innopay

Triport 3
Westelijke Randweg 43
1118 CR Amsterdam Airport
The Netherlands

PO Box 75643
1118 ZR Amsterdam Airport
The Netherlands

+31 20 6580651
info@innopay.com
www.innopay.com

Member of European Payments Consulting Association, EPCA
www.epca.de

European Central Bank
Secretariat Division
Postfach 160319
60066 FRANKFURT AM MAIN

Subject: response to 'Recommendations for the security of internet payment systems'

Dear Sir, Madam,

We welcome the fact that ECB is looking deeply into the issue of internet security for payments. Hereby we would like to briefly contribute to the debate by responding to the 'Recommendations for the security of internet payment systems', as published on 20 April 2012.

For now we have the following observations:

1. The more specific topic to be addressed, we believe, should be 'customer not present' transactions. This is the situation where the merchant cannot see or identify the customer. At that point many risks arise in terms of payments, shipment and contracting.
2. It is our opinion that the current massive use of credit cards is one of the main reasons for problems with internet payment security[1]. This payment mechanism was designed 60 years ago and does not have strong built-in security features. Therefore it is not by design suitable for the web:
    a. With 16 digits, a date and a code it is possible to charge someone's card globally without him or her knowing or having the need to authenticate/authorise;
    b. There are many parties involved in the chain, who all handle the crucial payment data which is attractive to hackers. Many points of failure make the system as a whole vulnerable to identity theft and reduces general trust in online payment systems;
    c. The poor built-in security of the cards system is mitigated by a series of additional technical measures (eg 3DSecure, fraud & risk software) as well as contractual protection of the customer (in terms and conditions) that allows him to unilaterally reverse (charge back) the transaction.

[1] Similar risks exist with direct debits, but these are smaller because of the (thus far) local nature of direct debit solutions. The SEPA Direct Debit will be more vulnerable for trust issues. E-mandates and white listing will reduce risks for payers and payees

3. Recommendation nr 7 is the key of this report and represents a clear direction. Strong authentication of payers will reduce fraud, which will benefit both payers and payees. Regulated entities (Payment Institutions incl. banks) are well placed to offer these authentication services, since they have to comply with the KYC (Know Your Customer) criteria. Nowadays enough good technology exists to be able to offer attractive service in this field to payers and payees.
4. Stakeholders in the payment industry could consider restricting the entering of sensitive payment data (e.g. credit numbers and bank account numbers) at unregulated entities (such as merchants and gateways) and should require a proper authentication of the payer by a regulated PSP. This is contrary to today's practice where sensitive payment details are stored in uncontrolled environments such as merchant's website and processor's systems. Such a restriction will put strong requirements to the PSPs in the field of authentication offerings.
5. More focus on payer authentication will shift the risk to the authentication solutions (issuing process, one/two factor tokens, re-use existing tokens, 'man in the middle'). Guidelines should be developed for the authentication of payments. The financial industry could look more deeply into European developments currently being done in the field of e-identity, e.g. in the projects STORK and SSEDIC. We think a lot can be learned and re-used from the challenge the public sector is facing when it comes to e-business (and vice versa).

In summary we strongly support the observation that internet payments security can be improved by strong authentication of payers and payees. As a follow up we suggest additional research to be done on the current authentication landscape and the related strategic industry options.

Sincerely,

Douwe Lycklama à Nijeholt
Director
douwe@innopay.com
+31655711150