



DenverDA

Mitchell R. Morrissey, District Attorney - Second Judicial District
201 W. Colfax Avenue, Dept. 801, Denver, CO 80202

Bus. Phone: 720-913-9000
Fax: 720-913-9035



Mitch Morrissey
Denver District Attorney

Returning a Rental Car? Don't Leave Your Personal Data Behind

photo credit Jeff Roberts



Rental cars can be fun, once you get past the paperwork. By now you are an experienced scam spotter, so you know that in order to protect yourself get everything in writing, take pictures of its condition, mark any places that might later look like a bump that you caused and, make sure all equipment is working before you drive away from the rental company. Once you are in the car, you can enjoy driving something you wouldn't normally own. Especially a car that has all the bells and whistles, like an infotainment system.

So you get in your cool rental, put the top down and plug your phone into the infotainment system. *Your* music at your finger tips, a navigation system and all of your contacts listed on the car console making it easy to call your friends with a touch of the button. No problem right? Well, not exactly.

This month's warning comes from the Federal Trade Commission which highlights the downside of so-called "connected cars." The gist of it is that today, a strange car is just like a strange computer, and consumers should be careful how they connect to them.

Here's the issue, once your phone is connected to the car, it can access all your phone's information such as GPS searches, home address, phone calls, contacts, etc. The information is stored indefinitely, waiting for the next person to connect to the car, and to your private information. The risk is obvious.

The FTC provides a few precautions that rental car customers should take to protect their privacy and still enjoy the fancy features of their rental:

- If you just need to charge your phone, avoid connecting to the infotainment center. It's safer to use a cigarette lighter adapter to charge phones and tablets, instead of a built in USB port. Some USB ports may connect to the infotainment center and transfer data automatically.
- Check your permissions when you connect. If you do want to connect your device to the infotainment system, the system may present a screen that lets you specify which types of information you want the system to access. Grant access only to the info you think is necessary.
- **Delete your data from the infotainment system before returning the car.** Before returning the vehicle, go into the infotainment system menu settings and find a list of devices that have been connected. Find your device and follow the system's instructions on how to delete the device. If you have questions about how to delete the mobile device, consult the owner's manual or call the rental company.

Now when you return a rental car, remember to fill up the tank, and take all your valuables from the car, including your personal data.



Need Help Spotting a Scam?

Spot Imposters.

Scammers often pretend to be someone you trust, like a government official, a family member, a charity, or a company you do business with. Don't send money or give out personal information in response to an unexpected request – whether it comes as a text, a phone call or an email.

Do online searches.

Type a company or product name into your favorite search engine with words like "review," "complaint" or "scam." Or search for a phrase that describes your situation, like "IRS call." You can even search for phone numbers to see if other people have reported them as scams.

Don't believe your caller ID.

Technology makes it easy for scammers to fake caller ID information, so the name and number you see aren't always real. If someone calls asking for money or personal information, hang up. If you think the caller might be telling the truth, call back to a number you know is genuine.

Don't pay upfront for a promise.

Someone might ask you to pay in advance for things like debt relief, credit and loan offers, mortgage assistance, or a job. They might even say you've won a prize, but first you have to pay taxes or fees. If you do, they will probably take the money and disappear. Learn where to get real help with these issues at consumer.ftc.gov

Consider how you pay.

Credit cards have significant fraud protection built in, but some payment methods don't. Wiring money through services like Western Union or MoneyGram is risky because it's nearly impossible to get your money back. That's also true for reloadable cards like MoneyPak, Reloadit or Vanilla. Government offices and honest companies won't require you to use these payment methods.

Talk to someone.

Before you give up your money or personal information, talk to someone you trust. Con artists want you to make decisions in a hurry. They might even threaten you. Slow down, check out the story, do an online search, consult an expert – or just tell a friend.

Hang up on robocalls.

If you answer the phone and hear a recorded sales pitch, hang up and report it to the FTC. These calls are illegal, and often the products are bogus. Don't press 1 to speak to a person or to be taken off the list. That could lead to more calls.

Be skeptical about free trial offers.

Some companies use free trials to sign you up for products and bill you every month until you cancel. Before you agree to a free trial, research the company and read the cancellation policy. And always review your monthly statements for charges you don't recognize.

Don't deposit a check and wire money back.

By law, banks must make funds from deposited checks available within days, but uncovering a fake check can take weeks. If a check you deposit turns out to be a fake, you're responsible for repaying the bank.



THINK YOU'VE BEEN SCAMMED?

If you suspect you've been scammed or exploited,
call our
Fraud Hot Line to report it.
720-913-9179

SCHEDULE A SPEAKER

Email me if you would like a Word document version of this newsletter. Interested in learning more about scams happening in Denver? Do you want to know how to protect yourself from identity theft? Maro Casparian is available for speaking engagements to any group or organization. Contact her at:



Maro Casparian

Director Consumer Protection 720-913-9036

Email amc@denverda.org to: Subscribe to this newsletter, schedule a presentation or to send suggestions for the next newsletter.

