BANK VAN DE NEDERLANDSE ANTILLEN

Visa and MasterCard Holders Security Information Fraud Warning Notice – Circular – Advisory Issue No 4– Februarv 2004

These Warnings contain the names of entities/persons and/or associates recently brought to BNA's attention through some form of notice, inquiry or complaint. If these entities and/or associates are operating in/or out of the Netherlands Antilles, 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 BNA's website at **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
security@visa-security.com		Central Bank NA

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 Trust Service Providers, and also other and future supervisory regulations.**

BANK VAN DE NEDERLANDSE ANTILLEN

Case Description

This scam alert refers to the latest official-looking email (and/or phone) messages, using the Internet to obtain local (Visa and Master) cardholders personal data and account information for fraudulent purposes. These fraudulent messages have now also reached cardholders (including depositors of financial institutions) in the Netherlands Antilles. The message pretends to originate from an official-looking security and fraud department involved, saying your card has been flagged for an unusual purchase pattern and security information update has become necessary. The message will then direct you to an apparent legitimate website (a "spoof") and urge you to forward certain specific personal information (PIN secret number or password), so called to avoid and prevent any further fraud and billing mistakes and to refund your credit card. The Central Bank strongly advises cardholders not to respond whatsoever to these fraudulent messages, fishing for sensitive personal information for obvious criminal reasons (called 'phishing'). Please note that cardholders outside USA and Canada are normally not protected in the event of unauthorized card use (no Zero Liability Program applicable). Furthermore, the exchange of sensitive or payment (related) information via Internet is not recommended because of their vulnerable nature, unless secured by SSL, SET or any other Internet security program. The golden rule of thumb in this respect is that this information should be exchanged directly between you (as the cardholder) and your bank (the official card issuer) thereby using the security tools mentioned before. Intermediaries are therefore not allowed unless explicitly authorized by your bank.

Bank van de Nederlandse Antillen
Unit Integrity Financial Sector
Simon Bolivar Plein 1
Willemstad, Curaçao
Netherlands Antilles

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