THE CLEARING BANKS ASSOCIATION
FINANCIAL SERVICES - FRAUD AWARENESS
PART I

Recently there has been a surge of activity related to email spoofing, phishing and spam, involving the commercial bank customers within The Bahamas. The Clearing Banks Association would like to provide useful information on the subject and guidance on how incidences involving spoofing, phishing or spam should be handled.

Below are definitions for spoofing, phishing and spam:

- **Spoofing**
  Email spoofing is the forgery of an email header so that the message appears to have originated from someone or somewhere other than the actual source. Distributors of spam often use spoofing in an attempt to get recipients to open, and possibly even respond to, their solicitations. Look at the sender's email address not the "From" address displayed in the inbox. You can often identify malicious emails when the two are not consistent.

- **Phishing**
  The practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, online.

- **Spam**
  Irrelevant or unsolicited messages sent over the Internet, typically to large numbers of users, for the purposes of advertising, phishing, spreading malware, etc..

Don't unsubscribe from emails you didn't sign up for; it just reveals your email address is good.

THE CLEARING BANKS ASSOCIATION
FINANCIAL SERVICES - FRAUD AWARENESS (Continued)
PART 2

All of the activities of Spoofing, Phishing and Spamming schemes are intended to provide unsolicited information, obtain private information and/or spread viruses. Typically, fraudsters will send you an email with an attachment or a link. The email will appear to come from your bank and there is normally a request for personal information or give directions asking you to select the enclosed link or attachment to update account information.

Look for clues of a phishing message:

- General or missing greeting
- Typos and grammar mistakes
- Incorrect or confusing message
- Messages that direct you to do something
- Suspicious links (URLs)
- Email messages with missing recipient's address or aliased sender's address

Delete messages that:

- Ask for private information
- Look suspicious

Don't click on links (URLs) or call phone numbers provided in messages. Instead, look them up yourself.

Do not respond to any suspicious message or click on any links/attachments contained within one. If you have clicked on a link or opened an attachment, we advise you to go to your bank and change your account password/PIN immediately.

It is not a practice of any commercial bank in the country to request personal customer information via email. If you receive an email from your bank that looks suspicious, you should contact the bank immediately for guidance. Please ensure you use the contact information from the telephone directory or another reliable source. Contact numbers in the email may be fraudulent, and linked to persons perpetrating the scheme.

THE CLEARING BANKS ASSOCIATION
FIANCIAL SERVICES - FRAUD AWARENESS (Continued)
PART 3

Mystery Shopping Scam

The Mystery Shopping Scam is a scheme often used by fraudsters to gain the assistance of third party victims in money laundering. Phishing emails are used to recruit persons.

The scheme begins with an email or Facebook message offering you a job to carry out an evaluation of the services provided by a money transfer agent (such as Western Union or MoneyGram), on behalf of a Mystery Shopping company.

You are asked to confirm whether you have an account at a specific bank and also to provide your bank account number, phone number and a copy of a national ID (passport/Driver's license). Once you have confirmed your bank account number, you are told that monies will be sent to your account, of which you are to keep 10% and send the balance to the destination that the Mystery Shopping Company wants it sent to. Once the monies are credited to your account, you receive another communication (via Email, Facebook or WhatsApp) instructing you to send the money to a third party, usually located outside of the country.

The funds that are credited to your bank account are proceeds from a previous theft. If you withdraw the funds and send them out, you are liable and will have to pay the bank back. A money transfer can be paid out to the receiver within a very short time. After the money is paid, you generally cannot obtain a refund from a money transfer agent, even if the transfer was a result of fraud.

THE CLEARING BANKS ASSOCIATION
FINANCIAL SERVICES - FRAUD AWARENESS (Continued)
PART 4

Tips that can help you avoid falling victim to a mystery shopping scam:

- Beware of Mystery Shopper Offers received from unknown parties.
- **Do your research**. Most legitimate secret shopper jobs are posted online by reputable marketing research or merchandising companies.
- **Never wire money to someone you don't know**. Wiring money is the same as sending cash – once you send it, you can't get it back.
- **NEVER give your personal or financial information out online**. Guard your personal information, and treat it as if it were cash.

Continue to look for signs in your local branch and advertisements on your bank's online banking platform for updates and tips on how to keep your banking credentials safe.

By working together we can reduce financial services fraud.