**CLASS ACTION LAWSUIT FILED TO HOLD TOYOTA, FORD AND GM ACCOUNTABLE FOR DANGEROUS DEFECTS ALLOWING CARS TO BE HACKED AND DRIVERS TO LOSE CONTROL**

For Immediate Release
Tuesday, March 10, 2015

Contact: Melanie Sloan
(202) 365-0606

Today, Dallas-based trial attorney Marc R. Stanley filed a class action lawsuit against Toyota, Ford and General Motors for failing to address a defect that allows cars to be hacked and control wrested away from the driver. The case was filed in the United States District Court for the Northern District of California.

Car manufacturers long have known about the risks posed by this hazard. Last month, *60 Minutes* aired a segment demonstrating how a hacker using a laptop could disable the brakes, preventing a driver from stopping or slowing down.

Lead attorney Marc Stanley explained, "Toyota, Ford and GM have deliberately hidden the dangers associated with car computer systems, misleading consumers."

In today's cars, electronic control units (ECUs) are connected through a controller area network, referred to as a CAN or CAN bus. The ECUs communicate by sending CAN packets, which are digital messages containing small amounts of data. If a hacker can send a CAN packet to an ECU on the car's CAN bus, he can take control of basic functions of the car, including braking, steering and acceleration.

A 2013 study by the Defense Advanced Research Projects Agency (DARPA) found researchers could make vehicles "suddenly accelerate, turn, [and] kill the brakes." DARPA reported the defect represents a "real threat to the physical well being of drivers and passengers." Before releasing its study, DARPA shared its finding with car manufacturers so they could address the vulnerabilities, but they did nothing.

Senator Ed Markey (D-Mass) recently released a report, "Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk," noting that wireless technologies in cars represent "potential threats to both automobile security and to consumer privacy." Sen. Markey specifically asked numerous automobile manufacturers, including Toyota, Ford and GM, about how they were dealing with this defect, but found "a clear lack of appropriate security measures to protect drivers against hackers. . ."

Toyota owner and named plaintiff Helene Cahen said, "It's scary to know you could be driving down the highway and a hacker could seize control of your car. Toyota never mentions this risk when extolling its technology to sell you the car."

Among other things, the lawsuit alleges Toyota, Ford and GM concealed or suppressed material facts concerning the safety, quality and functionality of vehicles equipped with these systems. It charges the car companies with fraud, false advertising and violation of consumer protections statutes.

Stanley continued, "We shouldn't need to wait for a hacker or terrorist to prove exactly how dangerous this is before requiring car makers to fix the defect. Just as Honda has been forced to recall cars to repair potentially deadly airbags, Toyota, Ford and GM should be required to recall cars with these dangerous electronic systems."

Stanley is a founder of the Stanley Law Group, a law firm that focuses on complex litigation. He previously served as president of the Texas Trial Lawyers Association.

###