## Cyber Crime Bulletin

As business practices and technology change over time, criminals adapt and develop new tactics to commit fraud. **“Social engineering”** is a type of fraud that has continued to impact businesses in our industry. These email scams frequently include fraudulent payment instructions posing as legitimate communications from someone with whom you have recently done business. Both auctions and dealers can suffer financial losses as a result of this scam.

Auctions should advise their customers to stay vigilant in assessing the validity of all emails, particularly those presenting payment instructions that are different than the payment instructions or methods typically used by the auction involved. Likewise, auctions should follow these same precautions regarding emails they receive from their customers.

**Here are some tips that both you and your customers can use to avoid falling for these scams:**

1. Verify any emails that contain payment requests or changes to payment instructions with a telephone call to a known contact at that business to confirm authenticity.

2. Check the email address and any hyperlinks for misspellings of known websites. For example, www.bankofarnerica.com – the “m” is really two characters: “r” and “n.”

3. Hover your mouse over any hyperlink that is displayed in the email message to ensure the link-to address is not for a different website than what is written.

Effectively preventing this type of fraud requires awareness and vigilance from both your business and your customers, so communication to your customers about this risk and how to avoid falling victim to it is key.