1. Automated Clearinghouse (ACH) Transactions.

   a. Automated Clearinghouse (ACH) transactions are increasingly becoming the preferred method of bill payment and are the next logical progression from wire transfers.

   b. With the advent of ACH transactions, there has been a corresponding rise in fraudulent transactions.

   c. ACH/Wire Transfer fraud occurs when employees are deceived by fraudulent vendors to wire/ACH to bank accounts that are controlled by the fraudulent actor(s).

      i. They use language that might be specific to the person or the company they are targeting and then request a fraudulent ACH/wire transfer using dollar amounts that would not be out of the ordinary based on the vendor.

      ii. These cybercriminals use phishing emails to gain access to email accounts, then leverage trusted relationships between individuals who authorize wire transfers/ACH transactions and those who send them out.

   d. To prevent ACH/Wire Transfer fraud, the following practices shall be employed by all employees granted ACH/Wire Transfer privileges:

      i. Always verify the authenticity of each wire transfer request. Call the person, using a number you have previously called — not one from the current wire transfer request! — to verbally verify it

      ii. A call-back verification process must be used when setting up payment instructions for a new vendor or making changes to payment instructions for an existing vendor

      iii. Implement dual control and segregation of duties. The Clerk/Treasurer should never be the primary source of ACH/Wire Transfer transactions; however, whenever the Clerk/Treasurer must make such transactions, the Utility Clerk or the Court Clerk must review each transaction.