Royal Bank

March 22, 2016

Dear Valued Client:

RBC is aware of ongoing attempts to fraudulently obtain banking information from personal and business clients of financial institutions through Phishing.

Phishing is the practice of sending phony e-mail messages designed to look legitimate. This tricks individuals into disclosing their confidential information which can lead to identity theft and online fraud.

At RBC, our priority is to protect your information and ensure the security of your financial transactions. As a client, in order to maximize your own online security it is crucial for you to always be informed.

A good rule of thumb is to be wary of unsolicited e-mails and telephone calls:

For e-mails: RBC will **NOT** send you an e-mail asking you to:

• Verify your account details or provide any confidential information online
• Update or log on to Online Banking through a link provided in the e-mail
• Provide your PASSWORD, USER ID or other CREDENTIALS

If you receive an e-mail request to provide confidential information – **DO NOT respond or click on any links provided.** Instead, please forward the e-mail to phishing@rbc.com.

For telephone calls: NEVER provide your confidential information.

• Instead ask the caller for a contact number and indicate that you will return the call – **DO NOT use the number provided by the caller,** but provide this information to us.

If you believe that your account or other confidential information has been compromised, please contact us IMMEDIATELY. We may also advise you to:

- Have your computer devices professionally checked for viruses
- Change your passwords
- Monitor your accounts

We hope that the information provided will assist in helping you to avoid potential dangers associated with identify theft and online fraud.

Tips to Protect Against Phishing

RBC has extensive resources to protect against Phishing and other types of fraud. For more information please visit our website at http://www.rbcroyalbank.com/caribbean/privacy-and-security/phishing-and-website-fraud.html.

Follow these tips to help you avoid falling victim to Phishing:

• Never provide your confidential information in response to unsolicited communications.

• **Play it safe!** If you don't know the source of an e-mail or if it looks suspicious, delete it.

• **Be cautious!** Even if you recognize a sender's e-mail address, always pay close attention to the contents of the e-mail as e-mail addresses can be faked.

• **Be alert!** Just because an e-mail or website appears to be from a legitimate company doesn't mean it is. If you are unsure that the website is valid do not sign in or enter any confidential information.

Tips to Protect Against Scams

It is important to be aware of a number of **Scams** that may be related to Phishing, as these may appear to provide opportunities to earn extra money but are not legitimate.

If it sounds too good to be true, it probably is.

Always ensure that any potential employers and requests are legitimate. Be wary of:

• Any job where you are asked to receive money in your bank account from unknown persons.

• Any requests to transfer money from one bank account to another.

• Being asked for your bank account number so that someone else's salary or money owing to them can be credited to your account.

• Instructions to wire funds to persons abroad.