March 15, 2021

Docket Management Facility

US Department of Transportation

1200 New Jersey Avenue SE
West Building, Ground Floor, W12-140

Washington, DC 20590-0001

Attn: Cem Hatipoglu

Associate Administrator for Vehicle Safety Research

National Highway Traffic Safety Administration

**Cybersecurity Best Practices for the Safety of Modern Vehicles**

**Docket Number: NHTSA – 2020 – 0087**

Dear Associate Administrator Hatipoglu,

Since the 2016 publication of NHTSA’s “Cybersecurity Best Practices for Modern Vehicles” original equipment manufacturers have deployed new technologies improving cybersecurity but restricting legitimate repairs. Modern cybersecurity best practices must provide open access to legitimate repairs performed by automobile owners and the independent repair community. These groups maintain the vast majority of the nearly 300 million vehicles on America’s roads. We ask NHTSA to address legitimate third-party access, particularly in the context of vehicle repair, in the next publication of Cybersecurity Best Practices.

The Current Market Situation is Untenable

The current draft and prior Best Practices publications do not directly address our mutual concerns. The American public’s safety is at risk when legitimate repairs are blocked by cybersecurity barriers.

In 2017 a domestic OEM placed the first known cybersecure barrier on the OBDII port blocking advanced diagnostics to most repairers and virtually all consumers. Only after two years of difficult discussions, the OEM implemented a proprietary and expensive solution that is generally affordable to the professional repair community but continues to block the “do it yourself” segment of vehicle owners. Other OEMs followed suit by installing barriers on the OBDII port, including three Asian and one German manufacturer, but unlike the domestic OEM, the other four OEMs have yet to provide access. Currently there is no practical solution.[[1]](#footnote-1)

In closing the OBDII port to bi-directional diagnostic communication, advanced driver assistance (ADAS) systems cannot be calibrated and repairs including replacing anti-lock brake control modules cannot be programed by most independent repair shops unless proprietary and costly tools and software are purchased from OEMs. This ultimately jeopardizes the American public’s safety.

Additionally, virtually all original equipment manufacturers have deployed telematics systems containing vital vehicle operating data and justify their exclusive and proprietary wireless communication networks as essential for cybersecurity. Telematics contain vital information for remote detection of diagnostic information, including the status of safety critical systems and for real-time accident notification.

Going forward the repair community will likely face new cybersecurity barriers including encrypted data networks. Like telematics and the closing of the OBDII port, encryption without access for repair solves cybersecurity challenges but creates new ones that ultimately create safety concerns until solved.

Market forces alone will not solve this dilemma. To the contrary, market forces favor the continued deployment of proprietary systems closed for repair in serval ways. First closed and proprietary systems less expensive too design, deploy and administer. Second, they force consumers to purchase parts and services from franchised new car dealers economically benefiting vehicle manufacturers. Last and alarmingly, from a cybersecurity perspective, it is easier to meet industry best practices and NHTSA draft best practices without any consideration for repair over the lifetime of the vehicle.

We urge NHTSA to provide cybersecurity guidance recommending that OEMs offer access at a fair, reasonable, and non-discriminatory manner to the independent repair community and vehicle owners.

Recommended Best Practices

Proprietary and closed cybersecure systems create a safety risk. We strongly recommend NHTSA address these challenges with five best practices or policies to ensure vehicles remain open for repair:

* First, a self-governance structure is required to grant access rights to legitimate repairers and to administer open access policies.
* Access rights include standardized or harmonized technical and administrative processes. With over 7,000 year, make, model combinations sold over the past decade, the heterogeneity of vehicle population makes it impossible for third parties to conform to uncoordinated OEM processes and procedures to gain access through a potential myriad of cybersecure systems.
* The access rights must be provided on a fair, non-discriminatory basis. As a reference point, vehicle owners and third parties should pay the same costs for access as franchised new car dealers. Any bias, of any kind against legitimate repairs is not in the public’s interest.
* NHTSA should track vehicles that cannot be repaired or maintained by legitimate third parties and their owners. At a minimum the public has the right to be informed of cybersecurity barriers that prevent legitimate repairs.
* Highly automated vehicles deserve special attention in the context of repair and particularly to barriers to repair. Cybersecurity protecting their automated systems is vital, but if these systems cannot be maintained their efficacy erodes, and the public will be put at risk. Impediments to repair may also be barriers to any future periodic test and inspection program of automated safety and autonomous driving systems. These barriers should be known to NHTSA and public as special category of risk.

In developing cybersecurity best practices, we ask that NHTSA defend what the American public expects and from which it has benefited for more than a century, that vehicles remain open systems for repair. We recognize that cybersecurity creates new challenges, as its purpose is to block unauthorized access. That is why NHTSA’s best practices must support authorized, legitimate repairs to be conducted in a competitive environment that fosters innovation, convenience, and fair pricing. Without open systems for repair, cybersecurity barriers create a safety risk to the American public.

Regarding LKQ Corporation

LKQ Corporation is an S&P 500 and a Fortune 300 company based in Chicago. LKQ has over 20,000 employees and over 500 locations in the U.S, with 50,000 globally. LKQ distributes, through our 6,000-vehicle trucking fleet, automotive replacement parts for the repair of consumers’ vehicles. The vast majority of LKQ parts are new aftermarket parts or recycled, reconditioned, or remanufactured parts – all of which provide consumers lower-cost, high-quality alternatives to new OEM parts.

LKQ is also the largest provider of mobile diagnosticians in the United States. With over 100 vehicle diagnostic experts, repairing every conceivable year, make, model combination, our organization has first-hand knowledge of cybersecure barriers to legitimate repairs.

LKQ’s key principle is to support a vibrant, active aftermarket that provides consumers with choices in the parts they use to repair their cars, while maintaining the highest safety and quality standards.

Sincerely,



Ian Musselman

1. LKQ can provide specific company names upon request. [↑](#footnote-ref-1)