PLEASE ADDRESS CORRESPONDENCE TO:
THE HEAD OF THE SAMOA MONEY LAUNDERING PREVENTION AUTHORITY

PUBLIC NOTICE

BEWARE OF FRAUD AND SCAMS

The Central Bank is seriously concerned over the increased number of scam cases brought to its attention regarding Samoan residents being lured into believing that he or she is expecting to receive large sums of money from unknown sources communicated through ***the internet, emails or mobile phones***. And, with the improved and sophisticated application of modern computer and electronic technologies, the risk of Samoan residents and businesses becoming victims of these fraudulent activities has also increased.

The Central Bank wishes to remind the Public again that letters, emails or mobile phone messages, offering commissions or rewards on uncollected millions of dollars, or lotto winnings from overseas, or requesting for monetary assistance, are nothing but **SCAMS.**

Unfortunately, there are reports of some local people who have been adversely affected by these scams and have lost quite large of sums of money.

There are many variations of these scams. Basically, almost all of these scams promise millions of dollars/euros and require the victims to first provide up-front fees and other costs as well as some letters of support. ***Below are some examples:***

a) Email Scams:

- emails notifying the victim that he/she has won a large amount of price money in a lottery or online promotions or inherit large sums of funds;
- emails offering the victim a business proposal from a foreign partner to assist him/her in claiming the account and getting the funds or cash out of the country for investment purposes;
- emails requesting the victim for monetary assistance for his/her distressed relative or friend living overseas or out of the country temporarily.

b) Internet Banking Scams:

- emails with a local commercial bank logo instructing the bank customer to "*click to unlock your account"* that will automatically connect a bank customer to a different Website (not the bank's Website) and risk the security of customer information such as account number and other personal details;
- online scammers hacked into a bank customer account (victim) and transfer funds to another person's account (third party) and giving instructions for that person to keep ten (10) percent commission of the fund credited into his/her account and remit the remaining balance to its final destination through a money transfer operator;
- fraudsters (using facebook, bebo, etc) requesting the victim to provide his/her bank account details for funds to be remitted in and then demand the money to be sent through a money

transfer operator. (***NB: This is common using connections with students being targeted as mules and who lack knowledge or awareness of such fraudulent activities and amount of funds is usually in the vicinity of SAT$1,500).***

c) <u>Fake Foreign Cheques (e.g. Travellers cheques, Money Order, Bank Draft, etc):</u>

The fraudsters/scammers used fake foreign cheques to:

- make advanced payments (well in excess of the actual cost being incurred) for accommodations and/or other services and products being offered online, with specific instructions to the owners of these businesses to deduct their fees and remit back the remaining balance;
- make payment to a local firm as settlement of a debt to an unknown/mysterious person without any arrangements being made; and
- make payment to a local firm as settlement of a transaction or an agreement done in Europe/Asia/Africa with the same specific instructions to keep the 10% fee/commission and remit back the rest of the money.

d) <u>Online Sale Scams:</u>

- emails requesting the victim for payments of goods he/she has bought online from an unknown company offering lucrative deal.

In most of these cases, all the victim has to do is to take care of the endless fees these perpetrators or scammers come up with to cover for things like taxes, lawyer fees, insurance premiums or bank fees and he or she will reap millions in return. Usually, the fraudster demands urgency and confidentiality. In some cases, the fraudster requested the money to be sent through a **Money Transfer Operator (MTO) which he/she believes is the fastest and easiest way to send money.**

The Public is therefore advised to be alert and vigilant with these types of messages or proposals. The perpetrators are professionals. They will go to any length to produce **fake letterheads, invoices, cheques, personal letters or hack into email addresses to make their scams look convincing.**

In this regard, the Central Bank (**and also the Money Laundering Prevention Authority**) again strongly reminds members of the public to consult the Central Bank first before making any commitment in response to these fraudulent proposals or correspondence from overseas.

Remember, it is a breach of the prevailing Foreign Exchange legislations to participate and send funds overseas as payment for these illegal activities.

Maiava Atalina Ainu'u-Enari
<u>GOVERNOR AND</u>
<u>HEAD OF THE MONEY LAUNDERING PREVENTION AUTHORITY</u>

22 September 2013