Consumer Scam Prevention Checklist

- ☐ Don't respond to any email communications requesting money, private information, or asking you to make a purchase on behalf of someone else, especially if they include multiple typos or seem remotely fishy.
- ☐ Conduct your own research to validate the legitimacy of any business or person offering any kind of financial opportunity or product offering before making any purchase or supplying private information – i.e. perform an online search of the company's name and number, read online reviews about the company, etc.
- ☐ Delete any unexpected or suspicious emails asking you to open a link or attachment. If you recognize the sender's name, email/contact the person directly to validate the legitimacy of the initial request.
- ☐ Be extremely cautious of telephone calls where personal information is requested. If you receive such a call, hang-up and call your financial institution or the number on the reverse side of your credit or debit card.
- ☐ Do not send cash, gift cards, or wire money to any person or entity you do not know, because it's nearly impossible to trace or refund these payments.
- ☐ Review your account statements frequently, and quickly report any unknown or unauthorized activity to your financial institution or card processor.
- ☐ Work with your financial institution to setup multiple account access requirements – i.e. an access PIN, secret questions, or text/callback authorization.
- ☐ Use only traceable payment methods when making any kind of purchase online. These trusted methods include credit cards, debit cards, or a trusted mobile/online payment tool (i.e. PayPal or Apple Pay).
- ☐ Don't agree to deposit a check and/or wire money on anyone's behalf. Anyone who overpays with a check and requests that a portion of the funds be returned is almost certainly attempting fraud. If these checks turn out to be bogus, you will likely be held responsible for paying it back.
- ☐ Sign up for instant account notifications through your financial institution or a trust external resource (i.e. Mint), if available.
- ☐ Sign up for Identity Theft Protection through your financial institution, if available and if you are not already covered.
- ☐ Sign up for "FTC Consumer Alerts" to receive email updates with the latest scam attempts.
- ☐ Immediately contact your financial institution or call the number of the back of your credit or debit card to report any suspected scam or identity theft attempt.
- ☐ Consider also reporting scam or ID theft attempts to one of the following agencies:
    - ID theft, fraud, or scams of any kind: www.ftc.gov/complaint
    - International scams: www.econsumer.gov
    - Internet crimes: www.ic3.gov

Information in the checklist provided by Allied Solutions. This checklist is for information purposes only and is not to be considered legal advice.