



RECOMMENDATIONS FOR THE SECURITY OF INTERNET PAYMENTS **April 2012 (EUROPEAN CENTRAL BANK)**

EURO 6000 considerations

Risk control and mitigation

Some merchants manage payment data for their own services (loyalty programs, security tools, and others). Of course they must do it properly with the right security measures, and PSPs and acquirers must help them with these issues.

Nevertheless many merchants do not need to manage payment data for other purposes than payment processing. In this case PSPs or merchants should manage directly the payment data. In this way, merchants do not have to worry about payment data (they do not really manage or store it in any way) and the security will be higher (merchant data bases cannot be compromised to obtain payment details).

Strong customer authentication

CVX2 is one of the right security solutions, and merchants, PSPs, and acquirers have to use it if possible. In the last months new solutions are arriving, especially wallet solutions. In this case CVX2 can be used in the first wallet transaction (in many cases enrollment transactions), but CVX2 cannot be used in the next transactions, just because the wallet cannot store CVX2 value for security reasons.

Customer education and communication

PSPs, Issuers and acquirers must educate and communicate highlights security best practices to customers, but they cannot be liable for all the customers' behavior, especially the ones related with the device security (firewall, antimalware, antivirus, etc).

Notificating, setting of limits

Limits and filters must be easy to understand for cardholders. An excess of options can be confusing for cardholders.

It is especially important to manage the time between the website customer purchase and the authorization transaction. Several merchants do not launch the authorization transaction till they are ready to deliver the product. This can take hours or days. Cardholders can open the internet transactions filter, buy in the internet (website purchase), and close the internet transactions filter. In this case, the authorization transaction will be declined. So, Issuers need to implement smart limits and filters which allow customers to use them properly.

