Doc EPC424-10
(Version 1.1 Approved)

31 January 2011
CS/FG

Resolution:
Preventing Card Fraud in a mature EMV Environment

(Approved by Plenary)

Circulation: Publicly available
Restricted: No

BACKGROUND

Card fraud prevention represents an opportunity to save or reduce the more than 1.5 billion euro annual costs faced by 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.
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 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 plenary is requested to approve a new Resolution "*Preventing Card Fraud in a Mature environment*" that was extensively discussed with various market participants in the EPC Cards WG and Cards Fraud Prevention TF and in a dedicated Forum in last June.

RESOLUTIONS

It is hereby resolved that the following Resolutions are approved (also for inclusion in to the next version of the SCF). The EPC Cards Working Group will monitor their implementation and report to the Plenary.

[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.

- ***Resolution # 1: Limiting the potential impact of an incomplete migration to EMV outside SEPA on SEPA issuing***

Resolution 1.1: The EPC requests Schemes to ensure through cross-regional liability shifts SEPA issuers and acquirers are shielded from any negative impact of an incomplete global migration to EMV outside SEPA. For markets that have started their plans for a mature EMV environment, the implementation of the liability shift should be effective at the latest by end-2015. For other markets, the implementation of this Resolution rests on the persuasion power of European regulators (ECB, EC) and the action of EU Banks with global presence.

Resolution 1.2: The EPC reaffirms its statement on magnetic stripe fallbacks: card schemes should aim at restricting the use of magnetic stripe fallback to exceptional cases. PAN key entry as a fallback should be prohibited.

Resolution 1.3: The EPC recommends that SEPA card schemes grant issuers the option to adopt a chiponly approach be it by issuing chip only cards or by allowing them to refuse magnetic stripe transactions if they so wish, providing that there is clear communication with the cardholder.

Resolution # 2: For Card-Not-Present environments ("e-Commerce", "Mail Order", "Telephone Order") EPC recommends that cards schemes and their members implement within SEPA the following measures: (to progress on security, pending further dialogue and indications from Authorities)

- **E-Commerce on the issuing side**:
  - **Resolution # 2.1**: Issuers and card schemes shall evidence at the latest **by end 2013 that** appropriate authentication solutions at equivalent level of security are in place,
  - Such authentication solutions could be:
    - Risk-based authentication
    - Challenge-response mechanism
    - Dual channel authentication such as SMS
    - Hardware based authentication such as a token or chip reader
    - Virtual cards
    - Or any innovative solutions considered effective by payment schemes

    The above should be combined with appropriate risk management tools.
  - **E-Commerce on the acquiring side**:
  - **Resolution # 2.2**: Stakeholders shall evidence at the latest by **end 2013** that they are able to support such authentication solutions on the acquiring side.
- **Mandatory usage of CVX2 in all Card-Not-Present environments**:
  - **Resolution # 2.3**: Except for merchants having implemented or submitted plans to acquirers to comply to Resolution 2.1 and 2.2: In all Card-Not-Present environments, and for cards capable of transactions in such environments, card schemes shall mandate at a minimum as from 1 January 2012:

- Acquirers to acquire and transmit CVX2[2] values or their equivalent.
- Issuers to decline any authorization request made with a false CVX2 value or its equivalent ("CVX2 mismatch")

However, for *recurring* payment transactions where the merchant has stored the card number and the expiry date but not the CVX2 or its equivalent, the presence of the CVX2 value, or its equivalent or better means of authentication is only required for the initial transaction.

Card schemes may also allow exceptions or temporary waivers for specific, low-fraud sectors, as long as these represent in total at most 10% of the SEPA acceptance basis.

For environments not responding to waivers, Issuers should be advised to decline any authorization request not carrying a CVX2 value or its equivalent ("CVX2 missing").

NB: The main objective of this resolution on the usage of CVX2 or its equivalent is to prevent cross-contamination (i.e. the reuse in CNP environments of data potentially compromised in Chip / Magstripe card present environments), by requiring the presence of a data element (the CVx2 or its equivalent) which is not present in other card present environments (Chip or Magstripe transactions).

- ***Resolution # 3: Protect payment data, notably from data compromise***

As general principle, the storage or the transportation of sensitive data in a secure way should be restricted to the strict necessary for handling cards transactions.

The EPC will consider endorsement of Data Security Standards, and promote them to the Card Stakeholders Group community. The Card Stakeholders Group will be invited to deliver its view on migration.

In such a migration plan, data protection (e.g. encryption) efforts should focus on sensitive card data that could be misused for card transactions – capitalising on a risk based approach, taking into consideration notably EMV migration and efforts to make the use of compromised data difficult (e.g. dynamic EMV & eCVx based transactions or end-to-end data encryption). "Sensitive data" will be defined in the SEPA Card Standardisation Volume – Book of Requirements.

To that end, EPC will cooperate with the relevant stakeholders to include data protection or encryption 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 (e.g. PCI SSC).

As regards standard implementation, the recommendation to use CVx2 or an equivalent for all card-not-present transactions should be considered as a priority to avoid cross contamination between secure and non–secure environments (see above Resolution # 2.3). Consequently, Data Security Standards should only be mandated when sensitive data are stored or not protected and should only be enforced on a risk-based prioritised approach based on the reduced risk inherent to EMV.

- ***Resolution # 4:***

The Cards Working Group intends to incorporate the above where appropriate in the EPC principles or requirements for SCF and Volume compliance.

[2] As defined in the SEPA Cards Standardisation Volume Book of Requirements