UNITED BANK

Response Checklist

1. Recognize the signs of a cyberattack and know who to notify within your company
2. STOP, unplug the computer (including any wireless connections)
3. Contact United Bank
4. Work with us to:
   - Disable online access to accounts
   - Change online banking passwords
   - Open new accounts (if appropriate)
   - Reviews all recent transactions, identifying and canceling any suspicious active transactions
   - Ensure that no one has added any new payees, requested address or phone number changes, created any new accounts, changed access to any existing accounts, changed existing wire/ACH template profiles, changed PIN numbers or ordered new cards, checks or other account documents be sent to another address
5. Document the chronology of the events surrounding the loss
6. File a police report - for substantial losses contact the FBI at: www.fbi.gov/contact-us/field/field-offices
7. Contact your insurance company
8. Contact a forensic IT professional to locate and remove sophisticated malware
9. Consider whether other data may have been compromised
10. Incorporate “lessons learned” in future employee fraud training