agreements between regions.
- In e-commerce, there are major concerns on the extent of the migration to the "3D-Secure" security protocol[3]. Although in some countries e-merchants made good progress in adopting this feature, the total number of SEPA transactions protected by "3D-Secure" currently seems to be limited to 10% to 20% in the largest SEPA countries.
- The coherence of data security standards implementation in SEPA was strongly debated including the relevance of applying data protection to dynamically authenticated transactions[4] such as chip and PIN payments. The participants agreed that these data security standards should only be applied in environments still using the magnetic stripe (e.g. non-SEPA cards), or in e-commerce.
- The participants welcomed the EPC's recent decisions on the SEPA security requirements and certification framework to build a SEPA "Certification Management Body".
- The need for installation of devices to prevent the copying of the magnetic stripe on cards ("anti-skimmers") was discussed in detail. The EPC published "*Recommended ATM anti-skimming solutions within SEPA*" (see link below) to help ATM managers create a secure environment. Iddo de Jong of the European Central Bank explained that although most of the magnetic stripe fraud is now taking place outside SEPA, Europeans, rather than blaming their global counterparts, should act locally to fight against the copying of their own magnetic stripes, which often takes place in Europe. Declining all magnetic stripe-based authorisations, unless the cardholder has - temporarily - requested his issuer to do otherwise, would be a good information security measure. Completely removing the (card data contained in the) magnetic stripe from SEPA cards - unless the cardholder has requested differently - could also be a good prevention strategy.
- The building of anti-fraud databases, both at national and European level, is another effective tool to consolidate fraud figures and trends: such databases allow card schemes to exchange operational information thus empowering them to react quickly and appropriately to fraud attacks. Stephanie Czák of the ECB presented the card fraud statistics project which is aimed at consolidating fraud statistics and identifying fraud trends. The first pan-European card fraud statistics are expected to be available by the end of this year.

Many proposals to improve card fraud prevention in SEPA

On the second day of the Forum, four important subjects were debated:

1. Card standardisation and migration to chip and PIN at the global level

The participants considered that the priorities should be to:

- Finalise migration to chip and PIN in Europe and continue standardisation efforts as reflected in the SEPA Cards Standardisation Volume - Book of Requirements.
- Increase pressure by the public and the private sectors on global schemes (such as Visa and MasterCard) to extend EMV liability shifts to the other regions in the world.
- Receive a clear EPC statement on magnetic stripe fallbacks[5]: the support of fallback by acquirers should not be imposed, and preferably not used at all.
- Ensure that in all SEPA card schemes, issuers and acquirers have the option to adopt a chip-only approach, allowing them to systematically refuse magnetic stripe transactions if they so wish.

2. Securing card-not-present transactions

The Forum generated the following recommendations on this subject:

- Amplify efforts on "3D-Secure" implementation by merchants, recognising that although not fully convincing, "3D-Secure" is currently the most widely spread solution available.
- Make authentication possible in non-3D-Secure environments and consider efficient alternatives to 3D-Secure for the initiation of authentication such as wallets or virtual cards[6].
- Ensure protection of the different channels used to initiate card payments: mail orders, telephone, and / or internet.
- Improve the quality of authentication: move from static to dynamic authentication.

- Enforce a CVx2 mandate[7] for all card-not-present transactions to avoid the use of compromised chip or magnetic stripe data by fraudsters and to prevent cross contamination.

3. Data security standards

With regard to data protection, the participants recommended implementation of the following measures:

- Include data protection requirements in the SEPA Card Standardisation Volume - Book of Requirements.
- Agree on a European approach on data security standards and increase European influence in global organisations (i.e. PCI SSC)[8].
- As regards standard implementation, a CVx2 mandate for all card-not-present transactions should be enforced as a priority thus avoiding cross contamination between secure and non-secure environments (see above). Consequently, PCI DSS[9] would have to be applied only to sensitive data (static payment data used in magnetic stripe or in the e-commerce environment), not to chip and PIN transaction data.

4. Improve coordination

To this end, the participants agreed on the following proposals:

- Improve exchange of information with public authorities, notably police forces working at the European level.
- Improve cooperation between relevant stakeholders at operational level.
- Involve more public authorities and stakeholders including merchants and industry in EPC card fraud prevention groups.

A new EPC plan to fight card fraud in a mature chip card market

The participants further agreed that the EPC would update its approach and policy on card fraud prevention and that it would notably amend the current draft of the envisaged EPC Resolution "*Preventing Card Fraud in a Mature CHIP Environment*" to reflect the valuable proposals brought forth on the occasion of this EPC Card Fraud Prevention Forum.

In his closing remarks, Gerard Hartsink, Chairman of the EPC, said: "I am very satisfied that the EPC could organise such an open and fruitful debate on improving card security in Europe. This topic of fraud prevention ranks very high on our agenda and we are determined to address it together with the card payment stakeholders in order to combine our forces ... and beat the fraudsters!"

Cédric Sarazin is the Chairman of the EPC Card Fraud Prevention Task Force.

Related links:

EPC recommended anti-skimming Solutions within SEPA

SEPA Cards Standardisation Volume (version 4.0)

Related articles in this issue:

Standardisation is Key. Focus on security requirements and a European certification framework

New Business Opportunities with Chip and PIN. How to create added value based on EMV technology

Related article in previous issue:

European ATM Fraud Losses down 36 Percent. EMV rollout at ATMs in Europe is helping to reduce skimming losses in some SEPA countries (EPC Newsletter, Issue 6, April 2010)

[1]The EPC's SEPA Cards Framework (SCF) recognises the EMV standard for SEPA-wide acceptance of payments with cards at very high levels of security. EMV is an industry standard to implement chip and PIN security for card transactions.

[2]EMV liability shifts are interbank scheme rules which put the financial responsibility in case of fraud on the party which did not invest in the EMV chip card or terminal.

[3]3D-Secure is a security oriented internet protocol aimed at initiating customer authentication for internet card transactions. The name "3D" comes from the fact that there are 3 domains: one between the cardholder and the merchant, one between the merchant and its card transaction acquirer and a new one between the cardholder and his card issuer allowing the latter to authenticate his cardholder directly.

[4]A dynamic authentication takes place when the elements used for this authentication vary each time. Static authentication, on the contrary, is performed with elements which do not vary and can therefore be intercepted and reused by fraudsters.

[5]Magnetic stripe fallbacks are used in case the payment terminal would have a problem to process the transaction with the chip of the card. This consists of going back to the magnetic stripe type of transaction. This possibility is sometimes used by fraudsters who want to exploit the weaknesses of the magnetic stripe even on chip cards.

[6]Wallets or virtual cards are small pieces of software provided by the card issuer to the cardholder who can generate dynamic card transaction data usable only for a given transaction or within certain limits.

[7]The CVx2 is a set of 3 or 4 numbers printed on the back of the cards which are requested from the cardholder when he does a transaction on the internet or over the phone. These numbers not being present in magnetic stripe or chip transaction data, if the CVx2 were mandated for all card-not-present transactions, this would stop fraudsters who capture data in a card-present environment and make fraudulent payments in card-not-present environments with it.

[8]PCI SSC is the Payment Card Industry Security Standards Council, a global forum developing and maintaining the PCI security standards such as PCI DSS (Data Security Standards) or PCI PED (Pin Entry Device).

[9]See footnote 7.

ARTICLE126

Other articles in this issue

DOWNLOAD FULL ISSUE