COMMISSION de SURVEILLANCE du SECTEUR FINANCIER

In case of discrepancies between the French and the English text, the French text shall prevail

Luxembourg, 11 March 2011

To all the establishments subject to the supervision of the CSSF*

CIRCULAR CSSF 11/504

Re: Frauds and incidents due to external computer attacks

Ladies and Gentlemen,

In view of the regular occurrence of new external computer attacks which may result in frauds or incidents, the CSSF deems appropriate to draw up a regular assessment of the situation in order to:

- closely follow the development of the phenomenon;
- be able to inform the supervised establishments on the types and frequency of the attacks;
- anticipate as much as possible the cycles in relation to attack phases as well as the probable consequences for the financial centre;
- contribute to a better protection of the activity of the financial centre through recommendations adapted to the reported incidents.

To this end, the CSSF requests all the establishments under its supervision to report as soon as possible any frauds and any incidents due to external computer attacks and to keep at their own initiative this information up to date after the date of the report concerned.

This circular comes into force with immediate effect.

Yours faithfully,

COMMISSION DE SURVEILLANCE DU SECTEUR FINANCIER

Claude SIMON	Andrée BILLON	Simone DELCOURT	Jean GUILL
Director	Director	Director	Director General

Annexe: Incidents and information to be reported

* Applies to Supervised Entities as defined in point 2 e) to j) in Section 1.1. of Circular CSSF 24/847

Annexe: Incidents and information to be reported

1. Nature of the incidents to be reported

An incident should be reported as soon as an actual attack succeeded (e.g. confirmed attempt of embezzlement, corrupted IT system) even if the attack did not lead to a fraud (e.g. absence of actual misappropriation of funds).

It should be borne in mind that "phishing" attacks are excluded from the perimeter and shall therefore not be reported.

2. Possible services aimed by the attacks

Even though the financial services provided through Internet are the preferred target for computer attacks, the latter may also aim at other types of service or internal activity. Thus the reports concern any fraud or incident following an external computer attack in relation to:

a) Financial services provided through Internet which include all the services provided online by a Luxembourg establishment, *via* Internet, by direct or indirect way to private or professional clients irrespective of the fact that the IT platform is operated by the establishment itself or by third parties.

The direct way concerns online financial services provided directly to private or professional clients for the management of their assets. The indirect way means that the services are used by professionals or by the personnel of the establishment for the management of one or several clients.

Therefore, the establishments offering online e-banking or e-brokerage services to private clients are not the only ones concerned. The establishments which put in place a management or an online access for their managers or which make such an arrangement available to other professionals acting on behalf of one or several clients are also concerned.

b) Any other internal or external service or activity of the supervised establishments, in order to include in the perimeter the attacks through Internet targeting for example the internal network, internal servers or data exchanges between an establishment and a third party (partner, correspondent, parent company, subcontractor, ...).

3. Information to be reported

The report to be sent to the CSSF shall include a description of the incident (points a) – f), and depending on the situation points g) and h) or i) and j) in addition):

a) type of the incident or fraud with a description;
b) total amount of the damages if it can be estimated, with an indication of the distribution over the period:
    - total amount of the fraudulent transactions taken together;
    - total amount of the damages for the clients;
    - minimum and maximum amount of the individual damages;
    - total amount of the damages for the establishment, including administrative and legal costs, application of corrective measures and eventual reimbursement of the client;
c) an indication per incident or fraud if the establishment lodged a complaint with the judicial authorities;
d) any other striking information, including of technical nature, likely to help understand the incident or fraud;
e) classification of the incident by the establishment (e.g. minor, significant, major, critical) with specification of the position on the classification scale used (e.g. incident classified "2 - significant" on a scale ranging from 1 to 4);
f) possible measures taken by the establishment to compensate or reduce the risks.

As regards the frauds or incidents following an external computer attack in relation with financial services provided through Internet, the following additional information shall be reported:

g) the nature and name of the Internet service concerned with an indication of the specificities (consultative, transactional, mono- or multi-client management, private and/or professional clients, access by client or by manager/employee, own or shared IT platform, internal or outsourced [with the name of the subcontractor] ...);
h) the number of clients concerned by each type of incident or fraud over the given period.

As regards the frauds or incidents following an external computer attack in relation with any other internal or external service of the supervised establishments, the following additional information shall be reported:

i) the nature and name of the technical target(s) (server, flow…) and of the service(s) or activity(ies) concerned with an indication of the specificities (own or shared IT platform, internal or outsourced [with the name of the subcontractor] …);
j) the nature and number of direct or indirect users concerned by each type of incident or fraud over the given period (one user may be a client, employee or internal service, a partner, an entity of the group,...).