



RFConnect speaks with **Pat Carroll, CEO of ValidSoft** to find out his professional opinion on recent Europol stats and its policy on fighting cross-border card fraud (please read the full Europol report [here](#)).

During the interview we highlighted the card fraud issues in banking industry and identified a few tips on how consumers can protect themselves from card fraudsters in 2013.

ValidSoft
Redefining Fraud Prevention

Measure thrice and cut once

In your opinion, does EU banking industry fully realise a possible negative repercussion of such cross-border decline policies? Do you support the statement that Europol's recommendations in this case are totally destructive for the whole banking industry?

In my opinion, it is a mistake for Europol to recommend such a blunt solution, namely that all EU issuing banks should geo-block EU issued EMV cards, meaning they will not work in non-EMV countries without the mag stripe being explicitly reactivated. EU issuing banks already lose large amounts of interchange fee revenue, incur substantial processing overheads and routinely upset their travelling customers through aggressive cross-border decline policies. Those using practices such as "travel flags" still incur administrative costs, still annoy their customers (I have personally spent over 40 minutes in a phone queue), are no guarantee that the card will not be blocked and can also be exploited by the fraudsters themselves. There is a cost to banks and their customers today from excessive cross-border declines which does not feature in the aforementioned 600m euro.

What types of technologies/solutions should be considered by EU banks which wage a fight with card fraudsters?

Rather than simply basing their decisions as to whether to accept or decline a transaction using historic data and behavioural patterns of customers, the technology exists today to tackle this problem from both perspectives; fraud prevention and

false-positive (decline) reduction. Importantly, the technology does not require the EU banking industry to break the fundamental tenant of universal acceptance or to incur ever more overheads which will, eventually, be passed onto the consumer. The way the security solution can work is to use Proximity Correlation Logic (PCL) as one of the multiple factors of authentication. By using a mobile phone in a completely invisible and unobtrusive fashion, PCL can detect if a cardholder is not where the transaction is being made in non-EU countries. What's more, the solution has been granted a prestigious European Privacy Seal given its strict adherence to EU data protection legislation. Rather than banks spending more at the back-end on investigations and card re-activations, we should be looking to reduce both cross-border fraud and excessive declines at source.

Please tell us more about your company and its flagship products, giving a few examples of your best practices in card fraud prevention. Does your product/solution comply with any regulatory requirements and what are they?

Validsoft protects all banking channels through telecommunication based authentication solutions. We combine visible and invisible layers of security for strong authentication in real-time. We pride ourselves on being the only company in the world with three European Privacy Seals. Using the specific example of card fraud prevention, one of the greatest challenges faced is cross-border fraud committed at ATMs and Point-of-Sale (POS) devices. Whilst the actual fraud losses are significant,

of equal if not greater concern, is the resultant impact caused by high decline rates. False-positives (declining legitimate transactions) are a major problem and can account for as much as 90% of cross-border declines. This results in lost interchange fee revenue, high costs of fraud case-management and inconvenienced customers. At ValidSoft we have designed a solution that can tackle both fraud and reduce false-positives in what we define as a “no or low friction” model from the customers perspective, by utilising real-time invisible security checks that result in a very strong security model but with total ease of use.

The ValidSoft platform detects fraudulent cross-border transactions but more importantly can do so without the collateral damage of high false-positive rates. Using the patent-pending Proximity Correlation Logic™ (PCL) for card-present transactions, ValidSoft can reduce cross-border false-positive rates to single digits, all in a completely invisible and real-time fashion, within the authorisation process itself. It requires no more than the cardholder having their registered mobile device with them and active when transacting at ATMs and POS devices abroad. The customer will not be contacted if it is deemed to be a legitimate transaction; there is no cost to the cardholder and the only visible sign of change is legitimate transactions will now be approved rather than declined. In the event that a fraudulent transaction is suspected the customer is contacted in real-time before the transaction is consummated thereby protecting the customer and the bank. Because this patent-pending solution has been granted a prestigious European Privacy Seal (EuroPriSe) for its processing model, it can be deployed on the basis of informed prior consent, removing the onerous requirement of explicit Opt-in. Once again the same platform and device used to protect the electronic commerce channels is used to transform international card-present fraud processing.

How do you think it will be possible to liquidate / reduce the number of card frauds in the future, or will the problem remain / deteriorate? What are your future predictions?

Collaborative thinking in the fight against cybercrime is what will drive effective security solutions for card fraud, and more generally payments fraud. Cards are slowly going to be moving onto the

mobile world. This shift will bring in new threats; there is no doubt that electronic fraud will certainly be drawn to the new medium. Security software companies (like ValidSoft) that can bring the power of telecommunications to the world of security to create innovative solutions, will be able to make security usable, flexible and ultimately reliable. There is a terrific opportunity to shape this new landscape and I fully anticipate that ValidSoft will be at the core of this industry shift. EU banks, security software companies and card issuers need to get together to fight cross-channel fraud, whilst as an industry we move to a new paradigm of fraud detection and prevention.

Can you please give a few tips on how to protect yourself from card fraudsters in 2013? What are the most efficient ways not to become a victim of card fraud and cybercrime?

Using the customer's mobile phone will increasingly become central to card fraud prevention. It is all part of what is called context-aware security solutions. Avoiding being the victim of fraud or cybercrime is not the right question in my opinion. The financial industry's main focus should be on preventing fraudsters from using stolen data. Technology can already show that an individual (in fact his/her mobile phone) is not in the country (eg US) when his/her credit card is being used at a POS in New York. Technology can do so in total respect of privacy laws, through anonymous correlation, and in a way that is totally invisible to the customer before such withdrawals and purchases are authorised. Technology can also support additional strong transaction authentication and verification methods, namely through an automated call to that phone can immediately confirm that fact, and – if the card holder rejects the transaction – alert the issuing bank to block the card.

The level of authentication can be tailored to the transaction type and size, and can even include voice biometrics for added security if the card issuer wants to use it.

The key lies in real-time detection, prevention and immediate resolution enabled by the empowered customer. The security technology industry has a job to do in encouraging customers to question just how it is possible in 2013 for card fraud to be so profitable on such a scale. That really is a mind-boggling thought.