

EDA DEALER UPDATE

HELP PROTECT YOUR DEALERSHIP EMPLOYEES AND CUSTOMERS FROM CORONAVIRUS-RELATED SCAMS

Several government agencies have released helpful information to the general public about ongoing scams in the wake of the Covid-19 pandemic. **EDA encourages equipment dealers, as employers and community leaders, to share these** resources with their dealership employees and customers to help stop these criminals from taking advantage of those in your community.

The <u>Federal Trade Commission</u> (FTC) has created a list of recommendations to help thwart scams. The FTC's resources include <u>an easy to print poster</u> that you can print for use around your dealership. While the guidance provided by the <u>FTC is extensive</u>, the following list is a summary of the FTC's advice for dealerships to utilize in educating employees and customers:

- Ignore offers for vaccinations and home test kits. There are no products
 proven to treat or prevent Covid-19 currently. Scammers are targeting Medicare
 recipients and asking for personal information such as bank accounts, social
 security numbers, Medicare numbers, etc. Medicare is not making any such calls
 and recipients of such calls are encouraged to report it immediately.
- 2. **Hang up on robocalls.** A robocall trying to sell you something is illegal unless a company has your written permission to call you that way. To get your permission, the company has to be clear it's asking to call you with robocalls, and it can't make you agree to the calls to get a product or service. If you give permission, you have the right to change your mind later.
- 3. Don't respond to texts, emails or calls about checks from the government. According to the FTC, as long as you filed taxes for 2018 and/or 2019, the federal government likely has the information it needs to send you your money. Social Security recipients and railroad retirees who are otherwise not required to file a tax return also do not need to do anything to receive their money.
- 4. Watch out for phishing emails and text messages. The FBI's Internet Crime Complaint Center reported that people lost \$57 million to phishing schemes in











<u>one year</u>. Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. They may:

- a. say they've noticed some suspicious activity or log-in attempts
- b. claim there's a problem with your account or your payment information
- c. say you must confirm some personal information
- d. include a fake invoice
- e. want you to click on a link to make a payment
- f. say you're eligible to register for a government refund
- g. offer a coupon for free stuff
- 5. **Research before you donate to a charitable organization.** Don't let anyone rush you into making a donation. That's something scammers do. When you consider giving to a specific charity, search its name plus "complaint," "review," "rating," or "scam."
- 6. Beware of emails claiming to be from the CDC or the WHO and don't click on links from sources you do not know. Use sites like <u>coronavirus.gov</u> and <u>usa.gov/coronavirus</u> to get the latest information.

Similar to the FTC, the Internal Revenue Services (IRS) has encouraged taxpayers to be on the lookout for IRS impersonation calls, texts and email phishing attempts about the coronavirus or COVID-19 Economic Impact Payments. These scams can lead to tax-related fraud and identity theft. The IRS' guidance, issued on April 16, 2020, is as follows:

Dealerships should ensure their employees and customers know that:

- The IRS will not call, email or text to verify or request financial, banking or personal information.
- Watch out for websites and social media attempts to request money or personal information. The official website is IRS.gov.
- Don't open surprise emails that look like they're coming from the IRS or click on attachments or links.
- Taxpayers should not provide personal or financial information or engage with potential scammers online or over the phone.
- Forward suspicious emails to phishing@irs.gov, then delete.
- Go to <u>IRS.gov</u> for the most up-to-date information.

With respect to the Economic Impact Payments:











- The IRS will automatically deposit Economic Impact Payments into the bank account taxpayers provided on their 2019 or 2018 tax return for a direct deposit of their tax refund.
- Those without a direct deposit account on file may be able to provide their banking information online through a new secure tool, Get My Payment.
- Anyone who is eligible for an Economic Impact Payment and doesn't provide direct deposit information will receive a payment mailed to the last address the IRS has on file.
- The IRS does not charge a fee to issue the payment.

Scammers may:

- Ask an individual to sign over their Economic Impact Payment check to them.
- Ask for verification of personal or banking information.
- Suggest that they can get someone tax refund or Economic Impact Payment faster by working on their behalf.
- Issue a bogus check, often in an odd amount, then tell a person to call a number or verify information online in order to cash it.

This update and other COVID-19 resources are a benefit of membership of the Equipment Dealers Association. A full list of resources for dealers can be found here. Remember, EDA Members also have access to our legal hotline. Natalie Higgins, EDA's general counsel, is a practicing labor and employment attorney who can assist dealers with implementation questions. Email Natalie at nhiggins@equipmentdealer.org.

Information Citations/Sources:

IRS Guidance on Covid Related Scams

FTC Guidance on Covid Related Scams







