IT Security official comments on the ECB's report: Recommendations for the security of Internet payments.

Bank of Cyprus is operating as a PSP for internet payments. The Bank's management is demonstrating high concern regarding the security of the respective operations by adopting the latest defensive mechanisms and procedures and by reviewing, in a periodic basis, their effectiveness and the client's feedback.

The Bank's management and security executives are allied and support the recommendations provided by ECB. In general the Bank agrees with the recommendations and has implement a high number of them. Moreover Bank of Cyprus will be committed to incorporate those that apply with its infrastructure and operations, in the relevant policies, security and audit reviews, in the implementation of new internet payments systems and as a part of the IT risk management process.

In the rest of this document general comments on the report "Recommendations for the security of internet payments" are depicted, accompanied with some specific notes applied to certain recommendations.

General Comments:

For a successful program that will achieve adaptation of the recommendations, the most critical ones have to be exported as mandatory requirement with a strict deadline of implementation. Although the management recognized the necessity for security controls, no prioritization, implementation program and direction is up to the level of other projects that the financial institutions are committed to implement. Simply if these recommendations will not transform to an obligatory compliance requirement we are not so confident for their timely analysis and incorporation inside the institutions infrastructure and procedures. A similar example is the PCI standard: Although its articles support the effort for technical security, not only for the card payments but for the overall Information Security governance, many European financial institutions are not complied just because this is not a mandatory requirement from the Central Banks of their countries.

A lack of ability to identify internet payments risk appetite for each institution and country is observed leading to either very weak measures or extremely strict controls that are costly and have negative impact on the clients' experience. Moreover this situation leads to extra controls that do not provide value regarding the protection of the clients' transactions and data. These recommendations id proposed to be accompanied with documented official minimum non acceptable events and scenarios and with their protective measures. These measures have to be mandatory requirements and not recommendations.

The recommendations incorporate technical security controls that can be applied in general for all the financial institution's systems. More specific guidance and controls such as fraud patterns prevention and specific indicators for monitoring and reporting

would be considered of high value since they are not easily identified by the management and personnel responsible for the internet payments.

Difficulties are observed (due to limitations of knowledge, resources and time) for the accurate and timely information gathering and analysis of daily security events, attacks and vulnerabilities. A nation or industry wide service, supported financially by the institutions (e.g. iDefense) would be a broad value for knowledge and information sharing, notification, measures and strategic decisions in a timely and effective manner.

A high level of trust between the private sector and law enforcement is not easily been created. Confidentiality agreements, specific persons from both sides as liaisons and scheduled meetings with official minutes would enforce this relationship that is considered very important regarding the recommendations applied to incidents' response processes.

Nowadays a strategic step for many financial institutions is to implement solutions for the mobile (smart phones) platforms such as iOS and Android. All these technologies provide new capabilities but also security limitations (for example the self certification of a banking application on Android without a third party as a CA must not considered as sufficient to achieve and protect client's trust). Moreover they present new schemas of fraud. It is proposed that, although the recommendations have a generic character, to be re – evaluated so as to achieve certainty that are applicable for these technologies too. The report on Overlay Services from ECB has to be also evaluated when implementing similar systems.

If the recommendations are accepted, then the retailers (e – merchants) will be expected to apply the same standards as payment providers. Implications (for example the Bank compensates a customer for a fraudulent activity but the merchant has cancelled the activity with no notification or the merchant's website suffers from critical vulnerabilities) have to be considered though. Certain scenarios need to be assessed before adaptation of the recommendations, although that Bank of Cyprus believes that specific audits to the e – merchants have to pass also as a regulatory requirement. On the merchants' side many of the recommendations applied to them are not implemented because they are not enforced. ECB can communicate and agree for co-operation with their respective body authorities regarding security of internet payments. A proposed schema is the following one: There could be two levels of compliance (the standard level at which the PSP complies with the mandatory key considerations and the advanced level at which the PSP complies with all the key considerations). I believe that such an approach will give the PSPs a strong incentive to comply with as many key considerations as possible because this will be used as a marketing tool towards their customers (a higher certification level will imply a stronger commitment of the PSP towards transaction security).

Existing laws in countries (such as Ukraine, Russia etc) are mandating the usage of specific protocols for encryption, authentication and card clearance among others. These requirements restrict multinational European institutions to apply an internet payment system with specific security controls by means of cost and technological limitations. It is proposed that in the event of the recommendations acceptance, ECB

to cooperate with the respective central banks for facilitate the security controls implementation.

Specific comments regarding the 14 recommendations:

Internet payments services security policy

The initial requirements for the internet payments services security policy have to be aligned with of the business divisions and management expectations and goals and clearly depicting the institutions risk appetite and acceptance. No certain value will arise if only the IT Security or Information Security executives will develop solely and entirely such a policy. At a second level a review and self assessment of the existing policies has to be performed in order to avoid confusing overlaps and identify areas for updates and corrections.

Risk identification and assessment

The recommendation 2: Risk identification and assessment is considered by the Bank of Cyprus as the most critical and the outcome of a respective process execution is the basis to implement all the rest of the controls depicted in the report. Re – evaluation and gap analysis of the IT Risk Management has to be performed (and referred also to the recommendations). These actions have to be accompanied with evidence, presented to the management and regulatory authorities that validate the incorporation of the 4 KCs of the recommendation 2.

Phishing, Malware

Anti - phishing and anti Trojan (malware) services and software for internet payments systems can be considered as a nation based or industry based investment.

FPS

A certification body has to evaluate the Fraud Prevention Systems (FPS) in Europe for compliance with these recommendations. A potential change from the institution's part in order to harmonize its security level with these recommendations, presents significant cost and work load. So the chosen solution has to officially prove that implements the relevant controls presented in the ECB's report. The 10.1 KC regarding FPS needs to be a mandatory requirement and not a recommendation.

3D Secure

It is proposed the adaptation of a digipass solution or other dynamic password solution during the enrollment and authentication process rather than static passwords that are currently provided as a choice for clients.

Panagiotis Koumousis,

Bank of Cyprus Group, IT Systems Security Officer