McRAE CAPITAL MANAGEMENT, INC.

INVESTOR ALERT

Cyber Security: Recognizing Scams

These are four of the most common scams that we encounter. Be on the lookout for them, and be careful not to become a victim. Recovering from identity theft can be a long and challenging process.

Fraudulent Corporate Email Scam: There has been a rise in fraudulent emails that appear to come from well-known companies such as Chase, American Express or Amazon.com. These scams are often successful because emails appear to come from companies that you may use. The e-mail will most likely ask you to verify some information by clicking on a link or an attachment in the email. Some of these emails are VERY convincing. The sender's e-mail address will seem legitimate and the e-mail may include the corporate logo and even your name. As for Amazon.com, the email will state that an item, which you did not buy, has been shipped to an address that is not your own.

Our Tip: Resist the urge to click on a link or attachment in an email unless you are sure it is authentic. If you have any doubt, call the company directly and ask about the issue cited in the email. *Please note that the sender's address in the email may appear to come from the company.*

Continued on next page

Fraudulent Email from a Friend Scam: You may receive an email from a friend stating that he or she is in some kind of financial trouble, usually overseas, and needs money wired to a bank account immediately. In this case, your friend's email has been compromised and hackers are using the email to get you to reply. They will then converse with you as if they are your friend.

Our Tip: Remember, the phone is your friend. Call your friend to let them know you received this email and that their email has been compromised. Again, never click or respond to any email if you have a shred of doubt to its authenticity.

Phone Scams: You receive a phone call from an entity such as the phone company or a utility. There has been a widespread IRS phone scam going on recently. The person will tell you that if you do not clear up some issue immediately, your service will be discontinued or you will be audited. The goal is to have you give personal information to them over the phone.

Our Tip: Never give out information such as your Social Security number, account number, login or password if contacted by phone or email. No reputable organization will ever ask for this information in this manner. Find the company's phone number on a bill or website and call them back if you have any doubts.

Credit Card Scam: Someone gets your credit card number and starts making purchases. The hackers will often start with small, inconspicuous charges to see if you are paying attention.

Our Tip: Review your credit card statement frequently. If you have any concerns, call your credit card company immediately. If you shop on the internet, you may want to consider having a separate credit card for online shopping only.