Video Statement
by the CEO of Allianz Versicherungs-AG
Frank Sommerfeld
for the **8th Allianz Motor Day Digital Live**
on **September 22, 2020**

A very warm welcome to our 8th Allianz Motor Day in its new digital format. Today we're looking at IT risks in cars as a connected ecosystem, and at how we, as insurers, are dealing with these new risks, both in Germany and throughout Europe.

Hacker attacks on connected mobility ecosystems are not an unrealistic scenario – quite the contrary. We've already seen high-profile examples where hackers have been able to get access to individual vehicles and entire fleets while being parked and even while driving. Fortunately, these were so-called "white hat" hackers, who intend to detect a system's security vulnerabilities, and not to harm the respective drivers.

Luckily, cyberattacks have not played any role in causing traffic accidents so far. Allianz has not had to pay claims for any accident that was evidently caused by a hacker attack. However, as vehicles become increasingly connected and automated, the risks of cyberattacks on them will become more and more significant. The insurance industry has neither put a comprehensive or uniform figure on these new risks, nor even fully calculated them out. Not in Germany, and not in the rest of Europe. To make cyberrisks calculable for everyone involved, and thus insurable, it's important to look carefully at IT security and cybersecurity for connected vehicles.

Any new technology entails risks, and any new technology can also result in damage. We as insurers have the important job of safeguarding those who are affected by such cases. If you think about it, many new technologies would not exist today if the resulting risks had not been recognized and ultimately been covered by appropriate insurance. Insurability runs up against its limits when an event affects not just individuals, but potentially everybody who's insured. In the insurance industry, we call this an accumulation risk, in which the insurance system no longer works properly because everyone insured is suffering a loss simultaneously.

Concerning cyberrisk, connected vehicles in particular raise the question of where the limits of insurability lie. It’s not impossible that a single hacker could attack all the vehicles of a particular type with the mere touch of a button. We see comparable risks with classic computer viruses, and in cyberattacks on non-mobile systems like computer centers. What we’d like to discuss with you today at our 8th Allianz Motor Day is how we’re dealing with these novel risks.

As an insurer, we distinguish between several different risk scenarios associated with hacker attacks:

1. Hackers use electronic means to manipulate the access system and the immobilizer in order to **steal** the vehicle.

2. A vehicle gets hacked, and at first the only result is **a disruption of function** – for example to extract money by blackmail.

3. A hacker attack causes **an accident** that may result in damage to the vehicle and even injure people.

A **theft** enabled by a hacker attack is not just a future possibility but already a reality. Within this scenario a hacker finds a way to develop tools that can circumvent the vehicle’s electronic key.

A further already realistic scenario are hacker attacks, which cause **malfunctions in the vehicle**.. There are a variety of motives for this – sometimes it’s to detect security vulnerabilities, but sometimes it’s also to blackmail the manufacturer. The hackers then demand a cyber-ransom to let the vehicle run again, just as it has already been known from other sectors of industry.

But these two examples imply nothing worse than damage to the system or hardware, along with the technical and financial expenditure to fix the problem. Things become more drastic when there’s a danger to the life and limb of occupants or others on the road because the hacker attack results in **an accident**. Just imagine that a hacker virus takes over a car’s system and tells the braking assist system that an obstacle has suddenly appeared. The vehicle brakes while it’s running full speed down the freeway, and thus causes an accident involving many injuries and a great deal of property damage.

That risk could grow significantly if the hacker attack doesn't just involve a single vehicle, but is able to affect all the vehicles of a certain type simultaneously; and possibly not just regionally in one city, but all over Europe, or even all around the world.

So what does insurance coverage look like for these scenarios? The good news is, insurance can cover almost all the potential financial consequences I've just mentioned.

If a hacker attack causes an **accident** that injures people and damages one's own vehicle or someone else's, generally all of the Allianz Group's European subsidiaries provide insurance coverage, and vehicle insurance takes care of the financial loss – there's no general exclusion for hacking. **Motor liability insurance** will compensate for property damage or bodily injury to third parties or the vehicle's own occupants. Damage to the driver's own vehicle is included within motor hull insurance **policies**.

If a hacker attack enables a **vehicle theft**, standard partial-coverage policies cover this in most countries, including Germany.

The picture is somewhat different if a hacker attack results only in a software-induced **malfunction** of the vehicle. In **Germany,** Allianz additionally covers damage to software. For one year it has treated functional disruptions caused by a hacker the same as other forms of vandalism that are included under **motor hull insurance policies**. So in Germany, it no longer makes any difference to us whether a third party maliciously scratches up a vehicle, or attacks the vehicle by hacking its software, and damages it in that way; and fixing such malfunctions can get expensive. If the IT system has been infiltrated, the software has to be reloaded, and in some car models, according to the manufacturer's specifications, a whole string of control devices has to be replaced. The cost for that can quickly rise to the order of several thousand euros.

On the other hand, if there's an attack on the servers or the digital platform of a **vehicle manufacturer** that communicates with the vehicle, and the attack disrupts functions on multiple vehicles or even all the vehicles of a certain type, the responsibility falls on the manufacturer. Ensuring that produced cars' electronics operate properly for the long term, and protecting them from attack, lies within the manufacturer's sphere of risk.

Again, if these systematic functional disruptions from a cyberattack result in traffic accidents, we would cover that as the insurers. As you can see – in motor insurance, the focus is on protecting the victim of an accident. If accidents occur, if people are injured and vehicles are damaged, we insurers cover the loss.

Although some of these risks have fortunately not become a practical reality yet, at Allianz we firmly believe that motor insurance products all over Europe should focus more fully on these new **collective cyberrisks**. In addition to complex databases, this requires above all experience. In order to build up and expand both, we rely on our own technical investigations in our Allianz Center for Technology (AZT) as well as on further interdisciplinary exchange with vehicle manufacturers, suppliers, politics and science. We do this consistently in order to identify risks and potential dangers in good time, to improve risk prevention and to establish an appropriate response capability to claims events.

Mobility behavior is already changing today. New concepts in movement play a key role in planning a “Smart City.” Autonomous buses and taxis as well as driverless trucks are intrinsic to those plans. However, people will entrust themselves to automated, or even driverless, vehicles only if they can trust that those vehicles are adequately protected from hacking, and that any harm will be covered.

Thank you for your attention, and I hope you’ll enjoy an informative and fascinating Allianz Motor Day.