The role of payment providers in providing consumer protection mechanisms against fraud and in providing dispute resolution procedures – Valentim Oliveira

The Internet has, over the past three decades, grown from a mere experimental research network to a billion user network that has changed our social lives as well as projecting a whole new economy fabric. An ever growing threat to this development has been witnessed over this last decade through the emergence of cyber crime of unprecedented scale. The increase in sophistication of the attacks and the magnitude of infected systems is astounding. Confidence in payment means is a critical variable that has to be assured and thus the payment providers have endeavored to keep ahead, promoting various techniques to assure security to internet payments.

The use of the bank card number has been one of the most popular means of authentication on the internet. The adoption of the CVx2 cryptogram was but one of the initial techniques that was well accepted by users and brought through effective benefits. The adoption of virtual cards in some markets, containing tight spending limits and restricting the life time of this credential, has frustrated attack objectives, bringing in yet another vector of protection. The adoption of authentication means through the 3D Secure programs, currently being deployed by the International Payment Systems, bring in a much awaited means of augmenting the protection on e-commerce payments.

Authenticating home banking users and transactions has similarly observed a considerable evolution throughout recent years. Payment providers are offering payments through the use of the home banking credentials, promoting account based payments. As an example building upon this concept, the European Payment Council has defined a model for pan-European e-Mandates for Direct Debits. The familiarity of the user with his home banking authentication mechanisms contributes to user convenience and ultimately to a superior protection. Given the fact that these mechanisms are market, bank and even client specific, they have the benefit of adapting the protection levels to the particular user context. The use of OTP (One Time Password) and transaction signing with PC independent tokens is growing considerably, similarly is the use of secondary authentication channels such as short service messages (SMS). These methods greatly reduce the risk of payments on the internet even in the case where the PC's are under the control of malware.

Fraud detection systems have suffered considerable evolution in order to detect abnormal patterns and nowadays a mixture of rule based systems and neural based systems is ever more common. Profiling user habits is essential to detect shifts in spending patterns and quickly intervene. Given the global nature in which current fraud patterns occur, information sharing on cyber crime trends is crucial in order to tune the systems to new modus operandi. The payment industry makes use of in-place fraud deterrence networks in order to share intelligence; however the dynamic nature of the internet payments requires a swifter response capability.

Dispute resolution procedures at a global level are essential as an ultimate protection to internet payments. The industry has made use of practices that have been put in place by the card networks potentiating the already global nature that was present as a basis. However, the flexibility inherent to internet payments brings in an even higher demand for the efficiency of these mechanisms across

borders. Much work is still to be done in order to enhance and harmonize dispute procedures across alternative payment methods.

Secure payments on the internet are vital for the prosperity of internet usage experience and thus an imperative base for global economic and social development. User awareness is considered fundamental and therefore has been a continuous focal point of investment although results seem to dismay in many situations. The payment industry has brought on its experience on managing payments on traditional ATM and POS channels and has adapted to evolving business models that result from an economy that progresses at an unprecedented pace. In response to evolving attacks, a set of authentication mechanisms have been put available in balance with user convenience. Some attacks do manage to counter the controls in place and there fraud deterrence systems have been adapted to fight them off, giving the final user an adequate level of security whilst paying on the internet. The payments industry has thus managed to keep but one step ahead in securing internet payments.