



CENTRALE BANK VAN CURAÇAO EN SINT MAARTEN

Warning Notice – Circular – Advisory Fraudulent E-mails using forged internet banking sites of local banks hosted abroad for Phishing and Security Information Fraud Issued, November 2013

These Warnings contain the names of entities/persons and/or associates recently brought to the attention of the **Centrale Bank van Curaçao en Sint Maarten** (hereafter also: CBCS/Central Bank) through some form of notice, inquiry or complaint. If these entities and/or associates are operating in/or out of Curaçao or Sint Maarten, they may be violating provisions of the **Supervision Act or other financial regulation**,¹ thereby affecting the integrity of the financial sector.

A cumulative list of entities on previous Warning Circulars, Notices or Advisories is available on CBCS's website at <http://www.centralbank.an>.

Name and (Web) Address of Entity/Person	Name and (Web) Address of Associates (Entities/Persons)	Agency to contact with any further information
– Apparent legitimate websites abroad of local supervised banks		– Centrale Bank van Curaçao en Sint Maarten – Local police authority or your local banking institution

Case Description

This scam alert refers to the latest official-looking emails, using the Internet to obtain personal data and account information for fraudulent purposes. These fraudulent emails request you to login to an apparent legitimate but forged local banking website hosted abroad (a “spoof”

¹ Supervision Act covers, either jointly or separately, the 1994 National Ordinance on Supervision of the Banking and Credit System, 1990 National Ordinance on the Supervision of the Insurance Sector and their respective implementation decrees, the 1985 National Ordinance on the Supervision of Corporate Pension Funds, the 2003 National Ordinance on the Insurance Brokerage Business, the 1998 National Ordinance on the Supervision of Stock Exchanges, the 2002 National Ordinance on the Supervision of Investment Institutions and Administrators, the 2003 National Ordinance on the Supervision of Trust Service Providers, and also other and future supervisory regulations.



CENTRALE BANK VAN CURAÇAO EN SINT MAARTEN

website), thereby using certain specific personal information (PIN secret number or password).

Thus, spoof websites are fake websites that are directed to by phishing emails. These websites appear authentic but are, in fact, the mechanism for capturing your personal banking information in cyber space. These sites often contain incorrect grammar or spelling, which is usually an indication that they are not authentic sites.

The Central Bank strongly advises to be extra vigilant and to respond not whatsoever to these fraudulent email messages, fishing for sensitive personal information for obvious criminal reasons (called 'phishing'). Never click on a link in an email if you are unsure of its source, especially if the email asks for your personal financial information such as "*SignOn*" ID and "*SignOn*" Password. Also, the link in the email, asking your specific financial information, will not match with the URL of the site it takes you to.

Before submitting financial information through a website, confirm that you are on a secured web page:

- Look for the padlock in the lower right (Internet Explorer) corner of your browser window;
- Look in the address window above, the letters https:// should appear in front of the address of the form screen (instead of the non-secure http:// address)

The golden rule of thumb in this respect is that your specific personal data and account information should be exchanged directly between the bank and its clients, and not via email.

Centrale Bank van Curaçao en Sint Maarten
Unit Integrity Financial Sector
Simon Bolivar Plein 1
Willemstad, Curaçao

Tel. # 5999 9 434 5619/5500
Fax. No. # 599 9 461 5004