Republic of the Philippines
Department of Finance
INSURANCE COMMISSION
1071 United Nations Avenue
Manila

Head Office:
P.O. Box 3589 Manila
FAX No. 522-14-34
Tel. Nos. 523-84-61 to 70
Website : www.insurance.gov.ph

Circular Letter No.:	34-2011
Date:	October 12, 2011

CIRCULAR LETTER

To: **All Insurance/Reinsurance Companies, Intermediaries, Mutual Benefit Associations, Trusts for Charitable Uses and Pre-need Companies**

Subject: **Dissemination of AMLC Resolution No. 93 August 17, 2011**

Pursuant to Anti-Money Laundering Council (AMLC) Resolution No. 93 dated August 17, 2011 (copy attached), you are being directed to:

1. Defer, until further advice, the submission to the AMLC the hard copies of the suspicious transaction reports;

2. Only the compliance officers or duly authorized officers shall automatically sign the covered transaction reports and suspicious transaction reports; and

3. Preserve and safely store the electronic copies of covered transaction reports and suspicious transaction reports for at least five (5) years from the dates the same were reported to the AMLC.

For strict compliance.

EMMANUEL F. DOOC
Insurance Commissioner

INSURANCE COMMISSION
10-12-11
GEN. RECORDS

Anti-Money Laundering Council
Bangko Sentral ng Pilipinas Complex
Manila, Philippines

RESOLUTION NO. 93
Series of 2011

In the 2008 Mutual Evaluation Report (MER) on the Philippine AML/CFT Regime, the Joint Assessment Team from the World Bank and the Asia/Pacific Group on Money Laundering (APG), recommended, among others, that the *"AMLC should consider amending its requirement to allow only electronic transfer of STRs if an electronic signature is included"*. During the Plenary Meeting in Brisbane, Australia on 8 July 2009, the APG adopted the said MER.

Rule 9.3.b.2 of the Revised Implementing Rules and Regulations (RIRRs) of the Anti-Money Laundering Act of 2001 (AMLA), as amended, provides that "covered transaction reports and **suspicious transaction reports shall be submitted in a secured manner to the AMLC in electronic form,** either via diskettes, leased lines, or through internet facilities, **with the corresponding hard copy for suspicious transactions**" (emphasis supplied).

The AMLC, in its Resolution No. 408, Series of 2004, approved the implementation of the File Transfer and Reporting Facility (FTRF) which addresses the secure transfer of electronic reports from covered institutions to the AMLC's System. One of the security features of the FTRF is the **self-signed digital identification and certificate which allows the encrypting and the digital signing of messages.**

In the implementation of the FTRF, the AMLC and the covered institutions use Gnu Privacy Guard (GPG) Software, and the GPG supported algorithm (MD5) for the **encryption and authentication,** and the **digital signing of the electronic covered transaction reports and suspicious transaction reports (CTRs and STRs),** respectively. Upon installation of the said software, both the AMLC and the covered institutions generate their respective private and public keys, after which, the AMLC and the covered institutions exchange their public keys. The public keys of all covered institutions are stored in the AMLC's server. The AMLC's public key is in turn stored in the desktop of the covered institution which uses it in submitting CTRs and STRs.

Covered institutions use the public key of AMLC to encrypt the electronic file containing their CTRs and STRs which will be submitted to the AMLC. Before submitting the encrypted electronic file containing the CTRs and STRs, covered institutions will electronically or digitally sign the same using their private key.

Once the AMLC receives the encrypted electronic file containing CTRs and STRs, it will decrypt the same using its private key. The AMLC will verify the electronic or digital signature of the covered institutions by using the latter's public key.

It is worthy to note that under Section 1 (e), Rule 2 of the Rules on Electronic Evidence (A.M. 01-07-01), a **digital signature** is an *"electronic signature consisting of a transformation of an electronic document or an electronic data message using an asymmetric or public cryptosystem such that a person having the initial untransformed electronic document and the signer's public key can accurately determine:*

(i) whether the transformation was created using the private key that corresponds to the signer's key; and
(ii) whether the initial electronic document has been altered after the transformation was made."

Section 5 of Republic Act No. 8792 (RA 8792), otherwise known as the "Electronic Commerce Act", defines an **electronic signature** as referring to *"any distinctive mark, characteristics and/or sound in electronic form, representing the identity of a person and attached to or logically associated with the electronic data message or electronic document or any methodology or procedures employed or adopted by a person and executed or adopted by such person with the intention of authenticating or approving an electronic data message or electronic document".*

All the information contained in the hard copy of the STRs are the same as those contained in the electronic copy. Moreover, the submission of only the electronic copy of STRS would be cost-effective and more beneficial to covered institutions. Thus, such reports, STRs in particular, need not be submitted in hard copy. Furthermore, Section 2, Rule 3 of the Rules on Electronic Evidence provides that *"an electronic evidence is admissible in evidence if it complies with the rules on admissibility prescribed by the Rules of Court and related laws and is authenticated in the manner prescribed"* by the Rules on Electronic Evidence.

Section 10 (b) of the AMLA, as amended, in relation to Rules 9.2.a, 9.2.b and 9.2.c of its RIRRs, requires that *"all records of transactions of covered institutions shall be maintained and safely stored for five (5) years from the dates of transactions. With respect to closed accounts, the record on customer identification, account files and business correspondence, shall be preserved and safely stored for at least, five (5) years from the dates they were closed".* Rule 9.2.d of the RIRRs mandates that *"if a money laundering case based on any record kept by the covered institution concerned has been filed in court, said file must be retained beyond the period stipulated"* in Rules 9.2.a, 9.2.b and 9.2.c., as the case may be, *"until it is confirmed that the case has been finally resolved or terminated by the court".* In the same manner, the electronic copies of CTRs and STRs, must be preserved and safely stored for at least five (5) years from the dates the same were reported to the AMLC by covered institutions.

Foregoing considered, and pursuant to its power to implement such measures as may be necessary and justified to counteract money laundering (Section 7 [7] of the AMLA, as amended), the Council resolved to:

1. Direct covered institutions to defer, until further advice, the submission to the AMLC of the hard copies of their suspicious transaction reports;

2. Remind covered institutions that only their respective compliance officers or other duly authorized officers shall electronically sign their covered transaction reports and suspicious transaction reports;

3. Advise covered institutions to preserve and safely store the electronic copies of CTRs and STRs for at least five (5) years from the dates the same were reported to the AMLC; and

4. Request the Supervising Authorities to disseminate copies of this Resolution to the covered institutions under their respective jurisdictions.

17 August 2011, Manila, Philippines.

AMANDO M. TETANGCO, JR.
Chairman
(Governor, Bangko Sentral ng Pilipinas)

TERESITA J. HERBOSA
Member
(Chairperson, Securities and Exchange Commission)

EMMANUEL F. DOOC
Member
(Commissioner, Insurance Commission)