GALITT article

PCI-DSS – new French cultural exception?

France has been reluctant to implement PCI-DSS, this new acronym meaning improved security… and additional costs. However, security has always been a matter of cooperation among major players of payment systems, including financial institutions and the retail industry. But the PCI-DSS issue has caused significant opposition which had been surprisingly strong in France, despite a few moderate comments. Are we facing a new claim for "cultural exception"? Possible although not that obvious…

First of all, what are we talking about? PCI-DSS stands for "Payment Card Industry – Data Security Standard". The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. It is a full set of security rules to provide confidence in the sensitive data storage, specifically addressing card-related data (i.e. card numbers called PAN) by merchants and third-party processors. The standard aims at protecting cardholders and at keeping their trust in payment systems at the high level where it currently stands. PCI-DSS comes with a certification process which methods and practices depend on the volume of acquired transactions, whatever the payment channel. The rules are said to be "absolute", as they mandate security mechanism to be implemented and audited by QSAs ("Qualified Security Assessors"). There is a very few room if any for possible "shades" in implementation of the measures nor in their evaluation.

In France or abroad, there is a consensus that implementing PCI-DSS is actually complex and expensive. Furthermore, as the assessment process mandates repeating audits for larger merchants, the cost of implementation is not a one-off but a recurring one…

These security measures have been defined following the theft of files containing a huge number of credit card data in the United States (one was referring to 40 millions PAN stolen in 2005!) Card numbers were used to execute fraudulent purchase transactions over the Internet, and sometimes to create counterfeit magnetic stripe cards. Major international card schemes first reacted to this new risk by defining their own set of rules: the Visa AID program ("Account Information Security") and the MasterCard SDP programme ("Site Data Protection"). After a while, major stakeholders in the industry requested the schemes to agree on a single set of consistent rules, and thus was the Payment Card Industry standard defined. From 2006, the schemes established the new "Payment Card Industry - Security Standards Council" (PCI-SSC). The association is led by an executive committee, composed of representatives from the founding payment brands. But the association is open to so-called participating organisations, which provide input and feedback on the evolution of the standard via an advisory board. Large retailers, processors and payment-related organisations including the European Payments Council (EPC) have joined.

Besides the specifications of the standard itself, payment schemes mandated the application of PCI-DSS and introduced new penalties and fines including the exclusion of a merchant. This was the starting point for increased disputes, and France was among the countries where the opposition was and still is very strong. But France is not the only country disputing the rules. Even in the United States where the related risks of data protection and "Identity Theft" are highly sensitive, many voices are declaring that the costs are too high and are claiming for a more flexible and more fitted methodology.

Matters for disputes are basically four: the relevance or applicability of some measures, the claim for exclusion of EMV-processed transactions (this one being likely a French '"cultural exception"), the uselessness of the process, and the irrelevance of the methodology!

Let's avoid the dispute addressing the relevance or applicability of several measures: security experts may for sure discussed such issues for years. There might probably be among the dozen of

requirements a few which implementation is either difficult, too complex and/or possibly very expensive. But the founding principles and goals of the standard cannot be reasonably disputed and are not significantly disputed…

However, there is a true question with respect to the modularity in implementing the standard, or more precisely, the modularity in assessing its implementation. The PCI-DSS standard is indeed unique whatever the merchant or the processor. But payment systems define four levels of validation mechanisms. Larger merchants (processing more than 6 millions transactions per year), a yearly audit from an accredited assessor (QSA) is requested, in addition to quarterly forensics investigations of their systems. The validation requirements are then lowering with the size of the businesses, progressively introducing self-assessment and replacing mandates by recommendations. So, French merchants have then requested to take into account only the electronic commerce transactions where cards are not present. They were claiming that they invested a lot to support EMV upon the request of the French banking community. So they were reluctant to invest again in order to protect the players which declined making the same security efforts, and specifically the Americans whose denial of EMV is a matter of fact! Although such an argument is politically clever, it can easily be disputed with regards to security. Stealing card-related data (including the PAN and expiry date) is also possible during an EMV transaction, and such data can then be used for processing non-EMV transactions like e-commerce payments. And although Visa and MasterCard feel a bit embarrassed facing the French reactions, more or less supported by some French banks, they can easily argue that the suggested approach is inappropriate to protect stakeholders.

Mail order and e-commerce merchants then joined in supporting the argument, claiming that visual cryptograms, these 3- or 4-digit numbers printed either on the signature panel of Visa or MasterCard cards, or on the front of some other cards like American Express ones, cannot be captured during an electronically processed transactions, whether it is EMV or magstripe based. Hence the claim was that the PCI-DSS approach is useless: Issuers are protected from card data theft when they implemented the check of such visual cryptograms while authorizing card non present transactions. But it is assuming that e-commerce and mail order merchants are requesting such data from the cardholder and transmitting it in the authorization request. France and most of European countries have been implanting such a security feature, which has proven to be efficient, but other regions and specifically the US are lagging behind! French merchants again complained that the PCI-DSS mandates were requesting new investments to cover risks already addressed by previous investments, and that the beneficiaries were merchants refusing to invest! And even if a very few merchants may store this visual cryptogram, their level of protection is likely to be already very strong. In Europe indeed, and in France specifically, the personal data protection laws and rules have created for years an area of best practices with regard to sensitive data.

The last contesting argument, which is also claimed in the United States, relates to the irrelevance of the approach. The larger the merchant, the stronger the assessment process: and so the process is quite weak for small e-commerce sites. Every fraud expert knows that comprising sensitive data often occurs in smaller shops and stores, where the security is lower and the control mechanisms may be missing. So many argue that PCI-DSS should first focus on small merchants, where the risk is high although numbers are small …

In this context, what is the status in France? The number of certified sites remains low although it is slowly growing. PCI-DSS indeed creates an opportunity to initiate projects in order to improve the security level of their information systems. For, although payment-specific in its approach, PCI-DSS relies on a concrete know-how of data and system protection. Disputing the theoretical somewhat dogmatic approach makes sense, but there is no way claiming that such security recommendations should be ignored! And the dispute is actually focusing on the implementation and furthermore the validation process, and not at all on the content of the standard itself. Cautiously enough, banks are introducing new statements in their acquiring agreements, to mandate the merchant's compliance with PCI-DSS. Thus, banks would be able to call upon liability of the merchants in case of penalties or even

exclusion of the merchants by a payment scheme. Such an approach however requires the agreement of the merchant, which might not be that obvious!

In parallel, work is on-going to consider more flexible implementations of PCI-DSS. And the standard continues to evolve, becoming progressively mature. It is hard to envision the pace of its implementation in France, but the trend towards more secure systems is not to be discussed. Regardless of its weaknesses, PCI-DSS is contributing to a better awareness and a wider broadcasting of security best practices. The French “cultural exception”, which noticed with respect to the strength of the contest, should not last for long if payment systems are wise enough to consider a more flexible approach to favour PCI-DSS actual implementation.

Gérard de MOURA
Managing Director
GALITT