United States Senate

July 20, 2022

Sebastian Mackensen
Chief Executive Officer
BMW of North America, LLC
300 Chestnut Ridge Road
Woodcliff Lake, NJ 07675

Dear Mr. Mackensen,

I write to request information about the security of BMW's motor vehicle keyless entry systems. Keyless entry systems — which allow users to enter a vehicle and start its engine without inserting and turning a key — likely helped reduce vehicle thefts since the 1990s, but the dramatic 30-year decline has suddenly gone into reverse. Although the exact cause of this turnaround is unclear, a growing body of evidence suggests that keyless entry systems may play a role. We therefore urge BMW to take all necessary steps to ensure that keyless entry systems, once a security innovation that deterred thieves, do not become a security liability for them to exploit.

After their adoption in the 1990s, keyless entry systems contributed to the impressive decline in car thefts from 1990 to 2019. These systems come in different forms. Some simply allow the driver to enter a vehicle without inserting a physical key into the door lock, while others, called passive entry systems, allow the driver to start the vehicle without inserting a physical key into the ignition. In both cases, the vehicle and a key fob communicate through radio signals, and an "engine immobilizer" prevents the vehicle from starting unless the key fob is nearby.

These systems were a critical advancement in vehicle security. Old-fashioned "hotwiring" a vehicle — that is, bypassing the ignition and starting a vehicle without a key — became far more difficult; with keyless entry systems, cars would not start unless they detected, through the radio signals, the presence of the key fob. In 1995, the European Union required manufacturers to include engine immobilizers on all new vehicles within three years, and Australia and Canada passed similar laws soon thereafter. One study estimated that the EU mandate reduced vehicle thefts in the Netherlands from 1995 to 2008 by 40 percent.[1] The United States never imposed a similar requirement, but many manufacturers have voluntarily adopted keyless entry systems, and car thefts per capita decreased by two-thirds from 1990 to 2019.[2]

---

[1] Jan C. van Ours and Ben Vollaard, *The Engine Immobiliser: A Non-Starter for Car Thieves*, 126 ECON. J. 1264, 1266 (2016), https://onlinelibrary.wiley.com/doi/abs/10.1111/ecoj.12196.

[2] Crime Data Explorer, FED. BUREAU OF INVESTIGATIONS, https://crime-data-explorer.app.cloud.gov/pages/explorer/crime/crime-trend (select "1990" in "From" and "2019" in "To" and "Motor vehicle theft" in "Crime Select").

Although this decrease tracked the overall decline in violent and property crime,[3] news reports have nevertheless attributed part of the decline to the adoption of keyless ignitions.[4]

This remarkably consistent trend towards fewer vehicle thefts, however, has made a concerning U-turn since the end of 2019. According to data compiled by the Federal Bureau of Investigation (FBI), U.S. car thefts per capita increased nationally by 11.8 percent in 2020.[5] Although national data has not yet been released for 2021, news reports suggest that car thefts continued to accelerate across the country last year. For example, in 2021, the number of car thefts appears to have increased by 132 percent in Milwaukee,[6] 70 percent in Washington, DC,[7] and 60 percent in Philadelphia.[8] This trend appears to have continued into 2022. So far this year, as compared with the same period in 2021, the number of car thefts has increased 74 percent in Portland, Ore.,[9] 54 percent in Richmond, Va.,[10] and 51 percent in New York City.[11] After so many years of progress, this rapid reversal in car thefts is alarming.

The same keyless entry systems that contributed to the decline in car thefts may now be providing an opportunity for thieves. Keyless entry systems are vulnerable in two ways. First, drivers may leave their key fobs in their cars, allowing a thief to easily start and steal a vehicle.[12] Whereas drivers used to have to remove the physical key from the ignition when they exited the vehicle, no similar action is necessary when a driver need only push a button to start or stop an engine. According to the New York Police Department, roughly 40 percent of car thefts in New York City so far this year were the result of motorists leaving their vehicles running or unlocked, often with keys or a key fob inside.[13] Keyless technology has thus escalated the consequences of ordinary human error.

---

[3] *Id.* (select "All Property Crimes" or "All Violent Crimes" in "Crime Select").

[4] *See, e.g.,* Sarah Maslin Nir, *Here's Why Car Thefts Are Soaring (Hint: Check Your Cup Holder)*, N.Y. TIMES (Jan. 6, 2021), www.nytimes.com/2021/01/06/nyregion/car-thefts-nyc.html; Brad Stone, *Pinch My Ride*, Wired (Aug. 1, 2006), www.wired.com/2006/08/carkey/.

[5] Crime Data Explorer, *supra* note 3 (select "2019" in "From" and "2020" in "To" and "Motor vehicle theft" in "Crime Select").

[6] *See* Teddy Nykiel, *Over 500% Spike in Auto Thefts Troubles Downtown*, MILWAUKEE BUS. J. (Feb. 9, 2022), https://www.bizjournals.com/milwaukee/news/2022/02/09/crime-statistics-mpd-2021-car-lefts.html.

[7] *See* Bruce Leshan, *Surge in Carjackings, Car Thefts Has Police Struggling to Respond*, WUSA (Feb. 9, 2021), www.wusa9.com/article/news/crime/surge-in-carjackings-car-thefts-dc-police-form-task-force/65-8c4b0c03-e343-430e-9c77-c5d9daade558.

[8] *See* Chad Pradelli and Cheryl Mettendorf, *Action News Investigation into Rise of Dealership Auto Thefts in Philadelphia Region*, ABC ACTION NEWS (Jan. 14, 2022), 6abc.com/car-thefts-auto-dealerships-6abc-investigation-barbera-autoland/11464047/.

[9] *See* Stolen Vehicle Statistics, CITY OF PORTLAND, https://www.portlandoregon.gov/police/74369 (compare selecting Jan. – May 2022 with Jan. – May 2021 in "Filter by Reported Date of Theft").

[10] *See* Henry Graff, *Richmond Police See 54% Increase in Vehicle Thefts Over Last Year*, NBC12 (Apr. 7, 2022), www.nbc12.com/2022/04/07/richmond-police-see-54-increase-vehicle-thefts-over-last-year/.

[11] *See* Rocco Parascandola, *NYPD Reports 51% Surge in Stolen Cars This Year*, N.Y. DAILY NEWS (June 12, 2022), www.nydailynews.com/new-york/nyc-crime/ny-car-vehicle-theft-surge-careless-motorists-nypd-20220612-eojbb2hhx5a3tn34vzhilc2fdq-story.html.

[12] *See* Nathan Bomey, *Thieves strike: Auto Theft Spikes During the Pandemic as Cars Are Left Unattended*, USA TODAY (Aug. 31, 2021), usatoday.com/story/money/cars/2021/08/31/auto-theft-spikes-stolen-car-vehicle-theft-pandemic-nicb/5652615001/.

[13] Rocco Parascandola, *supra* note 11.

Second, and perhaps more worryingly, a common type of keyless entry system that allows a driver to unlock and start the vehicle without needing to touch the key — known as a passive entry system — appear to be vulnerable to a "relay attack," in which a thief uses a signal amplifier to fool the car into believing that the owner is nearby.[14] Researchers have long known that bad actors could amplify radio signals emitted from the vehicle and key, allowing them to enter and start a vehicle even if the fob is nowhere nearby.[15] In recent years, devices that enable relay attacks have become widely available,[16] and news reports have identified thefts involving relay attacks in Austin,[17] Cincinnati,[18] and Los Angeles.[19]

More recently, researchers have shown that carmakers that use Bluetooth Low Energy (BLE) entry systems — which uses Bluetooth technology to determine whether the vehicle is within a certain distance of the connected device — are also vulnerable to theft using similar relay technology, affecting manufacturers such as Tesla that have adopted BLE passive entry systems.[20] For that reason, the Bluetooth Special Interest Group, the standard-setting organization that oversees the development of Bluetooth technologies, warns that BLE "should not be used as the only protection of valuable assets."[21] Car manufacturers have only recently begun using BLE technology to determine the proximity of a key fob, so researchers have not yet confirmed any vehicles stolen through a BLE relay attack. However, as manufacturers increasingly equip devices — such as smart locks for homes[22] — with BLE passive entry systems, this vulnerability could put a broad range of critical security systems at risk.

Fortunately, researchers have also identified methods to mitigate the risk of passive entry thefts. For example, manufacturers can prevent a fob from unlocking a vehicle if the fob was not recently in motion, as typically occurs as a driver approaches a vehicle. In other words, if the fob is idle, the driver is likely not trying to unlock their own vehicle; any attempt to use the fob in that state may be a sign of a relay attack. Similarly, manufacturers could require consumers to complete an additional verification, such as inputting a PIN number, to enter the vehicle. While such systems inherently inconvenience consumers, they also are a strong defense against relay

---

[14] Rachel Wait, *Keyless Car Crime: How to Thwart the Thieves*, FORBES ADVISOR (Mar. 24, 2022), www.forbes.com/uk/advisor/car-insurance/keyless-car-crime/.

[15] *See* ARI JUELS, RFID SECURITY AND PRIVACY: A RESEARCH SURVEY 13 (2005), www.arijuels.com/wp-content/uploads/2013/09/J06a.pdf.

[16] *See* Joseph Cox, *Meet the Guy Selling Wireless Tech to Steal Luxury Cars in Seconds*, VICE NEWS (Feb. 11, 2020), www.vice.com/en/article/7kz48x/guy-selling-relay-attack-keyless-repeaters-to-steal-cars.

[17] *See* Bettie Cross, *Car Thieves Are Hacking Key Fobs to Quickly and Quietly Steal Vehicles*, CBS AUSTIN (May 12, 2022), cbsaustin.com/news/local/car-thieves-are-hacking-key-fobs-to-quickly-and-quietly-steal-vehicles.

[18] *See* Jatara McGee, *Hackers Are Using New Tech to Steal Locked Cars Without Keys*, WLWT (May 9, 2019), www.wlwt.com/article/hackers-are-using-new-tech-to-steal-locked-cars-without-keys/27424367#.

[19] *See* Nick Bilton, *Keeping Your Car Safe From Electronic Thieves*, N.Y. TIMES (Apr. 15, 2015), www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html.

[20] *See* Sultan Khan, *Technical Advisory – Tesla BLE Phone-as-a-Key Passive Entry Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-tesla-ble-phone-as-a-key-passive-entry-vulnerable-to-relay-attacks/.

[21] BLUETOOTH SIG, PROXIMITY PROFILE 17 (2015), www.bluetooth.com/specifications/specs/proximity-profile-1-0-1/.

[22] *See* Sultan Khan, *Technical Advisory – Kwikset/Weiser BLE Proximity Authentication in Kevo Smart Locks Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-kwikset-weiser-ble-proximity-authentication-in-kevo-smart-locks-vulnerable-to-relay-attacks/.

attacks. Finally, automakers could also adopt Ultra-Wide-Band (UWB) technology, which enables a precise measurement between the vehicle and key fob and, in combination with other technologies, allows the vehicle to determine if the radio signal has been improperly amplified. Experts have suggested that UWB technology could significantly reduce the risk of relay theft.[23]

Given the recent surge in vehicle thefts and the potential security risks involved in keyless entry systems, I respectfully request that you respond in writing to the following questions by August 10, 2022:

1. Please provide the following data, as available, on thefts of vehicles manufactured by your company:

    a. How many vehicles manufactured by your company were stolen in 2019, 2020, 2021, and through the first six months of 2022?

    b. Of those vehicle thefts, how many were caused by thieves taking advantage of key fobs left in vehicles?

    c. Of those vehicle thefts, how many were caused by relay attacks?

2. Please describe the type of transponder and the technology standard that vehicles manufactured by your company use to communicate with key fobs and other devices. If vehicles manufactured by your company use different types of transponders and technology standards, please provide information on all types.

3. Please describe the testing that your company has done to assess the security of its keyless entry systems.

4. What specific steps has your company taken to reduce the vulnerability of its keyless entry system?

    a. Has your company considered making the keyless entry system motion activated?

    b. Has your company considered adopting Ultra-Wide-Band technology?

    c. Has your company considered creating mechanisms to alert owners if their key fob is left inside the vehicle?

5. Does your company plan to take any further steps to reduce any vulnerability of its keyless entry system?

Thank you for your prompt attention to these questions.

---

[23] *See e.g.,* Mridula Singh et al., *UWB with Pulse Reordering: Securing Ranging against Relay and Physical-Layer Attacks*, NETWORK AND DISTRIB. SYS, SEC. SYMP. (2019), www.ndss-symposium.org/ndss-paper/uwb-with-pulse-reordering-securing-ranging-against-relay-and-physical-layer-attacks/.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

July 20, 2022

James D. Farley, Jr.
President and Chief Executive Officer
Ford Motor Company
One American Road
Dearborn, MI 48126

Dear Mr. Farley,

I write to request information about the security of Ford's motor vehicle keyless entry systems. Keyless entry systems — which allow users to enter a vehicle and start its engine without inserting and turning a key — likely helped reduce vehicle thefts since the 1990s, but the dramatic 30-year decline has suddenly gone into reverse. Although the exact cause of this turnaround is unclear, a growing body of evidence suggests that keyless entry systems may play a role. We therefore urge Ford to take all necessary steps to ensure that keyless entry systems, once a security innovation that deterred thieves, do not become a security liability for them to exploit.

After their adoption in the 1990s, keyless entry systems contributed to the impressive decline in car thefts from 1990 to 2019. These systems come in different forms. Some simply allow the driver to enter a vehicle without inserting a physical key into the door lock, while others, called passive entry systems, allow the driver to start the vehicle without inserting a physical key into the ignition. In both cases, the vehicle and a key fob communicate through radio signals, and an "engine immobilizer" prevents the vehicle from starting unless the key fob is nearby.

These systems were a critical advancement in vehicle security. Old-fashioned "hotwiring" a vehicle — that is, bypassing the ignition and starting a vehicle without a key — became far more difficult; with keyless entry systems, cars would not start unless they detected, through the radio signals, the presence of the key fob. In 1995, the European Union required manufacturers to include engine immobilizers on all new vehicles within three years, and Australia and Canada passed similar laws soon thereafter. One study estimated that the EU mandate reduced vehicle thefts in the Netherlands from 1995 to 2008 by 40 percent.[1] The United States never imposed a similar requirement, but many manufacturers have voluntarily adopted keyless entry systems, and car thefts per capita decreased by two-thirds from 1990 to 2019.[2]

---

[1] Jan C. van Ours and Ben Vollaard, *The Engine Immobiliser: A Non-Starter for Car Thieves*, 126 ECON. J. 1264, 1266 (2016), https://onlinelibrary.wiley.com/doi/abs/10.1111/ecoj.12196.

[2] Crime Data Explorer, FED. BUREAU OF INVESTIGATIONS, https://crime-data-explorer.app.cloud.gov/pages/explorer/crime/crime-trend (select "1990" in "From" and "2019" in "To" and "Motor vehicle theft" in "Crime Select").

Although this decrease tracked the overall decline in violent and property crime,[3] news reports have nevertheless attributed part of the decline to the adoption of keyless ignitions.[4]

This remarkably consistent trend towards fewer vehicle thefts, however, has made a concerning U-turn since the end of 2019. According to data compiled by the Federal Bureau of Investigation (FBI), U.S. car thefts per capita increased nationally by 11.8 percent in 2020.[5] Although national data has not yet been released for 2021, news reports suggest that car thefts continued to accelerate across the country last year. For example, in 2021, the number of car thefts appears to have increased by 132 percent in Milwaukee,[6] 70 percent in Washington, DC,[7] and 60 percent in Philadelphia.[8] This trend appears to have continued into 2022. So far this year, as compared with the same period in 2021, the number of car thefts has increased 74 percent in Portland, Ore.,[9] 54 percent in Richmond, Va.,[10] and 51 percent in New York City.[11] After so many years of progress, this rapid reversal in car thefts is alarming.

The same keyless entry systems that contributed to the decline in car thefts may now be providing an opportunity for thieves. Keyless entry systems are vulnerable in two ways. First, drivers may leave their key fobs in their cars, allowing a thief to easily start and steal a vehicle.[12] Whereas drivers used to have to remove the physical key from the ignition when they exited the vehicle, no similar action is necessary when a driver need only push a button to start or stop an engine. According to the New York Police Department, roughly 40 percent of car thefts in New York City so far this year were the result of motorists leaving their vehicles running or unlocked, often with keys or a key fob inside.[13] Keyless technology has thus escalated the consequences of ordinary human error.

---

[3] *Id.* (select "All Property Crimes" or "All Violent Crimes" in "Crime Select").

[4] *See, e.g.,* Sarah Maslin Nir, *Here's Why Car Thefts Are Soaring (Hint: Check Your Cup Holder)*, N.Y. TIMES (Jan. 6, 2021), www.nytimes.com/2021/01/06/nyregion/car-thefts-nyc.html; Brad Stone, *Pinch My Ride*, Wired (Aug. 1, 2006), www.wired.com/2006/08/carkey/.

[5] Crime Data Explorer, *supra* note 3 (select "2019" in "From" and "2020" in "To" and "Motor vehicle theft" in "Crime Select").

[6] *See* Teddy Nykiel, *Over 500% Spike in Auto Thefts Troubles Downtown*, MILWAUKEE BUS. J. (Feb. 9, 2022), https://www.bizjournals.com/milwaukee/news/2022/02/09/crime-statistics-mpd-2021-car-lefts.html.

[7] *See* Bruce Leshan, *Surge in Carjackings, Car Thefts Has Police Struggling to Respond*, WUSA (Feb. 9, 2021), www.wusa9.com/article/news/crime/surge-in-carjackings-car-thefts-dc-police-form-task-force/65-8c4b0c03-e343-430e-9c77-c5d9daade558.

[8] *See* Chad Pradelli and Cheryl Mettendorf, *Action News Investigation into Rise of Dealership Auto Thefts in Philadelphia Region*, ABC ACTION NEWS (Jan. 14, 2022), 6abc.com/car-thefts-auto-dealerships-6abc-investigation-barbera-autoland/11464047/.

[9] *See* Stolen Vehicle Statistics, CITY OF PORTLAND, https://www.portlandoregon.gov/police/74369 (compare selecting Jan. – May 2022 with Jan. – May 2021 in "Filter by Reported Date of Theft").

[10] *See* Henry Graff, *Richmond Police See 54% Increase in Vehicle Thefts Over Last Year*, NBC12 (Apr. 7, 2022), www.nbc12.com/2022/04/07/richmond-police-see-54-increase-vehicle-thefts-over-last-year/.

[11] *See* Rocco Parascandola, *NYPD Reports 51% Surge in Stolen Cars This Year*, N.Y. DAILY NEWS (June 12, 2022), www.nydailynews.com/new-york/nyc-crime/ny-car-vehicle-theft-surge-careless-motorists-nypd-20220612-eojbb2hhx5a3tn34vzhilc2fdq-story.html.

[12] *See* Nathan Bomey, *Thieves strike: Auto Theft Spikes During the Pandemic as Cars Are Left Unattended*, USA TODAY (Aug. 31, 2021), usatoday.com/story/money/cars/2021/08/31/auto-theft-spikes-stolen-car-vehicle-theft-pandemic-nicb/5652615001/.

[13] Rocco Parascandola, *supra* note 11.

Second, and perhaps more worryingly, a common type of keyless entry system that allows a driver to unlock and start the vehicle without needing to touch the key — known as a passive entry system — appear to be vulnerable to a "relay attack," in which a thief uses a signal amplifier to fool the car into believing that the owner is nearby.[14] Researchers have long known that bad actors could amplify radio signals emitted from the vehicle and key, allowing them to enter and start a vehicle even if the fob is nowhere nearby.[15] In recent years, devices that enable relay attacks have become widely available,[16] and news reports have identified thefts involving relay attacks in Austin,[17] Cincinnati,[18] and Los Angeles.[19]

More recently, researchers have shown that carmakers that use Bluetooth Low Energy (BLE) entry systems — which uses Bluetooth technology to determine whether the vehicle is within a certain distance of the connected device — are also vulnerable to theft using similar relay technology, affecting manufacturers such as Tesla that have adopted BLE passive entry systems.[20] For that reason, the Bluetooth Special Interest Group, the standard-setting organization that oversees the development of Bluetooth technologies, warns that BLE "should not be used as the only protection of valuable assets."[21] Car manufacturers have only recently begun using BLE technology to determine the proximity of a key fob, so researchers have not yet confirmed any vehicles stolen through a BLE relay attack. However, as manufacturers increasingly equip devices — such as smart locks for homes[22] — with BLE passive entry systems, this vulnerability could put a broad range of critical security systems at risk.

Fortunately, researchers have also identified methods to mitigate the risk of passive entry thefts. For example, manufacturers can prevent a fob from unlocking a vehicle if the fob was not recently in motion, as typically occurs as a driver approaches a vehicle. In other words, if the fob is idle, the driver is likely not trying to unlock their own vehicle; any attempt to use the fob in that state may be a sign of a relay attack. Similarly, manufacturers could require consumers to complete an additional verification, such as inputting a PIN number, to enter the vehicle. While such systems inherently inconvenience consumers, they also are a strong defense against relay

---

[14] Rachel Wait, *Keyless Car Crime: How to Thwart the Thieves*, FORBES ADVISOR (Mar. 24, 2022), www.forbes.com/uk/advisor/car-insurance/keyless-car-crime/.

[15] *See* ARI JUELS, RFID SECURITY AND PRIVACY: A RESEARCH SURVEY 13 (2005), www.arijuels.com/wp-content/uploads/2013/09/J06a.pdf.

[16] *See* Joseph Cox, *Meet the Guy Selling Wireless Tech to Steal Luxury Cars in Seconds*, VICE NEWS (Feb. 11, 2020), www.vice.com/en/article/7kz48x/guy-selling-relay-attack-keyless-repeaters-to-steal-cars.

[17] *See* Bettie Cross, *Car Thieves Are Hacking Key Fobs to Quickly and Quietly Steal Vehicles*, CBS AUSTIN (May 12, 2022), cbsaustin.com/news/local/car-thieves-are-hacking-key-fobs-to-quickly-and-quietly-steal-vehicles.

[18] *See* Jatara McGee, *Hackers Are Using New Tech to Steal Locked Cars Without Keys*, WLWT (May 9, 2019), www.wlwt.com/article/hackers-are-using-new-tech-to-steal-locked-cars-without-keys/27424367#.

[19] *See* Nick Bilton, *Keeping Your Car Safe From Electronic Thieves*, N.Y. TIMES (Apr. 15, 2015), www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html.

[20] *See* Sultan Khan, *Technical Advisory – Tesla BLE Phone-as-a-Key Passive Entry Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-tesla-ble-phone-as-a-key-passive-entry-vulnerable-to-relay-attacks/.

[21] BLUETOOTH SIG, PROXIMITY PROFILE 17 (2015), www.bluetooth.com/specifications/specs/proximity-profile-1-0-1/.

[22] *See* Sultan Khan, *Technical Advisory – Kwikset/Weiser BLE Proximity Authentication in Kevo Smart Locks Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-kwikset-weiser-ble-proximity-authentication-in-kevo-smart-locks-vulnerable-to-relay-attacks/.

attacks. Finally, automakers could also adopt Ultra-Wide-Band (UWB) technology, which enables a precise measurement between the vehicle and key fob and, in combination with other technologies, allows the vehicle to determine if the radio signal has been improperly amplified. Experts have suggested that UWB technology could significantly reduce the risk of relay theft.[23]

Given the recent surge in vehicle thefts and the potential security risks involved in keyless entry systems, I respectfully request that you respond in writing to the following questions by August 10, 2022:

1. Please provide the following data, as available, on thefts of vehicles manufactured by your company:

    a. How many vehicles manufactured by your company were stolen in 2019, 2020, 2021, and through the first six months of 2022?

    b. Of those vehicle thefts, how many were caused by thieves taking advantage of key fobs left in vehicles?

    c. Of those vehicle thefts, how many were caused by relay attacks?

2. Please describe the type of transponder and the technology standard that vehicles manufactured by your company use to communicate with key fobs and other devices. If vehicles manufactured by your company use different types of transponders and technology standards, please provide information on all types.

3. Please describe the testing that your company has done to assess the security of its keyless entry systems.

4. What specific steps has your company taken to reduce the vulnerability of its keyless entry system?

    a. Has your company considered making the keyless entry system motion activated?

    b. Has your company considered adopting Ultra-Wide-Band technology?

    c. Has your company considered creating mechanisms to alert owners if their key fob is left inside the vehicle?

5. Does your company plan to take any further steps to reduce any vulnerability of its keyless entry system?

Thank you for your prompt attention to these questions.

---

[23] *See e.g.,* Mridula Singh et al., *UWB with Pulse Reordering: Securing Ranging against Relay and Physical-Layer Attacks*, NETWORK AND DISTRIB. SYS, SEC. SYMP. (2019), www.ndss-symposium.org/ndss-paper/uwb-with-pulse-reordering-securing-ranging-against-relay-and-physical-layer-attacks/.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

July 20, 2022

Mary Barra
Chair and Chief Executive Officer
General Motors Company
300 Renaissance Center
Detroit, MI 48265

Dear Ms. Barra,

I write to request information about the security of General Motor's motor vehicle keyless entry systems. Keyless entry systems — which allow users to enter a vehicle and start its engine without inserting and turning a key — likely helped reduce vehicle thefts since the 1990s, but the dramatic 30-year decline has suddenly gone into reverse. Although the exact cause of this turnaround is unclear, a growing body of evidence suggests that keyless entry systems may play a role. We therefore urge General Motors to take all necessary steps to ensure that keyless entry systems, once a security innovation that deterred thieves, do not become a security liability for them to exploit.

After their adoption in the 1990s, keyless entry systems contributed to the impressive decline in car thefts from 1990 to 2019. These systems come in different forms. Some simply allow the driver to enter a vehicle without inserting a physical key into the door lock, while others, called passive entry systems, allow the driver to start the vehicle without inserting a physical key into the ignition. In both cases, the vehicle and a key fob communicate through radio signals, and an "engine immobilizer" prevents the vehicle from starting unless the key fob is nearby.

These systems were a critical advancement in vehicle security. Old-fashioned "hotwiring" a vehicle — that is, bypassing the ignition and starting a vehicle without a key — became far more difficult; with keyless entry systems, cars would not start unless they detected, through the radio signals, the presence of the key fob. In 1995, the European Union required manufacturers to include engine immobilizers on all new vehicles within three years, and Australia and Canada passed similar laws soon thereafter. One study estimated that the EU mandate reduced vehicle thefts in the Netherlands from 1995 to 2008 by 40 percent.[1] The United States never imposed a similar requirement, but many manufacturers have voluntarily adopted keyless entry systems, and car thefts per capita decreased by two-thirds from 1990 to 2019.[2]

---

[1] Jan C. van Ours and Ben Vollaard, *The Engine Immobiliser: A Non-Starter for Car Thieves*, 126 ECON. J. 1264, 1266 (2016), https://onlinelibrary.wiley.com/doi/abs/10.1111/ecoj.12196.

[2] Crime Data Explorer, FED. BUREAU OF INVESTIGATIONS, https://crime-data-explorer.app.cloud.gov/pages/explorer/crime/crime-trend (select "1990" in "From" and "2019" in "To" and "Motor vehicle theft" in "Crime Select").

Although this decrease tracked the overall decline in violent and property crime,[3] news reports have nevertheless attributed part of the decline to the adoption of keyless ignitions.[4]

This remarkably consistent trend towards fewer vehicle thefts, however, has made a concerning U-turn since the end of 2019. According to data compiled by the Federal Bureau of Investigation (FBI), U.S. car thefts per capita increased nationally by 11.8 percent in 2020.[5] Although national data has not yet been released for 2021, news reports suggest that car thefts continued to accelerate across the country last year. For example, in 2021, the number of car thefts appears to have increased by 132 percent in Milwaukee,[6] 70 percent in Washington, DC,[7] and 60 percent in Philadelphia.[8] This trend appears to have continued into 2022. So far this year, as compared with the same period in 2021, the number of car thefts has increased 74 percent in Portland, Ore.,[9] 54 percent in Richmond, Va.,[10] and 51 percent in New York City.[11] After so many years of progress, this rapid reversal in car thefts is alarming.

The same keyless entry systems that contributed to the decline in car thefts may now be providing an opportunity for thieves. Keyless entry systems are vulnerable in two ways. First, drivers may leave their key fobs in their cars, allowing a thief to easily start and steal a vehicle.[12] Whereas drivers used to have to remove the physical key from the ignition when they exited the vehicle, no similar action is necessary when a driver need only push a button to start or stop an engine. According to the New York Police Department, roughly 40 percent of car thefts in New York City so far this year were the result of motorists leaving their vehicles running or unlocked, often with keys or a key fob inside.[13] Keyless technology has thus escalated the consequences of ordinary human error.

---

[3] *Id.* (select "All Property Crimes" or "All Violent Crimes" in "Crime Select").

[4] *See, e.g.,* Sarah Maslin Nir, *Here's Why Car Thefts Are Soaring (Hint: Check Your Cup Holder)*, N.Y. TIMES (Jan. 6, 2021), www.nytimes.com/2021/01/06/nyregion/car-thefts-nyc.html; Brad Stone, *Pinch My Ride*, Wired (Aug. 1, 2006), www.wired.com/2006/08/carkey/.

[5] Crime Data Explorer, *supra* note 3 (select "2019" in "From" and "2020" in "To" and "Motor vehicle theft" in "Crime Select").

[6] *See* Teddy Nykiel, *Over 500% Spike in Auto Thefts Troubles Downtown*, MILWAUKEE BUS. J. (Feb. 9, 2022), https://www.bizjournals.com/milwaukee/news/2022/02/09/crime-statistics-mpd-2021-car-lefts.html.

[7] *See* Bruce Leshan, *Surge in Carjackings, Car Thefts Has Police Struggling to Respond*, WUSA (Feb. 9, 2021), www.wusa9.com/article/news/crime/surge-in-carjackings-car-thefts-dc-police-form-task-force/65-8c4b0c03-e343-430e-9c77-c5d9daade558.

[8] *See* Chad Pradelli and Cheryl Mettendorf, *Action News Investigation into Rise of Dealership Auto Thefts in Philadelphia Region*, ABC ACTION NEWS (Jan. 14, 2022), 6abc.com/car-thefts-auto-dealerships-6abc-investigation-barbera-autoland/11464047/.

[9] *See* Stolen Vehicle Statistics, CITY OF PORTLAND, https://www.portlandoregon.gov/police/74369 (compare selecting Jan. – May 2022 with Jan. – May 2021 in "Filter by Reported Date of Theft").

[10] *See* Henry Graff, *Richmond Police See 54% Increase in Vehicle Thefts Over Last Year*, NBC12 (Apr. 7, 2022), www.nbc12.com/2022/04/07/richmond-police-see-54-increase-vehicle-thefts-over-last-year/.

[11] *See* Rocco Parascandola, *NYPD Reports 51% Surge in Stolen Cars This Year*, N.Y. DAILY NEWS (June 12, 2022), www.nydailynews.com/new-york/nyc-crime/ny-car-vehicle-theft-surge-careless-motorists-nypd-20220612-eojbb2hhx5a3tn34vzhilc2fdq-story.html.

[12] *See* Nathan Bomey, *Thieves strike: Auto Theft Spikes During the Pandemic as Cars Are Left Unattended*, USA TODAY (Aug. 31, 2021), usatoday.com/story/money/cars/2021/08/31/auto-theft-spikes-stolen-car-vehicle-theft-pandemic-nicb/5652615001/.

[13] Rocco Parascandola, *supra* note 11.

Second, and perhaps more worryingly, a common type of keyless entry system that allows a driver to unlock and start the vehicle without needing to touch the key — known as a passive entry system — appear to be vulnerable to a "relay attack," in which a thief uses a signal amplifier to fool the car into believing that the owner is nearby.[14] Researchers have long known that bad actors could amplify radio signals emitted from the vehicle and key, allowing them to enter and start a vehicle even if the fob is nowhere nearby.[15] In recent years, devices that enable relay attacks have become widely available,[16] and news reports have identified thefts involving relay attacks in Austin,[17] Cincinnati,[18] and Los Angeles.[19]

More recently, researchers have shown that carmakers that use Bluetooth Low Energy (BLE) entry systems — which uses Bluetooth technology to determine whether the vehicle is within a certain distance of the connected device — are also vulnerable to theft using similar relay technology, affecting manufacturers such as Tesla that have adopted BLE passive entry systems.[20] For that reason, the Bluetooth Special Interest Group, the standard-setting organization that oversees the development of Bluetooth technologies, warns that BLE "should not be used as the only protection of valuable assets."[21] Car manufacturers have only recently begun using BLE technology to determine the proximity of a key fob, so researchers have not yet confirmed any vehicles stolen through a BLE relay attack. However, as manufacturers increasingly equip devices — such as smart locks for homes[22] — with BLE passive entry systems, this vulnerability could put a broad range of critical security systems at risk.

Fortunately, researchers have also identified methods to mitigate the risk of passive entry thefts. For example, manufacturers can prevent a fob from unlocking a vehicle if the fob was not recently in motion, as typically occurs as a driver approaches a vehicle. In other words, if the fob is idle, the driver is likely not trying to unlock their own vehicle; any attempt to use the fob in that state may be a sign of a relay attack. Similarly, manufacturers could require consumers to complete an additional verification, such as inputting a PIN number, to enter the vehicle. While such systems inherently inconvenience consumers, they also are a strong defense against relay

---

[14] Rachel Wait, *Keyless Car Crime: How to Thwart the Thieves*, FORBES ADVISOR (Mar. 24, 2022), www.forbes.com/uk/advisor/car-insurance/keyless-car-crime/.

[15] *See* ARI JUELS, RFID SECURITY AND PRIVACY: A RESEARCH SURVEY 13 (2005), www.arijuels.com/wp-content/uploads/2013/09/J06a.pdf.

[16] *See* Joseph Cox, *Meet the Guy Selling Wireless Tech to Steal Luxury Cars in Seconds*, VICE NEWS (Feb. 11, 2020), www.vice.com/en/article/7kz48x/guy-selling-relay-attack-keyless-repeaters-to-steal-cars.

[17] *See* Bettie Cross, *Car Thieves Are Hacking Key Fobs to Quickly and Quietly Steal Vehicles*, CBS AUSTIN (May 12, 2022), cbsaustin.com/news/local/car-thieves-are-hacking-key-fobs-to-quickly-and-quietly-steal-vehicles.

[18] *See* Jatara McGee, *Hackers Are Using New Tech to Steal Locked Cars Without Keys*, WLWT (May 9, 2019), www.wlwt.com/article/hackers-are-using-new-tech-to-steal-locked-cars-without-keys/27424367#.

[19] *See* Nick Bilton, *Keeping Your Car Safe From Electronic Thieves*, N.Y. TIMES (Apr. 15, 2015), www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html.

[20] *See* Sultan Khan, *Technical Advisory – Tesla BLE Phone-as-a-Key Passive Entry Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-tesla-ble-phone-as-a-key-passive-entry-vulnerable-to-relay-attacks/.

[21] BLUETOOTH SIG, PROXIMITY PROFILE 17 (2015), www.bluetooth.com/specifications/specs/proximity-profile-1-0-1/.

[22] *See* Sultan Khan, *Technical Advisory – Kwikset/Weiser BLE Proximity Authentication in Kevo Smart Locks Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-kwikset-weiser-ble-proximity-authentication-in-kevo-smart-locks-vulnerable-to-relay-attacks/.

attacks. Finally, automakers could also adopt Ultra-Wide-Band (UWB) technology, which enables a precise measurement between the vehicle and key fob and, in combination with other technologies, allows the vehicle to determine if the radio signal has been improperly amplified. Experts have suggested that UWB technology could significantly reduce the risk of relay theft.[23]

Given the recent surge in vehicle thefts and the potential security risks involved in keyless entry systems, I respectfully request that you respond in writing to the following questions by August 10, 2022:

1. Please provide the following data, as available, on thefts of vehicles manufactured by your company:

    a. How many vehicles manufactured by your company were stolen in 2019, 2020, 2021, and through the first six months of 2022?

    b. Of those vehicle thefts, how many were caused by thieves taking advantage of key fobs left in vehicles?

    c. Of those vehicle thefts, how many were caused by relay attacks?

2. Please describe the type of transponder and the technology standard that vehicles manufactured by your company use to communicate with key fobs and other devices. If vehicles manufactured by your company use different types of transponders and technology standards, please provide information on all types.

3. Please describe the testing that your company has done to assess the security of its keyless entry systems.

4. What specific steps has your company taken to reduce the vulnerability of its keyless entry system?

    a. Has your company considered making the keyless entry system motion activated?

    b. Has your company considered adopting Ultra-Wide-Band technology?

    c. Has your company considered creating mechanisms to alert owners if their key fob is left inside the vehicle?

5. Does your company plan to take any further steps to reduce any vulnerability of its keyless entry system?

Thank you for your prompt attention to these questions.

---

[23] *See e.g.,* Mridula Singh et al., *UWB with Pulse Reordering: Securing Ranging against Relay and Physical-Layer Attacks*, NETWORK AND DISTRIB. SYS, SEC. SYMP. (2019), www.ndss-symposium.org/ndss-paper/uwb-with-pulse-reordering-securing-ranging-against-relay-and-physical-layer-attacks/.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

July 20, 2022

Noriya Kaihara
President and Chief Executive Officer
American Honda Motor Co., Inc.
1919 Torrance Blvd
Torrance, CA 90501

Dear Mr. Kaihara,

I write to request information about the security of Honda's motor vehicle keyless entry systems. Keyless entry systems — which allow users to enter a vehicle and start its engine without inserting and turning a key — likely helped reduce vehicle thefts since the 1990s, but the dramatic 30-year decline has suddenly gone into reverse. Although the exact cause of this turnaround is unclear, a growing body of evidence suggests that keyless entry systems may play a role. We therefore urge Honda to take all necessary steps to ensure that keyless entry systems, once a security innovation that deterred thieves, do not become a security liability for them to exploit.

After their adoption in the 1990s, keyless entry systems contributed to the impressive decline in car thefts from 1990 to 2019. These systems come in different forms. Some simply allow the driver to enter a vehicle without inserting a physical key into the door lock, while others, called passive entry systems, allow the driver to start the vehicle without inserting a physical key into the ignition. In both cases, the vehicle and a key fob communicate through radio signals, and an "engine immobilizer" prevents the vehicle from starting unless the key fob is nearby.

These systems were a critical advancement in vehicle security. Old-fashioned "hotwiring" a vehicle — that is, bypassing the ignition and starting a vehicle without a key — became far more difficult; with keyless entry systems, cars would not start unless they detected, through the radio signals, the presence of the key fob. In 1995, the European Union required manufacturers to include engine immobilizers on all new vehicles within three years, and Australia and Canada passed similar laws soon thereafter. One study estimated that the EU mandate reduced vehicle thefts in the Netherlands from 1995 to 2008 by 40 percent.[1] The United States never imposed a similar requirement, but many manufacturers have voluntarily adopted keyless entry systems, and car thefts per capita decreased by two-thirds from 1990 to 2019.[2]

---

[1] Jan C. van Ours and Ben Vollaard, *The Engine Immobiliser: A Non-Starter for Car Thieves*, 126 ECON. J. 1264, 1266 (2016), https://onlinelibrary.wiley.com/doi/abs/10.1111/ecoj.12196.

[2] Crime Data Explorer, FED. BUREAU OF INVESTIGATIONS, https://crime-data-explorer.app.cloud.gov/pages/explorer/crime/crime-trend (select "1990" in "From" and "2019" in "To" and "Motor vehicle theft" in "Crime Select").

Although this decrease tracked the overall decline in violent and property crime,[3] news reports have nevertheless attributed part of the decline to the adoption of keyless ignitions.[4]

This remarkably consistent trend towards fewer vehicle thefts, however, has made a concerning U-turn since the end of 2019. According to data compiled by the Federal Bureau of Investigation (FBI), U.S. car thefts per capita increased nationally by 11.8 percent in 2020.[5] Although national data has not yet been released for 2021, news reports suggest that car thefts continued to accelerate across the country last year. For example, in 2021, the number of car thefts appears to have increased by 132 percent in Milwaukee,[6] 70 percent in Washington, DC,[7] and 60 percent in Philadelphia.[8] This trend appears to have continued into 2022. So far this year, as compared with the same period in 2021, the number of car thefts has increased 74 percent in Portland, Ore.,[9] 54 percent in Richmond, Va.,[10] and 51 percent in New York City.[11] After so many years of progress, this rapid reversal in car thefts is alarming.

The same keyless entry systems that contributed to the decline in car thefts may now be providing an opportunity for thieves. Keyless entry systems are vulnerable in two ways. First, drivers may leave their key fobs in their cars, allowing a thief to easily start and steal a vehicle.[12] Whereas drivers used to have to remove the physical key from the ignition when they exited the vehicle, no similar action is necessary when a driver need only push a button to start or stop an engine. According to the New York Police Department, roughly 40 percent of car thefts in New York City so far this year were the result of motorists leaving their vehicles running or unlocked, often with keys or a key fob inside.[13] Keyless technology has thus escalated the consequences of ordinary human error.

---

[3] *Id.* (select "All Property Crimes" or "All Violent Crimes" in "Crime Select").

[4] *See, e.g.,* Sarah Maslin Nir, *Here's Why Car Thefts Are Soaring (Hint: Check Your Cup Holder)*, N.Y. TIMES (Jan. 6, 2021), www.nytimes.com/2021/01/06/nyregion/car-thefts-nyc.html; Brad Stone, *Pinch My Ride*, Wired (Aug. 1, 2006), www.wired.com/2006/08/carkey/.

[5] Crime Data Explorer, *supra* note 3 (select "2019" in "From" and "2020" in "To" and "Motor vehicle theft" in "Crime Select").

[6] *See* Teddy Nykiel, *Over 500% Spike in Auto Thefts Troubles Downtown*, MILWAUKEE BUS. J. (Feb. 9, 2022), https://www.bizjournals.com/milwaukee/news/2022/02/09/crime-statistics-mpd-2021-car-lefts.html.

[7] *See* Bruce Leshan, *Surge in Carjackings, Car Thefts Has Police Struggling to Respond*, WUSA (Feb. 9, 2021), www.wusa9.com/article/news/crime/surge-in-carjackings-car-thefts-dc-police-form-task-force/65-8c4b0c03-e343-430e-9c77-c5d9daade558.

[8] *See* Chad Pradelli and Cheryl Mettendorf, *Action News Investigation into Rise of Dealership Auto Thefts in Philadelphia Region*, ABC ACTION NEWS (Jan. 14, 2022), 6abc.com/car-thefts-auto-dealerships-6abc-investigation-barbera-autoland/11464047/.

[9] *See* Stolen Vehicle Statistics, CITY OF PORTLAND, https://www.portlandoregon.gov/police/74369 (compare selecting Jan. – May 2022 with Jan. – May 2021 in "Filter by Reported Date of Theft").

[10] *See* Henry Graff, *Richmond Police See 54% Increase in Vehicle Thefts Over Last Year*, NBC12 (Apr. 7, 2022), www.nbc12.com/2022/04/07/richmond-police-see-54-increase-vehicle-thefts-over-last-year/.

[11] *See* Rocco Parascandola, *NYPD Reports 51% Surge in Stolen Cars This Year*, N.Y. DAILY NEWS (June 12, 2022), www.nydailynews.com/new-york/nyc-crime/ny-car-vehicle-theft-surge-careless-motorists-nypd-20220612-eojbb2hhx5a3tn34vzhilc2fdq-story.html.

[12] *See* Nathan Bomey, *Thieves strike: Auto Theft Spikes During the Pandemic as Cars Are Left Unattended*, USA TODAY (Aug. 31, 2021), usatoday.com/story/money/cars/2021/08/31/auto-theft-spikes-stolen-car-vehicle-theft-pandemic-nicb/5652615001/.

[13] Rocco Parascandola, *supra* note 11.

Second, and perhaps more worryingly, a common type of keyless entry system that allows a driver to unlock and start the vehicle without needing to touch the key — known as a passive entry system — appear to be vulnerable to a "relay attack," in which a thief uses a signal amplifier to fool the car into believing that the owner is nearby.[14] Researchers have long known that bad actors could amplify radio signals emitted from the vehicle and key, allowing them to enter and start a vehicle even if the fob is nowhere nearby.[15] In recent years, devices that enable relay attacks have become widely available,[16] and news reports have identified thefts involving relay attacks in Austin,[17] Cincinnati,[18] and Los Angeles.[19]

More recently, researchers have shown that carmakers that use Bluetooth Low Energy (BLE) entry systems — which uses Bluetooth technology to determine whether the vehicle is within a certain distance of the connected device — are also vulnerable to theft using similar relay technology, affecting manufacturers such as Tesla that have adopted BLE passive entry systems.[20] For that reason, the Bluetooth Special Interest Group, the standard-setting organization that oversees the development of Bluetooth technologies, warns that BLE "should not be used as the only protection of valuable assets."[21] Car manufacturers have only recently begun using BLE technology to determine the proximity of a key fob, so researchers have not yet confirmed any vehicles stolen through a BLE relay attack. However, as manufacturers increasingly equip devices — such as smart locks for homes[22] — with BLE passive entry systems, this vulnerability could put a broad range of critical security systems at risk.

Fortunately, researchers have also identified methods to mitigate the risk of passive entry thefts. For example, manufacturers can prevent a fob from unlocking a vehicle if the fob was not recently in motion, as typically occurs as a driver approaches a vehicle. In other words, if the fob is idle, the driver is likely not trying to unlock their own vehicle; any attempt to use the fob in that state may be a sign of a relay attack. Similarly, manufacturers could require consumers to complete an additional verification, such as inputting a PIN number, to enter the vehicle. While such systems inherently inconvenience consumers, they also are a strong defense against relay

---

[14] Rachel Wait, *Keyless Car Crime: How to Thwart the Thieves*, FORBES ADVISOR (Mar. 24, 2022), www.forbes.com/uk/advisor/car-insurance/keyless-car-crime/.

[15] *See* ARI JUELS, RFID SECURITY AND PRIVACY: A RESEARCH SURVEY 13 (2005), www.arijuels.com/wp-content/uploads/2013/09/J06a.pdf.

[16] *See* Joseph Cox, *Meet the Guy Selling Wireless Tech to Steal Luxury Cars in Seconds*, VICE NEWS (Feb. 11, 2020), www.vice.com/en/article/7kz48x/guy-selling-relay-attack-keyless-repeaters-to-steal-cars.

[17] *See* Bettie Cross, *Car Thieves Are Hacking Key Fobs to Quickly and Quietly Steal Vehicles*, CBS AUSTIN (May 12, 2022), cbsaustin.com/news/local/car-thieves-are-hacking-key-fobs-to-quickly-and-quietly-steal-vehicles.

[18] *See* Jatara McGee, *Hackers Are Using New Tech to Steal Locked Cars Without Keys*, WLWT (May 9, 2019), www.wlwt.com/article/hackers-are-using-new-tech-to-steal-locked-cars-without-keys/27424367#.

[19] *See* Nick Bilton, *Keeping Your Car Safe From Electronic Thieves*, N.Y. TIMES (Apr. 15, 2015), www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html.

[20] *See* Sultan Khan, *Technical Advisory – Tesla BLE Phone-as-a-Key Passive Entry Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-tesla-ble-phone-as-a-key-passive-entry-vulnerable-to-relay-attacks/.

[21] BLUETOOTH SIG, PROXIMITY PROFILE 17 (2015), www.bluetooth.com/specifications/specs/proximity-profile-1-0-1/.

[22] *See* Sultan Khan, *Technical Advisory – Kwikset/Weiser BLE Proximity Authentication in Kevo Smart Locks Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-kwikset-weiser-ble-proximity-authentication-in-kevo-smart-locks-vulnerable-to-relay-attacks/.

attacks. Finally, automakers could also adopt Ultra-Wide-Band (UWB) technology, which enables a precise measurement between the vehicle and key fob and, in combination with other technologies, allows the vehicle to determine if the radio signal has been improperly amplified. Experts have suggested that UWB technology could significantly reduce the risk of relay theft.[23]

Given the recent surge in vehicle thefts and the potential security risks involved in keyless entry systems, I respectfully request that you respond in writing to the following questions by August 10, 2022:

1. Please provide the following data, as available, on thefts of vehicles manufactured by your company:

    a. How many vehicles manufactured by your company were stolen in 2019, 2020, 2021, and through the first six months of 2022?

    b. Of those vehicle thefts, how many were caused by thieves taking advantage of key fobs left in vehicles?

    c. Of those vehicle thefts, how many were caused by relay attacks?

2. Please describe the type of transponder and the technology standard that vehicles manufactured by your company use to communicate with key fobs and other devices. If vehicles manufactured by your company use different types of transponders and technology standards, please provide information on all types.

3. Please describe the testing that your company has done to assess the security of its keyless entry systems.

4. What specific steps has your company taken to reduce the vulnerability of its keyless entry system?

    a. Has your company considered making the keyless entry system motion activated?

    b. Has your company considered adopting Ultra-Wide-Band technology?

    c. Has your company considered creating mechanisms to alert owners if their key fob is left inside the vehicle?

5. Does your company plan to take any further steps to reduce any vulnerability of its keyless entry system?

Thank you for your prompt attention to these questions.

---

[23] *See e.g.,* Mridula Singh et al., *UWB with Pulse Reordering: Securing Ranging against Relay and Physical-Layer Attacks*, NETWORK AND DISTRIB. SYS, SEC. SYMP. (2019), www.ndss-symposium.org/ndss-paper/uwb-with-pulse-reordering-securing-ranging-against-relay-and-physical-layer-attacks/.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

July 20, 2022

José Muñoz
President and Chief Executive Officer
Hyundai Motor America, Inc.
10550 Talbert Avenue
Fountain Valley, CA 92708

Dear Mr. Muñoz,

I write to request information about the security of Hyundai's motor vehicle keyless entry systems. Keyless entry systems — which allow users to enter a vehicle and start its engine without inserting and turning a key — likely helped reduce vehicle thefts since the 1990s, but the dramatic 30-year decline has suddenly gone into reverse. Although the exact cause of this turnaround is unclear, a growing body of evidence suggests that keyless entry systems may play a role. We therefore urge Hyundai to take all necessary steps to ensure that keyless entry systems, once a security innovation that deterred thieves, do not become a security liability for them to exploit.

After their adoption in the 1990s, keyless entry systems contributed to the impressive decline in car thefts from 1990 to 2019. These systems come in different forms. Some simply allow the driver to enter a vehicle without inserting a physical key into the door lock, while others, called passive entry systems, allow the driver to start the vehicle without inserting a physical key into the ignition. In both cases, the vehicle and a key fob communicate through radio signals, and an "engine immobilizer" prevents the vehicle from starting unless the key fob is nearby.

These systems were a critical advancement in vehicle security. Old-fashioned "hotwiring" a vehicle — that is, bypassing the ignition and starting a vehicle without a key — became far more difficult; with keyless entry systems, cars would not start unless they detected, through the radio signals, the presence of the key fob. In 1995, the European Union required manufacturers to include engine immobilizers on all new vehicles within three years, and Australia and Canada passed similar laws soon thereafter. One study estimated that the EU mandate reduced vehicle thefts in the Netherlands from 1995 to 2008 by 40 percent.[1] The United States never imposed a similar requirement, but many manufacturers have voluntarily adopted keyless entry systems, and car thefts per capita decreased by two-thirds from 1990 to 2019.[2]

---

[1] Jan C. van Ours and Ben Vollaard, *The Engine Immobiliser: A Non-Starter for Car Thieves*, 126 ECON. J. 1264, 1266 (2016), https://onlinelibrary.wiley.com/doi/abs/10.1111/ecoj.12196.

[2] Crime Data Explorer, FED. BUREAU OF INVESTIGATIONS, https://crime-data-explorer.app.cloud.gov/pages/explorer/crime/crime-trend (select "1990" in "From" and "2019" in "To" and "Motor vehicle theft" in "Crime Select").

Although this decrease tracked the overall decline in violent and property crime,[3] news reports have nevertheless attributed part of the decline to the adoption of keyless ignitions.[4]

This remarkably consistent trend towards fewer vehicle thefts, however, has made a concerning U-turn since the end of 2019. According to data compiled by the Federal Bureau of Investigation (FBI), U.S. car thefts per capita increased nationally by 11.8 percent in 2020.[5] Although national data has not yet been released for 2021, news reports suggest that car thefts continued to accelerate across the country last year. For example, in 2021, the number of car thefts appears to have increased by 132 percent in Milwaukee,[6] 70 percent in Washington, DC,[7] and 60 percent in Philadelphia.[8] This trend appears to have continued into 2022. So far this year, as compared with the same period in 2021, the number of car thefts has increased 74 percent in Portland, Ore.,[9] 54 percent in Richmond, Va.,[10] and 51 percent in New York City.[11] After so many years of progress, this rapid reversal in car thefts is alarming.

The same keyless entry systems that contributed to the decline in car thefts may now be providing an opportunity for thieves. Keyless entry systems are vulnerable in two ways. First, drivers may leave their key fobs in their cars, allowing a thief to easily start and steal a vehicle.[12] Whereas drivers used to have to remove the physical key from the ignition when they exited the vehicle, no similar action is necessary when a driver need only push a button to start or stop an engine. According to the New York Police Department, roughly 40 percent of car thefts in New York City so far this year were the result of motorists leaving their vehicles running or unlocked, often with keys or a key fob inside.[13] Keyless technology has thus escalated the consequences of ordinary human error.

---

[3] *Id.* (select "All Property Crimes" or "All Violent Crimes" in "Crime Select").

[4] *See, e.g.,* Sarah Maslin Nir, *Here's Why Car Thefts Are Soaring (Hint: Check Your Cup Holder)*, N.Y. TIMES (Jan. 6, 2021), www.nytimes.com/2021/01/06/nyregion/car-thefts-nyc.html; Brad Stone, *Pinch My Ride*, Wired (Aug. 1, 2006), www.wired.com/2006/08/carkey/.

[5] Crime Data Explorer, *supra* note 3 (select "2019" in "From" and "2020" in "To" and "Motor vehicle theft" in "Crime Select").

[6] *See* Teddy Nykiel, *Over 500% Spike in Auto Thefts Troubles Downtown*, MILWAUKEE BUS. J. (Feb. 9, 2022), https://www.bizjournals.com/milwaukee/news/2022/02/09/crime-statistics-mpd-2021-car-lefts.html.

[7] *See* Bruce Leshan, *Surge in Carjackings, Car Thefts Has Police Struggling to Respond*, WUSA (Feb. 9, 2021), www.wusa9.com/article/news/crime/surge-in-carjackings-car-thefts-dc-police-form-task-force/65-8c4b0c03-e343-430e-9c77-c5d9daade558.

[8] *See* Chad Pradelli and Cheryl Mettendorf, *Action News Investigation into Rise of Dealership Auto Thefts in Philadelphia Region*, ABC ACTION NEWS (Jan. 14, 2022), 6abc.com/car-thefts-auto-dealerships-6abc-investigation-barbera-autoland/11464047/.

[9] *See* Stolen Vehicle Statistics, CITY OF PORTLAND, https://www.portlandoregon.gov/police/74369 (compare selecting Jan. – May 2022 with Jan. – May 2021 in "Filter by Reported Date of Theft").

[10] *See* Henry Graff, *Richmond Police See 54% Increase in Vehicle Thefts Over Last Year*, NBC12 (Apr. 7, 2022), www.nbc12.com/2022/04/07/richmond-police-see-54-increase-vehicle-thefts-over-last-year/.

[11] *See* Rocco Parascandola, *NYPD Reports 51% Surge in Stolen Cars This Year*, N.Y. DAILY NEWS (June 12, 2022), www.nydailynews.com/new-york/nyc-crime/ny-car-vehicle-theft-surge-careless-motorists-nypd-20220612-eojbb2hhx5a3tn34vzhilc2fdq-story.html.

[12] *See* Nathan Bomey, *Thieves strike: Auto Theft Spikes During the Pandemic as Cars Are Left Unattended*, USA TODAY (Aug. 31, 2021), usatoday.com/story/money/cars/2021/08/31/auto-theft-spikes-stolen-car-vehicle-theft-pandemic-nicb/5652615001/.

[13] Rocco Parascandola, *supra* note 11.

Second, and perhaps more worryingly, a common type of keyless entry system that allows a driver to unlock and start the vehicle without needing to touch the key — known as a passive entry system — appear to be vulnerable to a "relay attack," in which a thief uses a signal amplifier to fool the car into believing that the owner is nearby.[14] Researchers have long known that bad actors could amplify radio signals emitted from the vehicle and key, allowing them to enter and start a vehicle even if the fob is nowhere nearby.[15] In recent years, devices that enable relay attacks have become widely available,[16] and news reports have identified thefts involving relay attacks in Austin,[17] Cincinnati,[18] and Los Angeles.[19]

More recently, researchers have shown that carmakers that use Bluetooth Low Energy (BLE) entry systems — which uses Bluetooth technology to determine whether the vehicle is within a certain distance of the connected device — are also vulnerable to theft using similar relay technology, affecting manufacturers such as Tesla that have adopted BLE passive entry systems.[20] For that reason, the Bluetooth Special Interest Group, the standard-setting organization that oversees the development of Bluetooth technologies, warns that BLE "should not be used as the only protection of valuable assets."[21] Car manufacturers have only recently begun using BLE technology to determine the proximity of a key fob, so researchers have not yet confirmed any vehicles stolen through a BLE relay attack. However, as manufacturers increasingly equip devices — such as smart locks for homes[22] — with BLE passive entry systems, this vulnerability could put a broad range of critical security systems at risk.

Fortunately, researchers have also identified methods to mitigate the risk of passive entry thefts. For example, manufacturers can prevent a fob from unlocking a vehicle if the fob was not recently in motion, as typically occurs as a driver approaches a vehicle. In other words, if the fob is idle, the driver is likely not trying to unlock their own vehicle; any attempt to use the fob in that state may be a sign of a relay attack. Similarly, manufacturers could require consumers to complete an additional verification, such as inputting a PIN number, to enter the vehicle. While such systems inherently inconvenience consumers, they also are a strong defense against relay

---

[14] Rachel Wait, *Keyless Car Crime: How to Thwart the Thieves*, FORBES ADVISOR (Mar. 24, 2022), www.forbes.com/uk/advisor/car-insurance/keyless-car-crime/.

[15] *See* ARI JUELS, RFID SECURITY AND PRIVACY: A RESEARCH SURVEY 13 (2005), www.arijuels.com/wp-content/uploads/2013/09/J06a.pdf.

[16] *See* Joseph Cox, *Meet the Guy Selling Wireless Tech to Steal Luxury Cars in Seconds*, VICE NEWS (Feb. 11, 2020), www.vice.com/en/article/7kz48x/guy-selling-relay-attack-keyless-repeaters-to-steal-cars.

[17] *See* Bettie Cross, *Car Thieves Are Hacking Key Fobs to Quickly and Quietly Steal Vehicles*, CBS AUSTIN (May 12, 2022), cbsaustin.com/news/local/car-thieves-are-hacking-key-fobs-to-quickly-and-quietly-steal-vehicles.

[18] *See* Jatara McGee, *Hackers Are Using New Tech to Steal Locked Cars Without Keys*, WLWT (May 9, 2019), www.wlwt.com/article/hackers-are-using-new-tech-to-steal-locked-cars-without-keys/27424367#.

[19] *See* Nick Bilton, *Keeping Your Car Safe From Electronic Thieves*, N.Y. TIMES (Apr. 15, 2015), www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html.

[20] *See* Sultan Khan, *Technical Advisory – Tesla BLE Phone-as-a-Key Passive Entry Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-tesla-ble-phone-as-a-key-passive-entry-vulnerable-to-relay-attacks/.

[21] BLUETOOTH SIG, PROXIMITY PROFILE 17 (2015), www.bluetooth.com/specifications/specs/proximity-profile-1-0-1/.

[22] *See* Sultan Khan, *Technical Advisory – Kwikset/Weiser BLE Proximity Authentication in Kevo Smart Locks Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-kwikset-weiser-ble-proximity-authentication-in-kevo-smart-locks-vulnerable-to-relay-attacks/.

attacks. Finally, automakers could also adopt Ultra-Wide-Band (UWB) technology, which enables a precise measurement between the vehicle and key fob and, in combination with other technologies, allows the vehicle to determine if the radio signal has been improperly amplified. Experts have suggested that UWB technology could significantly reduce the risk of relay theft.[23]

Given the recent surge in vehicle thefts and the potential security risks involved in keyless entry systems, I respectfully request that you respond in writing to the following questions by August 10, 2022:

1. Please provide the following data, as available, on thefts of vehicles manufactured by your company:

    a. How many vehicles manufactured by your company were stolen in 2019, 2020, 2021, and through the first six months of 2022?

    b. Of those vehicle thefts, how many were caused by thieves taking advantage of key fobs left in vehicles?

    c. Of those vehicle thefts, how many were caused by relay attacks?

2. Please describe the type of transponder and the technology standard that vehicles manufactured by your company use to communicate with key fobs and other devices. If vehicles manufactured by your company use different types of transponders and technology standards, please provide information on all types.

3. Please describe the testing that your company has done to assess the security of its keyless entry systems.

4. What specific steps has your company taken to reduce the vulnerability of its keyless entry system?

    a. Has your company considered making the keyless entry system motion activated?

    b. Has your company considered adopting Ultra-Wide-Band technology?

    c. Has your company considered creating mechanisms to alert owners if their key fob is left inside the vehicle?

5. Does your company plan to take any further steps to reduce any vulnerability of its keyless entry system?

Thank you for your prompt attention to these questions.

---

[23] *See e.g.,* Mridula Singh et al., *UWB with Pulse Reordering: Securing Ranging against Relay and Physical-Layer Attacks*, NETWORK AND DISTRIB. SYS, SEC. SYMP. (2019), www.ndss-symposium.org/ndss-paper/uwb-with-pulse-reordering-securing-ranging-against-relay-and-physical-layer-attacks/.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

July 20, 2022

Joachim Eberhardt
President
Jaguar Land Rover North America, LLC
100 Jaguar Land Rover Way,
Mahwah, NJ 07495

Dear Mr. Eberhardt,

I write to request information about the security of Jaguar Land Rover's motor vehicle keyless entry systems. Keyless entry systems — which allow users to enter a vehicle and start its engine without inserting and turning a key — likely helped reduce vehicle thefts since the 1990s, but the dramatic 30-year decline has suddenly gone into reverse. Although the exact cause of this turnaround is unclear, a growing body of evidence suggests that keyless entry systems may play a role. We therefore urge Jaguar Land Rover to take all necessary steps to ensure that keyless entry systems, once a security innovation that deterred thieves, do not become a security liability for them to exploit.

After their adoption in the 1990s, keyless entry systems contributed to the impressive decline in car thefts from 1990 to 2019. These systems come in different forms. Some simply allow the driver to enter a vehicle without inserting a physical key into the door lock, while others, called passive entry systems, allow the driver to start the vehicle without inserting a physical key into the ignition. In both cases, the vehicle and a key fob communicate through radio signals, and an "engine immobilizer" prevents the vehicle from starting unless the key fob is nearby.

These systems were a critical advancement in vehicle security. Old-fashioned "hotwiring" a vehicle — that is, bypassing the ignition and starting a vehicle without a key — became far more difficult; with keyless entry systems, cars would not start unless they detected, through the radio signals, the presence of the key fob. In 1995, the European Union required manufacturers to include engine immobilizers on all new vehicles within three years, and Australia and Canada passed similar laws soon thereafter. One study estimated that the EU mandate reduced vehicle thefts in the Netherlands from 1995 to 2008 by 40 percent.[1] The United States never imposed a similar requirement, but many manufacturers have voluntarily adopted keyless entry systems, and car thefts per capita decreased by two-thirds from 1990 to 2019.[2]

---

[1] Jan C. van Ours and Ben Vollaard, *The Engine Immobiliser: A Non-Starter for Car Thieves*, 126 ECON. J. 1264, 1266 (2016), https://onlinelibrary.wiley.com/doi/abs/10.1111/ecoj.12196.

[2] Crime Data Explorer, FED. BUREAU OF INVESTIGATIONS, https://crime-data-explorer.app.cloud.gov/pages/explorer/crime/crime-trend (select "1990" in "From" and "2019" in "To" and "Motor vehicle theft" in "Crime Select").

Although this decrease tracked the overall decline in violent and property crime,[3] news reports have nevertheless attributed part of the decline to the adoption of keyless ignitions.[4]

This remarkably consistent trend towards fewer vehicle thefts, however, has made a concerning U-turn since the end of 2019. According to data compiled by the Federal Bureau of Investigation (FBI), U.S. car thefts per capita increased nationally by 11.8 percent in 2020.[5] Although national data has not yet been released for 2021, news reports suggest that car thefts continued to accelerate across the country last year. For example, in 2021, the number of car thefts appears to have increased by 132 percent in Milwaukee,[6] 70 percent in Washington, DC,[7] and 60 percent in Philadelphia.[8] This trend appears to have continued into 2022. So far this year, as compared with the same period in 2021, the number of car thefts has increased 74 percent in Portland, Ore.,[9] 54 percent in Richmond, Va.,[10] and 51 percent in New York City.[11] After so many years of progress, this rapid reversal in car thefts is alarming.

The same keyless entry systems that contributed to the decline in car thefts may now be providing an opportunity for thieves. Keyless entry systems are vulnerable in two ways. First, drivers may leave their key fobs in their cars, allowing a thief to easily start and steal a vehicle.[12] Whereas drivers used to have to remove the physical key from the ignition when they exited the vehicle, no similar action is necessary when a driver need only push a button to start or stop an engine. According to the New York Police Department, roughly 40 percent of car thefts in New York City so far this year were the result of motorists leaving their vehicles running or unlocked, often with keys or a key fob inside.[13] Keyless technology has thus escalated the consequences of ordinary human error.

---

[3] *Id.* (select "All Property Crimes" or "All Violent Crimes" in "Crime Select").

[4] *See, e.g.,* Sarah Maslin Nir, *Here's Why Car Thefts Are Soaring (Hint: Check Your Cup Holder)*, N.Y. TIMES (Jan. 6, 2021), www.nytimes.com/2021/01/06/nyregion/car-thefts-nyc.html; Brad Stone, *Pinch My Ride*, Wired (Aug. 1, 2006), www.wired.com/2006/08/carkey/.

[5] Crime Data Explorer, *supra* note 3 (select "2019" in "From" and "2020" in "To" and "Motor vehicle theft" in "Crime Select").

[6] *See* Teddy Nykiel, *Over 500% Spike in Auto Thefts Troubles Downtown*, MILWAUKEE BUS. J. (Feb. 9, 2022), https://www.bizjournals.com/milwaukee/news/2022/02/09/crime-statistics-mpd-2021-car-lefts.html.

[7] *See* Bruce Leshan, *Surge in Carjackings, Car Thefts Has Police Struggling to Respond*, WUSA (Feb. 9, 2021), www.wusa9.com/article/news/crime/surge-in-carjackings-car-thefts-dc-police-form-task-force/65-8c4b0c03-e343-430e-9c77-c5d9daade558.

[8] *See* Chad Pradelli and Cheryl Mettendorf, *Action News Investigation into Rise of Dealership Auto Thefts in Philadelphia Region*, ABC ACTION NEWS (Jan. 14, 2022), 6abc.com/car-thefts-auto-dealerships-6abc-investigation-barbera-autoland/11464047/.

[9] *See* Stolen Vehicle Statistics, CITY OF PORTLAND, https://www.portlandoregon.gov/police/74369 (compare selecting Jan. – May 2022 with Jan. – May 2021 in "Filter by Reported Date of Theft").

[10] *See* Henry Graff, *Richmond Police See 54% Increase in Vehicle Thefts Over Last Year*, NBC12 (Apr. 7, 2022), www.nbc12.com/2022/04/07/richmond-police-see-54-increase-vehicle-thefts-over-last-year/.

[11] *See* Rocco Parascandola, *NYPD Reports 51% Surge in Stolen Cars This Year*, N.Y. DAILY NEWS (June 12, 2022), www.nydailynews.com/new-york/nyc-crime/ny-car-vehicle-theft-surge-careless-motorists-nypd-20220612-eojbb2hhx5a3tn34vzhilc2fdq-story.html.

[12] *See* Nathan Bomey, *Thieves strike: Auto Theft Spikes During the Pandemic as Cars Are Left Unattended*, USA TODAY (Aug. 31, 2021), usatoday.com/story/money/cars/2021/08/31/auto-theft-spikes-stolen-car-vehicle-theft-pandemic-nicb/5652615001/.

[13] Rocco Parascandola, *supra* note 11.

Second, and perhaps more worryingly, a common type of keyless entry system that allows a driver to unlock and start the vehicle without needing to touch the key — known as a passive entry system — appear to be vulnerable to a "relay attack," in which a thief uses a signal amplifier to fool the car into believing that the owner is nearby.[14] Researchers have long known that bad actors could amplify radio signals emitted from the vehicle and key, allowing them to enter and start a vehicle even if the fob is nowhere nearby.[15] In recent years, devices that enable relay attacks have become widely available,[16] and news reports have identified thefts involving relay attacks in Austin,[17] Cincinnati,[18] and Los Angeles.[19]

More recently, researchers have shown that carmakers that use Bluetooth Low Energy (BLE) entry systems — which uses Bluetooth technology to determine whether the vehicle is within a certain distance of the connected device — are also vulnerable to theft using similar relay technology, affecting manufacturers such as Tesla that have adopted BLE passive entry systems.[20] For that reason, the Bluetooth Special Interest Group, the standard-setting organization that oversees the development of Bluetooth technologies, warns that BLE "should not be used as the only protection of valuable assets."[21] Car manufacturers have only recently begun using BLE technology to determine the proximity of a key fob, so researchers have not yet confirmed any vehicles stolen through a BLE relay attack. However, as manufacturers increasingly equip devices — such as smart locks for homes[22] — with BLE passive entry systems, this vulnerability could put a broad range of critical security systems at risk.

Fortunately, researchers have also identified methods to mitigate the risk of passive entry thefts. For example, manufacturers can prevent a fob from unlocking a vehicle if the fob was not recently in motion, as typically occurs as a driver approaches a vehicle. In other words, if the fob is idle, the driver is likely not trying to unlock their own vehicle; any attempt to use the fob in that state may be a sign of a relay attack. Similarly, manufacturers could require consumers to complete an additional verification, such as inputting a PIN number, to enter the vehicle. While such systems inherently inconvenience consumers, they also are a strong defense against relay

---

[14] Rachel Wait, *Keyless Car Crime: How to Thwart the Thieves*, FORBES ADVISOR (Mar. 24, 2022), www.forbes.com/uk/advisor/car-insurance/keyless-car-crime/.

[15] *See* ARI JUELS, RFID SECURITY AND PRIVACY: A RESEARCH SURVEY 13 (2005), www.arijuels.com/wp-content/uploads/2013/09/J06a.pdf.

[16] *See* Joseph Cox, *Meet the Guy Selling Wireless Tech to Steal Luxury Cars in Seconds*, VICE NEWS (Feb. 11, 2020), www.vice.com/en/article/7kz48x/guy-selling-relay-attack-keyless-repeaters-to-steal-cars.

[17] *See* Bettie Cross, *Car Thieves Are Hacking Key Fobs to Quickly and Quietly Steal Vehicles*, CBS AUSTIN (May 12, 2022), cbsaustin.com/news/local/car-thieves-are-hacking-key-fobs-to-quickly-and-quietly-steal-vehicles.

[18] *See* Jatara McGee, *Hackers Are Using New Tech to Steal Locked Cars Without Keys*, WLWT (May 9, 2019), www.wlwt.com/article/hackers-are-using-new-tech-to-steal-locked-cars-without-keys/27424367#.

[19] *See* Nick Bilton, *Keeping Your Car Safe From Electronic Thieves*, N.Y. TIMES (Apr. 15, 2015), www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html.

[20] *See* Sultan Khan, *Technical Advisory – Tesla BLE Phone-as-a-Key Passive Entry Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-tesla-ble-phone-as-a-key-passive-entry-vulnerable-to-relay-attacks/.

[21] BLUETOOTH SIG, PROXIMITY PROFILE 17 (2015), www.bluetooth.com/specifications/specs/proximity-profile-1-0-1/.

[22] *See* Sultan Khan, *Technical Advisory – Kwikset/Weiser BLE Proximity Authentication in Kevo Smart Locks Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-kwikset-weiser-ble-proximity-authentication-in-kevo-smart-locks-vulnerable-to-relay-attacks/.

attacks. Finally, automakers could also adopt Ultra-Wide-Band (UWB) technology, which enables a precise measurement between the vehicle and key fob and, in combination with other technologies, allows the vehicle to determine if the radio signal has been improperly amplified. Experts have suggested that UWB technology could significantly reduce the risk of relay theft.[23]

Given the recent surge in vehicle thefts and the potential security risks involved in keyless entry systems, I respectfully request that you respond in writing to the following questions by August 10, 2022:

1. Please provide the following data, as available, on thefts of vehicles manufactured by your company:

    a. How many vehicles manufactured by your company were stolen in 2019, 2020, 2021, and through the first six months of 2022?

    b. Of those vehicle thefts, how many were caused by thieves taking advantage of key fobs left in vehicles?

    c. Of those vehicle thefts, how many were caused by relay attacks?

2. Please describe the type of transponder and the technology standard that vehicles manufactured by your company use to communicate with key fobs and other devices. If vehicles manufactured by your company use different types of transponders and technology standards, please provide information on all types.

3. Please describe the testing that your company has done to assess the security of its keyless entry systems.

4. What specific steps has your company taken to reduce the vulnerability of its keyless entry system?

    a. Has your company considered making the keyless entry system motion activated?

    b. Has your company considered adopting Ultra-Wide-Band technology?

    c. Has your company considered creating mechanisms to alert owners if their key fob is left inside the vehicle?

5. Does your company plan to take any further steps to reduce any vulnerability of its keyless entry system?

Thank you for your prompt attention to these questions.

---

[23] *See e.g.,* Mridula Singh et al., *UWB with Pulse Reordering: Securing Ranging against Relay and Physical-Layer Attacks*, NETWORK AND DISTRIB. SYS, SEC. SYMP. (2019), www.ndss-symposium.org/ndss-paper/uwb-with-pulse-reordering-securing-ranging-against-relay-and-physical-layer-attacks/.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

July 20, 2022

SeungKyu Yoon
President and Chief Executive Officer
Kia Motors America, Inc.
111 Peters Canyon Road
Irvine, CA 92606

Dear Mr. Yoon,

I write to request information about the security of Kia's motor vehicle keyless entry systems. Keyless entry systems — which allow users to enter a vehicle and start its engine without inserting and turning a key — likely helped reduce vehicle thefts since the 1990s, but the dramatic 30-year decline has suddenly gone into reverse. Although the exact cause of this turnaround is unclear, a growing body of evidence suggests that keyless entry systems may play a role. We therefore urge Kia to take all necessary steps to ensure that keyless entry systems, once a security innovation that deterred thieves, do not become a security liability for them to exploit.

After their adoption in the 1990s, keyless entry systems contributed to the impressive decline in car thefts from 1990 to 2019. These systems come in different forms. Some simply allow the driver to enter a vehicle without inserting a physical key into the door lock, while others, called passive entry systems, allow the driver to start the vehicle without inserting a physical key into the ignition. In both cases, the vehicle and a key fob communicate through radio signals, and an "engine immobilizer" prevents the vehicle from starting unless the key fob is nearby.

These systems were a critical advancement in vehicle security. Old-fashioned "hotwiring" a vehicle — that is, bypassing the ignition and starting a vehicle without a key — became far more difficult; with keyless entry systems, cars would not start unless they detected, through the radio signals, the presence of the key fob. In 1995, the European Union required manufacturers to include engine immobilizers on all new vehicles within three years, and Australia and Canada passed similar laws soon thereafter. One study estimated that the EU mandate reduced vehicle thefts in the Netherlands from 1995 to 2008 by 40 percent.[1] The United States never imposed a similar requirement, but many manufacturers have voluntarily adopted keyless entry systems, and car thefts per capita decreased by two-thirds from 1990 to 2019.[2]

---

[1] Jan C. van Ours and Ben Vollaard, *The Engine Immobiliser: A Non-Starter for Car Thieves*, 126 ECON. J. 1264, 1266 (2016), https://onlinelibrary.wiley.com/doi/abs/10.1111/ecoj.12196.

[2] Crime Data Explorer, FED. BUREAU OF INVESTIGATIONS, https://crime-data-explorer.app.cloud.gov/pages/explorer/crime/crime-trend (select "1990" in "From" and "2019" in "To" and "Motor vehicle theft" in "Crime Select").

Although this decrease tracked the overall decline in violent and property crime,[3] news reports have nevertheless attributed part of the decline to the adoption of keyless ignitions.[4]

This remarkably consistent trend towards fewer vehicle thefts, however, has made a concerning U-turn since the end of 2019. According to data compiled by the Federal Bureau of Investigation (FBI), U.S. car thefts per capita increased nationally by 11.8 percent in 2020.[5] Although national data has not yet been released for 2021, news reports suggest that car thefts continued to accelerate across the country last year. For example, in 2021, the number of car thefts appears to have increased by 132 percent in Milwaukee,[6] 70 percent in Washington, DC,[7] and 60 percent in Philadelphia.[8] This trend appears to have continued into 2022. So far this year, as compared with the same period in 2021, the number of car thefts has increased 74 percent in Portland, Ore.,[9] 54 percent in Richmond, Va.,[10] and 51 percent in New York City.[11] After so many years of progress, this rapid reversal in car thefts is alarming.

The same keyless entry systems that contributed to the decline in car thefts may now be providing an opportunity for thieves. Keyless entry systems are vulnerable in two ways. First, drivers may leave their key fobs in their cars, allowing a thief to easily start and steal a vehicle.[12] Whereas drivers used to have to remove the physical key from the ignition when they exited the vehicle, no similar action is necessary when a driver need only push a button to start or stop an engine. According to the New York Police Department, roughly 40 percent of car thefts in New York City so far this year were the result of motorists leaving their vehicles running or unlocked, often with keys or a key fob inside.[13] Keyless technology has thus escalated the consequences of ordinary human error.

---

[3] *Id.* (select "All Property Crimes" or "All Violent Crimes" in "Crime Select").

[4] *See, e.g.,* Sarah Maslin Nir, *Here's Why Car Thefts Are Soaring (Hint: Check Your Cup Holder)*, N.Y. TIMES (Jan. 6, 2021), www.nytimes.com/2021/01/06/nyregion/car-thefts-nyc.html; Brad Stone, *Pinch My Ride*, Wired (Aug. 1, 2006), www.wired.com/2006/08/carkey/.

[5] Crime Data Explorer, *supra* note 3 (select "2019" in "From" and "2020" in "To" and "Motor vehicle theft" in "Crime Select").

[6] *See* Teddy Nykiel, *Over 500% Spike in Auto Thefts Troubles Downtown*, MILWAUKEE BUS. J. (Feb. 9, 2022), https://www.bizjournals.com/milwaukee/news/2022/02/09/crime-statistics-mpd-2021-car-lefts.html.

[7] *See* Bruce Leshan, *Surge in Carjackings, Car Thefts Has Police Struggling to Respond*, WUSA (Feb. 9, 2021), www.wusa9.com/article/news/crime/surge-in-carjackings-car-thefts-dc-police-form-task-force/65-8c4b0c03-e343-430e-9c77-c5d9daade558.

[8] *See* Chad Pradelli and Cheryl Mettendorf, *Action News Investigation into Rise of Dealership Auto Thefts in Philadelphia Region*, ABC ACTION NEWS (Jan. 14, 2022), 6abc.com/car-thefts-auto-dealerships-6abc-investigation-barbera-autoland/11464047/.

[9] *See* Stolen Vehicle Statistics, CITY OF PORTLAND, https://www.portlandoregon.gov/police/74369 (compare selecting Jan. – May 2022 with Jan. – May 2021 in "Filter by Reported Date of Theft").

[10] *See* Henry Graff, *Richmond Police See 54% Increase in Vehicle Thefts Over Last Year*, NBC12 (Apr. 7, 2022), www.nbc12.com/2022/04/07/richmond-police-see-54-increase-vehicle-thefts-over-last-year/.

[11] *See* Rocco Parascandola, *NYPD Reports 51% Surge in Stolen Cars This Year*, N.Y. DAILY NEWS (June 12, 2022), www.nydailynews.com/new-york/nyc-crime/ny-car-vehicle-theft-surge-careless-motorists-nypd-20220612-eojbb2hhx5a3tn34vzhilc2fdq-story.html.

[12] *See* Nathan Bomey, *Thieves strike: Auto Theft Spikes During the Pandemic as Cars Are Left Unattended*, USA TODAY (Aug. 31, 2021), usatoday.com/story/money/cars/2021/08/31/auto-theft-spikes-stolen-car-vehicle-theft-pandemic-nicb/5652615001/.

[13] Rocco Parascandola, *supra* note 11.

Second, and perhaps more worryingly, a common type of keyless entry system that allows a driver to unlock and start the vehicle without needing to touch the key — known as a passive entry system — appear to be vulnerable to a "relay attack," in which a thief uses a signal amplifier to fool the car into believing that the owner is nearby.[14] Researchers have long known that bad actors could amplify radio signals emitted from the vehicle and key, allowing them to enter and start a vehicle even if the fob is nowhere nearby.[15] In recent years, devices that enable relay attacks have become widely available,[16] and news reports have identified thefts involving relay attacks in Austin,[17] Cincinnati,[18] and Los Angeles.[19]

More recently, researchers have shown that carmakers that use Bluetooth Low Energy (BLE) entry systems — which uses Bluetooth technology to determine whether the vehicle is within a certain distance of the connected device — are also vulnerable to theft using similar relay technology, affecting manufacturers such as Tesla that have adopted BLE passive entry systems.[20] For that reason, the Bluetooth Special Interest Group, the standard-setting organization that oversees the development of Bluetooth technologies, warns that BLE "should not be used as the only protection of valuable assets."[21] Car manufacturers have only recently begun using BLE technology to determine the proximity of a key fob, so researchers have not yet confirmed any vehicles stolen through a BLE relay attack. However, as manufacturers increasingly equip devices — such as smart locks for homes[22] — with BLE passive entry systems, this vulnerability could put a broad range of critical security systems at risk.

Fortunately, researchers have also identified methods to mitigate the risk of passive entry thefts. For example, manufacturers can prevent a fob from unlocking a vehicle if the fob was not recently in motion, as typically occurs as a driver approaches a vehicle. In other words, if the fob is idle, the driver is likely not trying to unlock their own vehicle; any attempt to use the fob in that state may be a sign of a relay attack. Similarly, manufacturers could require consumers to complete an additional verification, such as inputting a PIN number, to enter the vehicle. While such systems inherently inconvenience consumers, they also are a strong defense against relay

---

[14] Rachel Wait, *Keyless Car Crime: How to Thwart the Thieves*, FORBES ADVISOR (Mar. 24, 2022), www.forbes.com/uk/advisor/car-insurance/keyless-car-crime/.

[15] *See* ARI JUELS, RFID SECURITY AND PRIVACY: A RESEARCH SURVEY 13 (2005), www.arijuels.com/wp-content/uploads/2013/09/J06a.pdf.

[16] *See* Joseph Cox, *Meet the Guy Selling Wireless Tech to Steal Luxury Cars in Seconds*, VICE NEWS (Feb. 11, 2020), www.vice.com/en/article/7kz48x/guy-selling-relay-attack-keyless-repeaters-to-steal-cars.

[17] *See* Bettie Cross, *Car Thieves Are Hacking Key Fobs to Quickly and Quietly Steal Vehicles*, CBS AUSTIN (May 12, 2022), cbsaustin.com/news/local/car-thieves-are-hacking-key-fobs-to-quickly-and-quietly-steal-vehicles.

[18] *See* Jatara McGee, *Hackers Are Using New Tech to Steal Locked Cars Without Keys*, WLWT (May 9, 2019), www.wlwt.com/article/hackers-are-using-new-tech-to-steal-locked-cars-without-keys/27424367#.

[19] *See* Nick Bilton, *Keeping Your Car Safe From Electronic Thieves*, N.Y. TIMES (Apr. 15, 2015), www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html.

[20] *See* Sultan Khan, *Technical Advisory – Tesla BLE Phone-as-a-Key Passive Entry Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-tesla-ble-phone-as-a-key-passive-entry-vulnerable-to-relay-attacks/.

[21] BLUETOOTH SIG, PROXIMITY PROFILE 17 (2015), www.bluetooth.com/specifications/specs/proximity-profile-1-0-1/.

[22] *See* Sultan Khan, *Technical Advisory – Kwikset/Weiser BLE Proximity Authentication in Kevo Smart Locks Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-kwikset-weiser-ble-proximity-authentication-in-kevo-smart-locks-vulnerable-to-relay-attacks/.

attacks. Finally, automakers could also adopt Ultra-Wide-Band (UWB) technology, which enables a precise measurement between the vehicle and key fob and, in combination with other technologies, allows the vehicle to determine if the radio signal has been improperly amplified. Experts have suggested that UWB technology could significantly reduce the risk of relay theft.[23]

Given the recent surge in vehicle thefts and the potential security risks involved in keyless entry systems, I respectfully request that you respond in writing to the following questions by August 10, 2022:

1. Please provide the following data, as available, on thefts of vehicles manufactured by your company:

    a. How many vehicles manufactured by your company were stolen in 2019, 2020, 2021, and through the first six months of 2022?

    b. Of those vehicle thefts, how many were caused by thieves taking advantage of key fobs left in vehicles?

    c. Of those vehicle thefts, how many were caused by relay attacks?

2. Please describe the type of transponder and the technology standard that vehicles manufactured by your company use to communicate with key fobs and other devices. If vehicles manufactured by your company use different types of transponders and technology standards, please provide information on all types.

3. Please describe the testing that your company has done to assess the security of its keyless entry systems.

4. What specific steps has your company taken to reduce the vulnerability of its keyless entry system?

    a. Has your company considered making the keyless entry system motion activated?

    b. Has your company considered adopting Ultra-Wide-Band technology?

    c. Has your company considered creating mechanisms to alert owners if their key fob is left inside the vehicle?

5. Does your company plan to take any further steps to reduce any vulnerability of its keyless entry system?

Thank you for your prompt attention to these questions.

---

[23] *See e.g.,* Mridula Singh et al., *UWB with Pulse Reordering: Securing Ranging against Relay and Physical-Layer Attacks*, NETWORK AND DISTRIB. SYS, SEC. SYMP. (2019), www.ndss-symposium.org/ndss-paper/uwb-with-pulse-reordering-securing-ranging-against-relay-and-physical-layer-attacks/.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

July 20, 2022

Jeffrey Guyton
President and Chief Executive Officer
Mazda Motor of America, Inc.
7755 Irvine Center Drive
Irvine, CA 92618

Dear Mr. Guyton,

I write to request information about the security of Mazda's motor vehicle keyless entry systems. Keyless entry systems — which allow users to enter a vehicle and start its engine without inserting and turning a key — likely helped reduce vehicle thefts since the 1990s, but the dramatic 30-year decline has suddenly gone into reverse. Although the exact cause of this turnaround is unclear, a growing body of evidence suggests that keyless entry systems may play a role. We therefore urge Mazda to take all necessary steps to ensure that keyless entry systems, once a security innovation that deterred thieves, do not become a security liability for them to exploit.

After their adoption in the 1990s, keyless entry systems contributed to the impressive decline in car thefts from 1990 to 2019. These systems come in different forms. Some simply allow the driver to enter a vehicle without inserting a physical key into the door lock, while others, called passive entry systems, allow the driver to start the vehicle without inserting a physical key into the ignition. In both cases, the vehicle and a key fob communicate through radio signals, and an "engine immobilizer" prevents the vehicle from starting unless the key fob is nearby.

These systems were a critical advancement in vehicle security. Old-fashioned "hotwiring" a vehicle — that is, bypassing the ignition and starting a vehicle without a key — became far more difficult; with keyless entry systems, cars would not start unless they detected, through the radio signals, the presence of the key fob. In 1995, the European Union required manufacturers to include engine immobilizers on all new vehicles within three years, and Australia and Canada passed similar laws soon thereafter. One study estimated that the EU mandate reduced vehicle thefts in the Netherlands from 1995 to 2008 by 40 percent.[1] The United States never imposed a similar requirement, but many manufacturers have voluntarily adopted keyless entry systems, and car thefts per capita decreased by two-thirds from 1990 to 2019.[2]

---

[1] Jan C. van Ours and Ben Vollaard, *The Engine Immobiliser: A Non-Starter for Car Thieves*, 126 ECON. J. 1264, 1266 (2016), https://onlinelibrary.wiley.com/doi/abs/10.1111/ecoj.12196.

[2] Crime Data Explorer, FED. BUREAU OF INVESTIGATIONS, https://crime-data-explorer.app.cloud.gov/pages/explorer/crime/crime-trend (select "1990" in "From" and "2019" in "To" and "Motor vehicle theft" in "Crime Select").

Although this decrease tracked the overall decline in violent and property crime,[3] news reports have nevertheless attributed part of the decline to the adoption of keyless ignitions.[4]

This remarkably consistent trend towards fewer vehicle thefts, however, has made a concerning U-turn since the end of 2019. According to data compiled by the Federal Bureau of Investigation (FBI), U.S. car thefts per capita increased nationally by 11.8 percent in 2020.[5] Although national data has not yet been released for 2021, news reports suggest that car thefts continued to accelerate across the country last year. For example, in 2021, the number of car thefts appears to have increased by 132 percent in Milwaukee,[6] 70 percent in Washington, DC,[7] and 60 percent in Philadelphia.[8] This trend appears to have continued into 2022. So far this year, as compared with the same period in 2021, the number of car thefts has increased 74 percent in Portland, Ore.,[9] 54 percent in Richmond, Va.,[10] and 51 percent in New York City.[11] After so many years of progress, this rapid reversal in car thefts is alarming.

The same keyless entry systems that contributed to the decline in car thefts may now be providing an opportunity for thieves. Keyless entry systems are vulnerable in two ways. First, drivers may leave their key fobs in their cars, allowing a thief to easily start and steal a vehicle.[12] Whereas drivers used to have to remove the physical key from the ignition when they exited the vehicle, no similar action is necessary when a driver need only push a button to start or stop an engine. According to the New York Police Department, roughly 40 percent of car thefts in New York City so far this year were the result of motorists leaving their vehicles running or unlocked, often with keys or a key fob inside.[13] Keyless technology has thus escalated the consequences of ordinary human error.

---

[3] *Id.* (select "All Property Crimes" or "All Violent Crimes" in "Crime Select").

[4] *See, e.g.,* Sarah Maslin Nir, *Here's Why Car Thefts Are Soaring (Hint: Check Your Cup Holder)*, N.Y. TIMES (Jan. 6, 2021), www.nytimes.com/2021/01/06/nyregion/car-thefts-nyc.html; Brad Stone, *Pinch My Ride*, Wired (Aug. 1, 2006), www.wired.com/2006/08/carkey/.

[5] Crime Data Explorer, *supra* note 3 (select "2019" in "From" and "2020" in "To" and "Motor vehicle theft" in "Crime Select").

[6] *See* Teddy Nykiel, *Over 500% Spike in Auto Thefts Troubles Downtown*, MILWAUKEE BUS. J. (Feb. 9, 2022), https://www.bizjournals.com/milwaukee/news/2022/02/09/crime-statistics-mpd-2021-car-lefts.html.

[7] *See* Bruce Leshan, *Surge in Carjackings, Car Thefts Has Police Struggling to Respond*, WUSA (Feb. 9, 2021), www.wusa9.com/article/news/crime/surge-in-carjackings-car-thefts-dc-police-form-task-force/65-8c4b0c03-e343-430e-9c77-c5d9daade558.

[8] *See* Chad Pradelli and Cheryl Mettendorf, *Action News Investigation into Rise of Dealership Auto Thefts in Philadelphia Region*, ABC ACTION NEWS (Jan. 14, 2022), 6abc.com/car-thefts-auto-dealerships-6abc-investigation-barbera-autoland/11464047/.

[9] *See* Stolen Vehicle Statistics, CITY OF PORTLAND, https://www.portlandoregon.gov/police/74369 (compare selecting Jan. – May 2022 with Jan. – May 2021 in "Filter by Reported Date of Theft").

[10] *See* Henry Graff, *Richmond Police See 54% Increase in Vehicle Thefts Over Last Year*, NBC12 (Apr. 7, 2022), www.nbc12.com/2022/04/07/richmond-police-see-54-increase-vehicle-thefts-over-last-year/.

[11] *See* Rocco Parascandola, *NYPD Reports 51% Surge in Stolen Cars This Year*, N.Y. DAILY NEWS (June 12, 2022), www.nydailynews.com/new-york/nyc-crime/ny-car-vehicle-theft-surge-careless-motorists-nypd-20220612-eojbb2hhx5a3tn34vzhilc2fdq-story.html.

[12] *See* Nathan Bomey, *Thieves strike: Auto Theft Spikes During the Pandemic as Cars Are Left Unattended*, USA TODAY (Aug. 31, 2021), usatoday.com/story/money/cars/2021/08/31/auto-theft-spikes-stolen-car-vehicle-theft-pandemic-nicb/5652615001/.

[13] Rocco Parascandola, *supra* note 11.

Second, and perhaps more worryingly, a common type of keyless entry system that allows a driver to unlock and start the vehicle without needing to touch the key — known as a passive entry system — appear to be vulnerable to a "relay attack," in which a thief uses a signal amplifier to fool the car into believing that the owner is nearby.[14] Researchers have long known that bad actors could amplify radio signals emitted from the vehicle and key, allowing them to enter and start a vehicle even if the fob is nowhere nearby.[15] In recent years, devices that enable relay attacks have become widely available,[16] and news reports have identified thefts involving relay attacks in Austin,[17] Cincinnati,[18] and Los Angeles.[19]

More recently, researchers have shown that carmakers that use Bluetooth Low Energy (BLE) entry systems — which uses Bluetooth technology to determine whether the vehicle is within a certain distance of the connected device — are also vulnerable to theft using similar relay technology, affecting manufacturers such as Tesla that have adopted BLE passive entry systems.[20] For that reason, the Bluetooth Special Interest Group, the standard-setting organization that oversees the development of Bluetooth technologies, warns that BLE "should not be used as the only protection of valuable assets."[21] Car manufacturers have only recently begun using BLE technology to determine the proximity of a key fob, so researchers have not yet confirmed any vehicles stolen through a BLE relay attack. However, as manufacturers increasingly equip devices — such as smart locks for homes[22] — with BLE passive entry systems, this vulnerability could put a broad range of critical security systems at risk.

Fortunately, researchers have also identified methods to mitigate the risk of passive entry thefts. For example, manufacturers can prevent a fob from unlocking a vehicle if the fob was not recently in motion, as typically occurs as a driver approaches a vehicle. In other words, if the fob is idle, the driver is likely not trying to unlock their own vehicle; any attempt to use the fob in that state may be a sign of a relay attack. Similarly, manufacturers could require consumers to complete an additional verification, such as inputting a PIN number, to enter the vehicle. While such systems inherently inconvenience consumers, they also are a strong defense against relay

---

[14] Rachel Wait, *Keyless Car Crime: How to Thwart the Thieves*, FORBES ADVISOR (Mar. 24, 2022), www.forbes.com/uk/advisor/car-insurance/keyless-car-crime/.

[15] *See* ARI JUELS, RFID SECURITY AND PRIVACY: A RESEARCH SURVEY 13 (2005), www.arijuels.com/wp-content/uploads/2013/09/J06a.pdf.

[16] *See* Joseph Cox, *Meet the Guy Selling Wireless Tech to Steal Luxury Cars in Seconds*, VICE NEWS (Feb. 11, 2020), www.vice.com/en/article/7kz48x/guy-selling-relay-attack-keyless-repeaters-to-steal-cars.

[17] *See* Bettie Cross, *Car Thieves Are Hacking Key Fobs to Quickly and Quietly Steal Vehicles*, CBS AUSTIN (May 12, 2022), cbsaustin.com/news/local/car-thieves-are-hacking-key-fobs-to-quickly-and-quietly-steal-vehicles.

[18] *See* Jatara McGee, *Hackers Are Using New Tech to Steal Locked Cars Without Keys*, WLWT (May 9, 2019), www.wlwt.com/article/hackers-are-using-new-tech-to-steal-locked-cars-without-keys/27424367#.

[19] *See* Nick Bilton, *Keeping Your Car Safe From Electronic Thieves*, N.Y. TIMES (Apr. 15, 2015), www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html.

[20] *See* Sultan Khan, *Technical Advisory – Tesla BLE Phone-as-a-Key Passive Entry Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-tesla-ble-phone-as-a-key-passive-entry-vulnerable-to-relay-attacks/.

[21] BLUETOOTH SIG, PROXIMITY PROFILE 17 (2015), www.bluetooth.com/specifications/specs/proximity-profile-1-0-1/.

[22] *See* Sultan Khan, *Technical Advisory – Kwikset/Weiser BLE Proximity Authentication in Kevo Smart Locks Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-kwikset-weiser-ble-proximity-authentication-in-kevo-smart-locks-vulnerable-to-relay-attacks/.

attacks. Finally, automakers could also adopt Ultra-Wide-Band (UWB) technology, which enables a precise measurement between the vehicle and key fob and, in combination with other technologies, allows the vehicle to determine if the radio signal has been improperly amplified. Experts have suggested that UWB technology could significantly reduce the risk of relay theft.[23]

Given the recent surge in vehicle thefts and the potential security risks involved in keyless entry systems, I respectfully request that you respond in writing to the following questions by August 10, 2022:

1. Please provide the following data, as available, on thefts of vehicles manufactured by your company:

    a. How many vehicles manufactured by your company were stolen in 2019, 2020, 2021, and through the first six months of 2022?

    b. Of those vehicle thefts, how many were caused by thieves taking advantage of key fobs left in vehicles?

    c. Of those vehicle thefts, how many were caused by relay attacks?

2. Please describe the type of transponder and the technology standard that vehicles manufactured by your company use to communicate with key fobs and other devices. If vehicles manufactured by your company use different types of transponders and technology standards, please provide information on all types.

3. Please describe the testing that your company has done to assess the security of its keyless entry systems.

4. What specific steps has your company taken to reduce the vulnerability of its keyless entry system?

    a. Has your company considered making the keyless entry system motion activated?

    b. Has your company considered adopting Ultra-Wide-Band technology?

    c. Has your company considered creating mechanisms to alert owners if their key fob is left inside the vehicle?

5. Does your company plan to take any further steps to reduce any vulnerability of its keyless entry system?

Thank you for your prompt attention to these questions.

---

[23] *See e.g.,* Mridula Singh et al., *UWB with Pulse Reordering: Securing Ranging against Relay and Physical-Layer Attacks*, NETWORK AND DISTRIB. SYS, SEC. SYMP. (2019), www.ndss-symposium.org/ndss-paper/uwb-with-pulse-reordering-securing-ranging-against-relay-and-physical-layer-attacks/.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

July 20, 2022

Dimitris Psillakis
President and Chief Executive Officer
Mercedes-Benz USA, L.L.C.
One Mercedes-Benz Drive
Sandy Springs, GA 30328

Dear Mr. Psillakis,

I write to request information about the security of Mercedes-Benz's motor vehicle keyless entry systems. Keyless entry systems — which allow users to enter a vehicle and start its engine without inserting and turning a key — likely helped reduce vehicle thefts since the 1990s, but the dramatic 30-year decline has suddenly gone into reverse. Although the exact cause of this turnaround is unclear, a growing body of evidence suggests that keyless entry systems may play a role. We therefore urge Mercedes-Benz to take all necessary steps to ensure that keyless entry systems, once a security innovation that deterred thieves, do not become a security liability for them to exploit.

After their adoption in the 1990s, keyless entry systems contributed to the impressive decline in car thefts from 1990 to 2019. These systems come in different forms. Some simply allow the driver to enter a vehicle without inserting a physical key into the door lock, while others, called passive entry systems, allow the driver to start the vehicle without inserting a physical key into the ignition. In both cases, the vehicle and a key fob communicate through radio signals, and an "engine immobilizer" prevents the vehicle from starting unless the key fob is nearby.

These systems were a critical advancement in vehicle security. Old-fashioned "hotwiring" a vehicle — that is, bypassing the ignition and starting a vehicle without a key — became far more difficult; with keyless entry systems, cars would not start unless they detected, through the radio signals, the presence of the key fob. In 1995, the European Union required manufacturers to include engine immobilizers on all new vehicles within three years, and Australia and Canada passed similar laws soon thereafter. One study estimated that the EU mandate reduced vehicle thefts in the Netherlands from 1995 to 2008 by 40 percent.[1] The United States never imposed a similar requirement, but many manufacturers have voluntarily adopted keyless entry systems, and car thefts per capita decreased by two-thirds from 1990 to 2019.[2]

---

[1] Jan C. van Ours and Ben Vollaard, *The Engine Immobiliser: A Non-Starter for Car Thieves*, 126 ECON. J. 1264, 1266 (2016), https://onlinelibrary.wiley.com/doi/abs/10.1111/ecoj.12196.

[2] Crime Data Explorer, FED. BUREAU OF INVESTIGATIONS, https://crime-data-explorer.app.cloud.gov/pages/explorer/crime/crime-trend (select "1990" in "From" and "2019" in "To" and "Motor vehicle theft" in "Crime Select").

Although this decrease tracked the overall decline in violent and property crime,[3] news reports have nevertheless attributed part of the decline to the adoption of keyless ignitions.[4]

This remarkably consistent trend towards fewer vehicle thefts, however, has made a concerning U-turn since the end of 2019. According to data compiled by the Federal Bureau of Investigation (FBI), U.S. car thefts per capita increased nationally by 11.8 percent in 2020.[5] Although national data has not yet been released for 2021, news reports suggest that car thefts continued to accelerate across the country last year. For example, in 2021, the number of car thefts appears to have increased by 132 percent in Milwaukee,[6] 70 percent in Washington, DC,[7] and 60 percent in Philadelphia.[8] This trend appears to have continued into 2022. So far this year, as compared with the same period in 2021, the number of car thefts has increased 74 percent in Portland, Ore.,[9] 54 percent in Richmond, Va.,[10] and 51 percent in New York City.[11] After so many years of progress, this rapid reversal in car thefts is alarming.

The same keyless entry systems that contributed to the decline in car thefts may now be providing an opportunity for thieves. Keyless entry systems are vulnerable in two ways. First, drivers may leave their key fobs in their cars, allowing a thief to easily start and steal a vehicle.[12] Whereas drivers used to have to remove the physical key from the ignition when they exited the vehicle, no similar action is necessary when a driver need only push a button to start or stop an engine. According to the New York Police Department, roughly 40 percent of car thefts in New York City so far this year were the result of motorists leaving their vehicles running or unlocked, often with keys or a key fob inside.[13] Keyless technology has thus escalated the consequences of ordinary human error.

---

[3] *Id.* (select "All Property Crimes" or "All Violent Crimes" in "Crime Select").

[4] *See, e.g.,* Sarah Maslin Nir, *Here's Why Car Thefts Are Soaring (Hint: Check Your Cup Holder)*, N.Y. TIMES (Jan. 6, 2021), www.nytimes.com/2021/01/06/nyregion/car-thefts-nyc.html; Brad Stone, *Pinch My Ride*, Wired (Aug. 1, 2006), www.wired.com/2006/08/carkey/.

[5] Crime Data Explorer, *supra* note 3 (select "2019" in "From" and "2020" in "To" and "Motor vehicle theft" in "Crime Select").

[6] *See* Teddy Nykiel, *Over 500% Spike in Auto Thefts Troubles Downtown*, MILWAUKEE BUS. J. (Feb. 9, 2022), https://www.bizjournals.com/milwaukee/news/2022/02/09/crime-statistics-mpd-2021-car-lefts.html.

[7] *See* Bruce Leshan, *Surge in Carjackings, Car Thefts Has Police Struggling to Respond*, WUSA (Feb. 9, 2021), www.wusa9.com/article/news/crime/surge-in-carjackings-car-thefts-dc-police-form-task-force/65-8c4b0c03-e343-430e-9c77-c5d9daade558.

[8] *See* Chad Pradelli and Cheryl Mettendorf, *Action News Investigation into Rise of Dealership Auto Thefts in Philadelphia Region*, ABC ACTION NEWS (Jan. 14, 2022), 6abc.com/car-thefts-auto-dealerships-6abc-investigation-barbera-autoland/11464047/.

[9] *See* Stolen Vehicle Statistics, CITY OF PORTLAND, https://www.portlandoregon.gov/police/74369 (compare selecting Jan. – May 2022 with Jan. – May 2021 in "Filter by Reported Date of Theft").

[10] *See* Henry Graff, *Richmond Police See 54% Increase in Vehicle Thefts Over Last Year*, NBC12 (Apr. 7, 2022), www.nbc12.com/2022/04/07/richmond-police-see-54-increase-vehicle-thefts-over-last-year/.

[11] *See* Rocco Parascandola, *NYPD Reports 51% Surge in Stolen Cars This Year*, N.Y. DAILY NEWS (June 12, 2022), www.nydailynews.com/new-york/nyc-crime/ny-car-vehicle-theft-surge-careless-motorists-nypd-20220612-eojbb2hhx5a3tn34vzhilc2fdq-story.html.

[12] *See* Nathan Bomey, *Thieves strike: Auto Theft Spikes During the Pandemic as Cars Are Left Unattended*, USA TODAY (Aug. 31, 2021), usatoday.com/story/money/cars/2021/08/31/auto-theft-spikes-stolen-car-vehicle-theft-pandemic-nicb/5652615001/.

[13] Rocco Parascandola, *supra* note 11.

Second, and perhaps more worryingly, a common type of keyless entry system that allows a driver to unlock and start the vehicle without needing to touch the key — known as a passive entry system — appear to be vulnerable to a "relay attack," in which a thief uses a signal amplifier to fool the car into believing that the owner is nearby.[14] Researchers have long known that bad actors could amplify radio signals emitted from the vehicle and key, allowing them to enter and start a vehicle even if the fob is nowhere nearby.[15] In recent years, devices that enable relay attacks have become widely available,[16] and news reports have identified thefts involving relay attacks in Austin,[17] Cincinnati,[18] and Los Angeles.[19]

More recently, researchers have shown that carmakers that use Bluetooth Low Energy (BLE) entry systems — which uses Bluetooth technology to determine whether the vehicle is within a certain distance of the connected device — are also vulnerable to theft using similar relay technology, affecting manufacturers such as Tesla that have adopted BLE passive entry systems.[20] For that reason, the Bluetooth Special Interest Group, the standard-setting organization that oversees the development of Bluetooth technologies, warns that BLE "should not be used as the only protection of valuable assets."[21] Car manufacturers have only recently begun using BLE technology to determine the proximity of a key fob, so researchers have not yet confirmed any vehicles stolen through a BLE relay attack. However, as manufacturers increasingly equip devices — such as smart locks for homes[22] — with BLE passive entry systems, this vulnerability could put a broad range of critical security systems at risk.

Fortunately, researchers have also identified methods to mitigate the risk of passive entry thefts. For example, manufacturers can prevent a fob from unlocking a vehicle if the fob was not recently in motion, as typically occurs as a driver approaches a vehicle. In other words, if the fob is idle, the driver is likely not trying to unlock their own vehicle; any attempt to use the fob in that state may be a sign of a relay attack. Similarly, manufacturers could require consumers to complete an additional verification, such as inputting a PIN number, to enter the vehicle. While such systems inherently inconvenience consumers, they also are a strong defense against relay

---

[14] Rachel Wait, *Keyless Car Crime: How to Thwart the Thieves*, FORBES ADVISOR (Mar. 24, 2022), www.forbes.com/uk/advisor/car-insurance/keyless-car-crime/.

[15] *See* ARI JUELS, RFID SECURITY AND PRIVACY: A RESEARCH SURVEY 13 (2005), www.arijuels.com/wp-content/uploads/2013/09/J06a.pdf.

[16] *See* Joseph Cox, *Meet the Guy Selling Wireless Tech to Steal Luxury Cars in Seconds*, VICE NEWS (Feb. 11, 2020), www.vice.com/en/article/7kz48x/guy-selling-relay-attack-keyless-repeaters-to-steal-cars.

[17] *See* Bettie Cross, *Car Thieves Are Hacking Key Fobs to Quickly and Quietly Steal Vehicles*, CBS AUSTIN (May 12, 2022), cbsaustin.com/news/local/car-thieves-are-hacking-key-fobs-to-quickly-and-quietly-steal-vehicles.

[18] *See* Jatara McGee, *Hackers Are Using New Tech to Steal Locked Cars Without Keys*, WLWT (May 9, 2019), www.wlwt.com/article/hackers-are-using-new-tech-to-steal-locked-cars-without-keys/27424367#.

[19] *See* Nick Bilton, *Keeping Your Car Safe From Electronic Thieves*, N.Y. TIMES (Apr. 15, 2015), www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html.

[20] *See* Sultan Khan, *Technical Advisory – Tesla BLE Phone-as-a-Key Passive Entry Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-tesla-ble-phone-as-a-key-passive-entry-vulnerable-to-relay-attacks/.

[21] BLUETOOTH SIG, PROXIMITY PROFILE 17 (2015), www.bluetooth.com/specifications/specs/proximity-profile-1-0-1/.

[22] *See* Sultan Khan, *Technical Advisory – Kwikset/Weiser BLE Proximity Authentication in Kevo Smart Locks Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-kwikset-weiser-ble-proximity-authentication-in-kevo-smart-locks-vulnerable-to-relay-attacks/.

attacks. Finally, automakers could also adopt Ultra-Wide-Band (UWB) technology, which enables a precise measurement between the vehicle and key fob and, in combination with other technologies, allows the vehicle to determine if the radio signal has been improperly amplified. Experts have suggested that UWB technology could significantly reduce the risk of relay theft.[23]

Given the recent surge in vehicle thefts and the potential security risks involved in keyless entry systems, I respectfully request that you respond in writing to the following questions by August 10, 2022:

1. Please provide the following data, as available, on thefts of vehicles manufactured by your company:

    a. How many vehicles manufactured by your company were stolen in 2019, 2020, 2021, and through the first six months of 2022?

    b. Of those vehicle thefts, how many were caused by thieves taking advantage of key fobs left in vehicles?

    c. Of those vehicle thefts, how many were caused by relay attacks?

2. Please describe the type of transponder and the technology standard that vehicles manufactured by your company use to communicate with key fobs and other devices. If vehicles manufactured by your company use different types of transponders and technology standards, please provide information on all types.

3. Please describe the testing that your company has done to assess the security of its keyless entry systems.

4. What specific steps has your company taken to reduce the vulnerability of its keyless entry system?

    a. Has your company considered making the keyless entry system motion activated?

    b. Has your company considered adopting Ultra-Wide-Band technology?

    c. Has your company considered creating mechanisms to alert owners if their key fob is left inside the vehicle?

5. Does your company plan to take any further steps to reduce any vulnerability of its keyless entry system?

Thank you for your prompt attention to these questions.

---

[23] *See e.g.,* Mridula Singh et al., *UWB with Pulse Reordering: Securing Ranging against Relay and Physical-Layer Attacks*, NETWORK AND DISTRIB. SYS, SEC. SYMP. (2019), www.ndss-symposium.org/ndss-paper/uwb-with-pulse-reordering-securing-ranging-against-relay-and-physical-layer-attacks/.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

July 20, 2022

Mark Chaffin
President and Chief Executive Officer
Mitsubishi Motors North America, Inc.
4031 Aspen Grove Drive
Franklin, TN 37067

Dear Mr. Chaffin,

I write to request information about the security of Mitsubishi's motor vehicle keyless entry systems. Keyless entry systems — which allow users to enter a vehicle and start its engine without inserting and turning a key — likely helped reduce vehicle thefts since the 1990s, but the dramatic 30-year decline has suddenly gone into reverse. Although the exact cause of this turnaround is unclear, a growing body of evidence suggests that keyless entry systems may play a role. We therefore urge Mitsubishi to take all necessary steps to ensure that keyless entry systems, once a security innovation that deterred thieves, do not become a security liability for them to exploit.

After their adoption in the 1990s, keyless entry systems contributed to the impressive decline in car thefts from 1990 to 2019. These systems come in different forms. Some simply allow the driver to enter a vehicle without inserting a physical key into the door lock, while others, called passive entry systems, allow the driver to start the vehicle without inserting a physical key into the ignition. In both cases, the vehicle and a key fob communicate through radio signals, and an "engine immobilizer" prevents the vehicle from starting unless the key fob is nearby.

These systems were a critical advancement in vehicle security. Old-fashioned "hotwiring" a vehicle — that is, bypassing the ignition and starting a vehicle without a key — became far more difficult; with keyless entry systems, cars would not start unless they detected, through the radio signals, the presence of the key fob. In 1995, the European Union required manufacturers to include engine immobilizers on all new vehicles within three years, and Australia and Canada passed similar laws soon thereafter. One study estimated that the EU mandate reduced vehicle thefts in the Netherlands from 1995 to 2008 by 40 percent.[1] The United States never imposed a similar requirement, but many manufacturers have voluntarily adopted keyless entry systems, and car thefts per capita decreased by two-thirds from 1990 to 2019.[2]

[1] Jan C. van Ours and Ben Vollaard, *The Engine Immobiliser: A Non-Starter for Car Thieves*, 126 ECON. J. 1264, 1266 (2016), https://onlinelibrary.wiley.com/doi/abs/10.1111/ecoj.12196.

[2] Crime Data Explorer, FED. BUREAU OF INVESTIGATIONS, https://crime-data-explorer.app.cloud.gov/pages/explorer/crime/crime-trend (select "1990" in "From" and "2019" in "To" and "Motor vehicle theft" in "Crime Select").

Although this decrease tracked the overall decline in violent and property crime,[3] news reports have nevertheless attributed part of the decline to the adoption of keyless ignitions.[4]

This remarkably consistent trend towards fewer vehicle thefts, however, has made a concerning U-turn since the end of 2019. According to data compiled by the Federal Bureau of Investigation (FBI), U.S. car thefts per capita increased nationally by 11.8 percent in 2020.[5] Although national data has not yet been released for 2021, news reports suggest that car thefts continued to accelerate across the country last year. For example, in 2021, the number of car thefts appears to have increased by 132 percent in Milwaukee,[6] 70 percent in Washington, DC,[7] and 60 percent in Philadelphia.[8] This trend appears to have continued into 2022. So far this year, as compared with the same period in 2021, the number of car thefts has increased 74 percent in Portland, Ore.,[9] 54 percent in Richmond, Va.,[10] and 51 percent in New York City.[11] After so many years of progress, this rapid reversal in car thefts is alarming.

The same keyless entry systems that contributed to the decline in car thefts may now be providing an opportunity for thieves. Keyless entry systems are vulnerable in two ways. First, drivers may leave their key fobs in their cars, allowing a thief to easily start and steal a vehicle.[12] Whereas drivers used to have to remove the physical key from the ignition when they exited the vehicle, no similar action is necessary when a driver need only push a button to start or stop an engine. According to the New York Police Department, roughly 40 percent of car thefts in New York City so far this year were the result of motorists leaving their vehicles running or unlocked, often with keys or a key fob inside.[13] Keyless technology has thus escalated the consequences of ordinary human error.

---

[3] *Id.* (select "All Property Crimes" or "All Violent Crimes" in "Crime Select").

[4] *See, e.g.,* Sarah Maslin Nir, *Here's Why Car Thefts Are Soaring (Hint: Check Your Cup Holder)*, N.Y. TIMES (Jan. 6, 2021), www.nytimes.com/2021/01/06/nyregion/car-thefts-nyc.html; Brad Stone, *Pinch My Ride*, Wired (Aug. 1, 2006), www.wired.com/2006/08/carkey/.

[5] Crime Data Explorer, *supra* note 3 (select "2019" in "From" and "2020" in "To" and "Motor vehicle theft" in "Crime Select").

[6] *See* Teddy Nykiel, *Over 500% Spike in Auto Thefts Troubles Downtown*, MILWAUKEE BUS. J. (Feb. 9, 2022), https://www.bizjournals.com/milwaukee/news/2022/02/09/crime-statistics-mpd-2021-car-lefts.html.

[7] *See* Bruce Leshan, *Surge in Carjackings, Car Thefts Has Police Struggling to Respond*, WUSA (Feb. 9, 2021), www.wusa9.com/article/news/crime/surge-in-carjackings-car-thefts-dc-police-form-task-force/65-8c4b0c03-e343-430e-9c77-c5d9daade558.

[8] *See* Chad Pradelli and Cheryl Mettendorf, *Action News Investigation into Rise of Dealership Auto Thefts in Philadelphia Region*, ABC ACTION NEWS (Jan. 14, 2022), 6abc.com/car-thefts-auto-dealerships-6abc-investigation-barbera-autoland/11464047/.

[9] *See* Stolen Vehicle Statistics, CITY OF PORTLAND, https://www.portlandoregon.gov/police/74369 (compare selecting Jan. – May 2022 with Jan. – May 2021 in "Filter by Reported Date of Theft").

[10] *See* Henry Graff, *Richmond Police See 54% Increase in Vehicle Thefts Over Last Year*, NBC12 (Apr. 7, 2022), www.nbc12.com/2022/04/07/richmond-police-see-54-increase-vehicle-thefts-over-last-year/.

[11] *See* Rocco Parascandola, *NYPD Reports 51% Surge in Stolen Cars This Year*, N.Y. DAILY NEWS (June 12, 2022), www.nydailynews.com/new-york/nyc-crime/ny-car-vehicle-theft-surge-careless-motorists-nypd-20220612-eojbb2hhx5a3tn34vzhilc2fdq-story.html.

[12] *See* Nathan Bomey, *Thieves strike: Auto Theft Spikes During the Pandemic as Cars Are Left Unattended*, USA TODAY (Aug. 31, 2021), usatoday.com/story/money/cars/2021/08/31/auto-theft-spikes-stolen-car-vehicle-theft-pandemic-nicb/5652615001/.

[13] Rocco Parascandola, *supra* note 11.

Second, and perhaps more worryingly, a common type of keyless entry system that allows a driver to unlock and start the vehicle without needing to touch the key — known as a passive entry system — appear to be vulnerable to a "relay attack," in which a thief uses a signal amplifier to fool the car into believing that the owner is nearby.[14] Researchers have long known that bad actors could amplify radio signals emitted from the vehicle and key, allowing them to enter and start a vehicle even if the fob is nowhere nearby.[15] In recent years, devices that enable relay attacks have become widely available,[16] and news reports have identified thefts involving relay attacks in Austin,[17] Cincinnati,[18] and Los Angeles.[19]

More recently, researchers have shown that carmakers that use Bluetooth Low Energy (BLE) entry systems — which uses Bluetooth technology to determine whether the vehicle is within a certain distance of the connected device — are also vulnerable to theft using similar relay technology, affecting manufacturers such as Tesla that have adopted BLE passive entry systems.[20] For that reason, the Bluetooth Special Interest Group, the standard-setting organization that oversees the development of Bluetooth technologies, warns that BLE "should not be used as the only protection of valuable assets."[21] Car manufacturers have only recently begun using BLE technology to determine the proximity of a key fob, so researchers have not yet confirmed any vehicles stolen through a BLE relay attack. However, as manufacturers increasingly equip devices — such as smart locks for homes[22] — with BLE passive entry systems, this vulnerability could put a broad range of critical security systems at risk.

Fortunately, researchers have also identified methods to mitigate the risk of passive entry thefts. For example, manufacturers can prevent a fob from unlocking a vehicle if the fob was not recently in motion, as typically occurs as a driver approaches a vehicle. In other words, if the fob is idle, the driver is likely not trying to unlock their own vehicle; any attempt to use the fob in that state may be a sign of a relay attack. Similarly, manufacturers could require consumers to complete an additional verification, such as inputting a PIN number, to enter the vehicle. While such systems inherently inconvenience consumers, they also are a strong defense against relay

---

[14] Rachel Wait, *Keyless Car Crime: How to Thwart the Thieves*, FORBES ADVISOR (Mar. 24, 2022), www.forbes.com/uk/advisor/car-insurance/keyless-car-crime/.

[15] *See* ARI JUELS, RFID SECURITY AND PRIVACY: A RESEARCH SURVEY 13 (2005), www.arijuels.com/wp-content/uploads/2013/09/J06a.pdf.

[16] *See* Joseph Cox, *Meet the Guy Selling Wireless Tech to Steal Luxury Cars in Seconds*, VICE NEWS (Feb. 11, 2020), www.vice.com/en/article/7kz48x/guy-selling-relay-attack-keyless-repeaters-to-steal-cars.

[17] *See* Bettie Cross, *Car Thieves Are Hacking Key Fobs to Quickly and Quietly Steal Vehicles*, CBS AUSTIN (May 12, 2022), cbsaustin.com/news/local/car-thieves-are-hacking-key-fobs-to-quickly-and-quietly-steal-vehicles.

[18] *See* Jatara McGee, *Hackers Are Using New Tech to Steal Locked Cars Without Keys*, WLWT (May 9, 2019), www.wlwt.com/article/hackers-are-using-new-tech-to-steal-locked-cars-without-keys/27424367#.

[19] *See* Nick Bilton, *Keeping Your Car Safe From Electronic Thieves*, N.Y. TIMES (Apr. 15, 2015), www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html.

[20] *See* Sultan Khan, *Technical Advisory – Tesla BLE Phone-as-a-Key Passive Entry Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-tesla-ble-phone-as-a-key-passive-entry-vulnerable-to-relay-attacks/.

[21] BLUETOOTH SIG, PROXIMITY PROFILE 17 (2015), www.bluetooth.com/specifications/specs/proximity-profile-1-0-1/.

[22] *See* Sultan Khan, *Technical Advisory – Kwikset/Weiser BLE Proximity Authentication in Kevo Smart Locks Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-kwikset-weiser-ble-proximity-authentication-in-kevo-smart-locks-vulnerable-to-relay-attacks/.

attacks. Finally, automakers could also adopt Ultra-Wide-Band (UWB) technology, which enables a precise measurement between the vehicle and key fob and, in combination with other technologies, allows the vehicle to determine if the radio signal has been improperly amplified. Experts have suggested that UWB technology could significantly reduce the risk of relay theft.[23]

Given the recent surge in vehicle thefts and the potential security risks involved in keyless entry systems, I respectfully request that you respond in writing to the following questions by August 10, 2022:

1. Please provide the following data, as available, on thefts of vehicles manufactured by your company:

    a. How many vehicles manufactured by your company were stolen in 2019, 2020, 2021, and through the first six months of 2022?

    b. Of those vehicle thefts, how many were caused by thieves taking advantage of key fobs left in vehicles?

    c. Of those vehicle thefts, how many were caused by relay attacks?

2. Please describe the type of transponder and the technology standard that vehicles manufactured by your company use to communicate with key fobs and other devices. If vehicles manufactured by your company use different types of transponders and technology standards, please provide information on all types.

3. Please describe the testing that your company has done to assess the security of its keyless entry systems.

4. What specific steps has your company taken to reduce the vulnerability of its keyless entry system?

    a. Has your company considered making the keyless entry system motion activated?

    b. Has your company considered adopting Ultra-Wide-Band technology?

    c. Has your company considered creating mechanisms to alert owners if their key fob is left inside the vehicle?

5. Does your company plan to take any further steps to reduce any vulnerability of its keyless entry system?

Thank you for your prompt attention to these questions.

---

[23] *See e.g.,* Mridula Singh et al., *UWB with Pulse Reordering: Securing Ranging against Relay and Physical-Layer Attacks*, NETWORK AND DISTRIB. SYS, SEC. SYMP. (2019), www.ndss-symposium.org/ndss-paper/uwb-with-pulse-reordering-securing-ranging-against-relay-and-physical-layer-attacks/.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

July 20, 2022

Jérémie Papin
Chairperson
Nissan North America, Inc.
One Nissan Way
Franklin, TN 37067

Dear Mr. Papin,

I write to request information about the security of Nissan's motor vehicle keyless entry systems. Keyless entry systems — which allow users to enter a vehicle and start its engine without inserting and turning a key — likely helped reduce vehicle thefts since the 1990s, but the dramatic 30-year decline has suddenly gone into reverse. Although the exact cause of this turnaround is unclear, a growing body of evidence suggests that keyless entry systems may play a role. We therefore urge Nissan to take all necessary steps to ensure that keyless entry systems, once a security innovation that deterred thieves, do not become a security liability for them to exploit.

After their adoption in the 1990s, keyless entry systems contributed to the impressive decline in car thefts from 1990 to 2019. These systems come in different forms. Some simply allow the driver to enter a vehicle without inserting a physical key into the door lock, while others, called passive entry systems, allow the driver to start the vehicle without inserting a physical key into the ignition. In both cases, the vehicle and a key fob communicate through radio signals, and an "engine immobilizer" prevents the vehicle from starting unless the key fob is nearby.

These systems were a critical advancement in vehicle security. Old-fashioned "hotwiring" a vehicle — that is, bypassing the ignition and starting a vehicle without a key — became far more difficult; with keyless entry systems, cars would not start unless they detected, through the radio signals, the presence of the key fob. In 1995, the European Union required manufacturers to include engine immobilizers on all new vehicles within three years, and Australia and Canada passed similar laws soon thereafter. One study estimated that the EU mandate reduced vehicle thefts in the Netherlands from 1995 to 2008 by 40 percent.[1] The United States never imposed a similar requirement, but many manufacturers have voluntarily adopted keyless entry systems, and car thefts per capita decreased by two-thirds from 1990 to 2019.[2]

[1] Jan C. van Ours and Ben Vollaard, *The Engine Immobiliser: A Non-Starter for Car Thieves*, 126 ECON. J. 1264, 1266 (2016), https://onlinelibrary.wiley.com/doi/abs/10.1111/ecoj.12196.

[2] Crime Data Explorer, FED. BUREAU OF INVESTIGATIONS, https://crime-data-explorer.app.cloud.gov/pages/explorer/crime/crime-trend (select "1990" in "From" and "2019" in "To" and "Motor vehicle theft" in "Crime Select").

Although this decrease tracked the overall decline in violent and property crime,[3] news reports have nevertheless attributed part of the decline to the adoption of keyless ignitions.[4]

This remarkably consistent trend towards fewer vehicle thefts, however, has made a concerning U-turn since the end of 2019. According to data compiled by the Federal Bureau of Investigation (FBI), U.S. car thefts per capita increased nationally by 11.8 percent in 2020.[5] Although national data has not yet been released for 2021, news reports suggest that car thefts continued to accelerate across the country last year. For example, in 2021, the number of car thefts appears to have increased by 132 percent in Milwaukee,[6] 70 percent in Washington, DC,[7] and 60 percent in Philadelphia.[8] This trend appears to have continued into 2022. So far this year, as compared with the same period in 2021, the number of car thefts has increased 74 percent in Portland, Ore.,[9] 54 percent in Richmond, Va.,[10] and 51 percent in New York City.[11] After so many years of progress, this rapid reversal in car thefts is alarming.

The same keyless entry systems that contributed to the decline in car thefts may now be providing an opportunity for thieves. Keyless entry systems are vulnerable in two ways. First, drivers may leave their key fobs in their cars, allowing a thief to easily start and steal a vehicle.[12] Whereas drivers used to have to remove the physical key from the ignition when they exited the vehicle, no similar action is necessary when a driver need only push a button to start or stop an engine. According to the New York Police Department, roughly 40 percent of car thefts in New York City so far this year were the result of motorists leaving their vehicles running or unlocked, often with keys or a key fob inside.[13] Keyless technology has thus escalated the consequences of ordinary human error.

---

[3] *Id.* (select "All Property Crimes" or "All Violent Crimes" in "Crime Select").

[4] *See, e.g.,* Sarah Maslin Nir, *Here's Why Car Thefts Are Soaring (Hint: Check Your Cup Holder)*, N.Y. TIMES (Jan. 6, 2021), www.nytimes.com/2021/01/06/nyregion/car-thefts-nyc.html; Brad Stone, *Pinch My Ride*, Wired (Aug. 1, 2006), www.wired.com/2006/08/carkey/.

[5] Crime Data Explorer, *supra* note 3 (select "2019" in "From" and "2020" in "To" and "Motor vehicle theft" in "Crime Select").

[6] *See* Teddy Nykiel, *Over 500% Spike in Auto Thefts Troubles Downtown*, MILWAUKEE BUS. J. (Feb. 9, 2022), https://www.bizjournals.com/milwaukee/news/2022/02/09/crime-statistics-mpd-2021-car-lefts.html.

[7] *See* Bruce Leshan, *Surge in Carjackings, Car Thefts Has Police Struggling to Respond*, WUSA (Feb. 9, 2021), www.wusa9.com/article/news/crime/surge-in-carjackings-car-thefts-dc-police-form-task-force/65-8c4b0c03-e343-430e-9c77-c5d9daade558.

[8] *See* Chad Pradelli and Cheryl Mettendorf, *Action News Investigation into Rise of Dealership Auto Thefts in Philadelphia Region*, ABC ACTION NEWS (Jan. 14, 2022), 6abc.com/car-thefts-auto-dealerships-6abc-investigation-barbera-autoland/11464047/.

[9] *See* Stolen Vehicle Statistics, CITY OF PORTLAND, https://www.portlandoregon.gov/police/74369 (compare selecting Jan. – May 2022 with Jan. – May 2021 in "Filter by Reported Date of Theft").

[10] *See* Henry Graff, *Richmond Police See 54% Increase in Vehicle Thefts Over Last Year*, NBC12 (Apr. 7, 2022), www.nbc12.com/2022/04/07/richmond-police-see-54-increase-vehicle-thefts-over-last-year/.

[11] *See* Rocco Parascandola, *NYPD Reports 51% Surge in Stolen Cars This Year*, N.Y. DAILY NEWS (June 12, 2022), www.nydailynews.com/new-york/nyc-crime/ny-car-vehicle-theft-surge-careless-motorists-nypd-20220612-eojbb2hhx5a3tn34vzhilc2fdq-story.html.

[12] *See* Nathan Bomey, *Thieves strike: Auto Theft Spikes During the Pandemic as Cars Are Left Unattended*, USA TODAY (Aug. 31, 2021), usatoday.com/story/money/cars/2021/08/31/auto-theft-spikes-stolen-car-vehicle-theft-pandemic-nicb/5652615001/.

[13] Rocco Parascandola, *supra* note 11.

Second, and perhaps more worryingly, a common type of keyless entry system that allows a driver to unlock and start the vehicle without needing to touch the key — known as a passive entry system — appear to be vulnerable to a "relay attack," in which a thief uses a signal amplifier to fool the car into believing that the owner is nearby.[14] Researchers have long known that bad actors could amplify radio signals emitted from the vehicle and key, allowing them to enter and start a vehicle even if the fob is nowhere nearby.[15] In recent years, devices that enable relay attacks have become widely available,[16] and news reports have identified thefts involving relay attacks in Austin,[17] Cincinnati,[18] and Los Angeles.[19]

More recently, researchers have shown that carmakers that use Bluetooth Low Energy (BLE) entry systems — which uses Bluetooth technology to determine whether the vehicle is within a certain distance of the connected device — are also vulnerable to theft using similar relay technology, affecting manufacturers such as Tesla that have adopted BLE passive entry systems.[20] For that reason, the Bluetooth Special Interest Group, the standard-setting organization that oversees the development of Bluetooth technologies, warns that BLE "should not be used as the only protection of valuable assets."[21] Car manufacturers have only recently begun using BLE technology to determine the proximity of a key fob, so researchers have not yet confirmed any vehicles stolen through a BLE relay attack. However, as manufacturers increasingly equip devices — such as smart locks for homes[22] — with BLE passive entry systems, this vulnerability could put a broad range of critical security systems at risk.

Fortunately, researchers have also identified methods to mitigate the risk of passive entry thefts. For example, manufacturers can prevent a fob from unlocking a vehicle if the fob was not recently in motion, as typically occurs as a driver approaches a vehicle. In other words, if the fob is idle, the driver is likely not trying to unlock their own vehicle; any attempt to use the fob in that state may be a sign of a relay attack. Similarly, manufacturers could require consumers to complete an additional verification, such as inputting a PIN number, to enter the vehicle. While such systems inherently inconvenience consumers, they also are a strong defense against relay

---

[14] Rachel Wait, *Keyless Car Crime: How to Thwart the Thieves*, FORBES ADVISOR (Mar. 24, 2022), www.forbes.com/uk/advisor/car-insurance/keyless-car-crime/.

[15] *See* ARI JUELS, RFID SECURITY AND PRIVACY: A RESEARCH SURVEY 13 (2005), www.arijuels.com/wp-content/uploads/2013/09/J06a.pdf.

[16] *See* Joseph Cox, *Meet the Guy Selling Wireless Tech to Steal Luxury Cars in Seconds*, VICE NEWS (Feb. 11, 2020), www.vice.com/en/article/7kz48x/guy-selling-relay-attack-keyless-repeaters-to-steal-cars.

[17] *See* Bettie Cross, *Car Thieves Are Hacking Key Fobs to Quickly and Quietly Steal Vehicles*, CBS AUSTIN (May 12, 2022), cbsaustin.com/news/local/car-thieves-are-hacking-key-fobs-to-quickly-and-quietly-steal-vehicles.

[18] *See* Jatara McGee, *Hackers Are Using New Tech to Steal Locked Cars Without Keys*, WLWT (May 9, 2019), www.wlwt.com/article/hackers-are-using-new-tech-to-steal-locked-cars-without-keys/27424367#.

[19] *See* Nick Bilton, *Keeping Your Car Safe From Electronic Thieves*, N.Y. TIMES (Apr. 15, 2015), www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html.

[20] *See* Sultan Khan, *Technical Advisory – Tesla BLE Phone-as-a-Key Passive Entry Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-tesla-ble-phone-as-a-key-passive-entry-vulnerable-to-relay-attacks/.

[21] BLUETOOTH SIG, PROXIMITY PROFILE 17 (2015), www.bluetooth.com/specifications/specs/proximity-profile-1-0-1/.

[22] *See* Sultan Khan, *Technical Advisory – Kwikset/Weiser BLE Proximity Authentication in Kevo Smart Locks Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-kwikset-weiser-ble-proximity-authentication-in-kevo-smart-locks-vulnerable-to-relay-attacks/.

attacks. Finally, automakers could also adopt Ultra-Wide-Band (UWB) technology, which enables a precise measurement between the vehicle and key fob and, in combination with other technologies, allows the vehicle to determine if the radio signal has been improperly amplified. Experts have suggested that UWB technology could significantly reduce the risk of relay theft.[23]

Given the recent surge in vehicle thefts and the potential security risks involved in keyless entry systems, I respectfully request that you respond in writing to the following questions by August 10, 2022:

1. Please provide the following data, as available, on thefts of vehicles manufactured by your company:

    a. How many vehicles manufactured by your company were stolen in 2019, 2020, 2021, and through the first six months of 2022?

    b. Of those vehicle thefts, how many were caused by thieves taking advantage of key fobs left in vehicles?

    c. Of those vehicle thefts, how many were caused by relay attacks?

2. Please describe the type of transponder and the technology standard that vehicles manufactured by your company use to communicate with key fobs and other devices. If vehicles manufactured by your company use different types of transponders and technology standards, please provide information on all types.

3. Please describe the testing that your company has done to assess the security of its keyless entry systems.

4. What specific steps has your company taken to reduce the vulnerability of its keyless entry system?

    a. Has your company considered making the keyless entry system motion activated?

    b. Has your company considered adopting Ultra-Wide-Band technology?

    c. Has your company considered creating mechanisms to alert owners if their key fob is left inside the vehicle?

5. Does your company plan to take any further steps to reduce any vulnerability of its keyless entry system?

Thank you for your prompt attention to these questions.

---

[23] *See e.g.,* Mridula Singh et al., *UWB with Pulse Reordering: Securing Ranging against Relay and Physical-Layer Attacks*, NETWORK AND DISTRIB. SYS, SEC. SYMP. (2019), www.ndss-symposium.org/ndss-paper/uwb-with-pulse-reordering-securing-ranging-against-relay-and-physical-layer-attacks/.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

July 20, 2022

Mark Stewart
Chief Operating Officer
Stellantis North America
1000 Chrysler Dr.
Auburn Hills, MI 48326

Dear Mr. Stewart,

I write to request information about the security of Stellantis' motor vehicle keyless entry systems. Keyless entry systems — which allow users to enter a vehicle and start its engine without inserting and turning a key — likely helped reduce vehicle thefts since the 1990s, but the dramatic 30-year decline has suddenly gone into reverse. Although the exact cause of this turnaround is unclear, a growing body of evidence suggests that keyless entry systems may play a role. We therefore urge Stellantis to take all necessary steps to ensure that keyless entry systems, once a security innovation that deterred thieves, do not become a security liability for them to exploit.

After their adoption in the 1990s, keyless entry systems contributed to the impressive decline in car thefts from 1990 to 2019. These systems come in different forms. Some simply allow the driver to enter a vehicle without inserting a physical key into the door lock, while others, called passive entry systems, allow the driver to start the vehicle without inserting a physical key into the ignition. In both cases, the vehicle and a key fob communicate through radio signals, and an "engine immobilizer" prevents the vehicle from starting unless the key fob is nearby.

These systems were a critical advancement in vehicle security. Old-fashioned "hotwiring" a vehicle — that is, bypassing the ignition and starting a vehicle without a key — became far more difficult; with keyless entry systems, cars would not start unless they detected, through the radio signals, the presence of the key fob. In 1995, the European Union required manufacturers to include engine immobilizers on all new vehicles within three years, and Australia and Canada passed similar laws soon thereafter. One study estimated that the EU mandate reduced vehicle thefts in the Netherlands from 1995 to 2008 by 40 percent.[1] The United States never imposed a similar requirement, but many manufacturers have voluntarily adopted keyless entry systems, and car thefts per capita decreased by two-thirds from 1990 to 2019.[2]

---

[1] Jan C. van Ours and Ben Vollaard, *The Engine Immobiliser: A Non-Starter for Car Thieves*, 126 ECON. J. 1264, 1266 (2016), https://onlinelibrary.wiley.com/doi/abs/10.1111/ecoj.12196.

[2] Crime Data Explorer, FED. BUREAU OF INVESTIGATIONS, https://crime-data-explorer.app.cloud.gov/pages/explorer/crime/crime-trend (select "1990" in "From" and "2019" in "To" and "Motor vehicle theft" in "Crime Select").

Although this decrease tracked the overall decline in violent and property crime,[3] news reports have nevertheless attributed part of the decline to the adoption of keyless ignitions.[4]

This remarkably consistent trend towards fewer vehicle thefts, however, has made a concerning U-turn since the end of 2019. According to data compiled by the Federal Bureau of Investigation (FBI), U.S. car thefts per capita increased nationally by 11.8 percent in 2020.[5] Although national data has not yet been released for 2021, news reports suggest that car thefts continued to accelerate across the country last year. For example, in 2021, the number of car thefts appears to have increased by 132 percent in Milwaukee,[6] 70 percent in Washington, DC,[7] and 60 percent in Philadelphia.[8] This trend appears to have continued into 2022. So far this year, as compared with the same period in 2021, the number of car thefts has increased 74 percent in Portland, Ore.,[9] 54 percent in Richmond, Va.,[10] and 51 percent in New York City.[11] After so many years of progress, this rapid reversal in car thefts is alarming.

The same keyless entry systems that contributed to the decline in car thefts may now be providing an opportunity for thieves. Keyless entry systems are vulnerable in two ways. First, drivers may leave their key fobs in their cars, allowing a thief to easily start and steal a vehicle.[12] Whereas drivers used to have to remove the physical key from the ignition when they exited the vehicle, no similar action is necessary when a driver need only push a button to start or stop an engine. According to the New York Police Department, roughly 40 percent of car thefts in New York City so far this year were the result of motorists leaving their vehicles running or unlocked, often with keys or a key fob inside.[13] Keyless technology has thus escalated the consequences of ordinary human error.

---

[3] *Id.* (select "All Property Crimes" or "All Violent Crimes" in "Crime Select").

[4] *See, e.g.,* Sarah Maslin Nir, *Here's Why Car Thefts Are Soaring (Hint: Check Your Cup Holder)*, N.Y. TIMES (Jan. 6, 2021), www.nytimes.com/2021/01/06/nyregion/car-thefts-nyc.html; Brad Stone, *Pinch My Ride*, Wired (Aug. 1, 2006), www.wired.com/2006/08/carkey/.

[5] Crime Data Explorer, *supra* note 3 (select "2019" in "From" and "2020" in "To" and "Motor vehicle theft" in "Crime Select").

[6] *See* Teddy Nykiel, *Over 500% Spike in Auto Thefts Troubles Downtown*, MILWAUKEE BUS. J. (Feb. 9, 2022), https://www.bizjournals.com/milwaukee/news/2022/02/09/crime-statistics-mpd-2021-car-lefts.html.

[7] *See* Bruce Leshan, *Surge in Carjackings, Car Thefts Has Police Struggling to Respond*, WUSA (Feb. 9, 2021), www.wusa9.com/article/news/crime/surge-in-carjackings-car-thefts-dc-police-form-task-force/65-8c4b0c03-e343-430e-9c77-c5d9daade558.

[8] *See* Chad Pradelli and Cheryl Mettendorf, *Action News Investigation into Rise of Dealership Auto Thefts in Philadelphia Region*, ABC ACTION NEWS (Jan. 14, 2022), 6abc.com/car-thefts-auto-dealerships-6abc-investigation-barbera-autoland/11464047/.

[9] *See* Stolen Vehicle Statistics, CITY OF PORTLAND, https://www.portlandoregon.gov/police/74369 (compare selecting Jan. – May 2022 with Jan. – May 2021 in "Filter by Reported Date of Theft").

[10] *See* Henry Graff, *Richmond Police See 54% Increase in Vehicle Thefts Over Last Year*, NBC12 (Apr. 7, 2022), www.nbc12.com/2022/04/07/richmond-police-see-54-increase-vehicle-thefts-over-last-year/.

[11] *See* Rocco Parascandola, *NYPD Reports 51% Surge in Stolen Cars This Year*, N.Y. DAILY NEWS (June 12, 2022), www.nydailynews.com/new-york/nyc-crime/ny-car-vehicle-theft-surge-careless-motorists-nypd-20220612-eojbb2hhx5a3tn34vzhilc2fdq-story.html.

[12] *See* Nathan Bomey, *Thieves strike: Auto Theft Spikes During the Pandemic as Cars Are Left Unattended*, USA TODAY (Aug. 31, 2021), usatoday.com/story/money/cars/2021/08/31/auto-theft-spikes-stolen-car-vehicle-theft-pandemic-nicb/5652615001/.

[13] Rocco Parascandola, *supra* note 11.

Second, and perhaps more worryingly, a common type of keyless entry system that allows a driver to unlock and start the vehicle without needing to touch the key — known as a passive entry system — appear to be vulnerable to a "relay attack," in which a thief uses a signal amplifier to fool the car into believing that the owner is nearby.[14] Researchers have long known that bad actors could amplify radio signals emitted from the vehicle and key, allowing them to enter and start a vehicle even if the fob is nowhere nearby.[15] In recent years, devices that enable relay attacks have become widely available,[16] and news reports have identified thefts involving relay attacks in Austin,[17] Cincinnati,[18] and Los Angeles.[19]

More recently, researchers have shown that carmakers that use Bluetooth Low Energy (BLE) entry systems — which uses Bluetooth technology to determine whether the vehicle is within a certain distance of the connected device — are also vulnerable to theft using similar relay technology, affecting manufacturers such as Tesla that have adopted BLE passive entry systems.[20] For that reason, the Bluetooth Special Interest Group, the standard-setting organization that oversees the development of Bluetooth technologies, warns that BLE "should not be used as the only protection of valuable assets."[21] Car manufacturers have only recently begun using BLE technology to determine the proximity of a key fob, so researchers have not yet confirmed any vehicles stolen through a BLE relay attack. However, as manufacturers increasingly equip devices — such as smart locks for homes[22] — with BLE passive entry systems, this vulnerability could put a broad range of critical security systems at risk.

Fortunately, researchers have also identified methods to mitigate the risk of passive entry thefts. For example, manufacturers can prevent a fob from unlocking a vehicle if the fob was not recently in motion, as typically occurs as a driver approaches a vehicle. In other words, if the fob is idle, the driver is likely not trying to unlock their own vehicle; any attempt to use the fob in that state may be a sign of a relay attack. Similarly, manufacturers could require consumers to complete an additional verification, such as inputting a PIN number, to enter the vehicle. While such systems inherently inconvenience consumers, they also are a strong defense against relay

---

[14] Rachel Wait, *Keyless Car Crime: How to Thwart the Thieves*, FORBES ADVISOR (Mar. 24, 2022), www.forbes.com/uk/advisor/car-insurance/keyless-car-crime/.

[15] *See* ARI JUELS, RFID SECURITY AND PRIVACY: A RESEARCH SURVEY 13 (2005), www.arijuels.com/wp-content/uploads/2013/09/J06a.pdf.

[16] *See* Joseph Cox, *Meet the Guy Selling Wireless Tech to Steal Luxury Cars in Seconds*, VICE NEWS (Feb. 11, 2020), www.vice.com/en/article/7kz48x/guy-selling-relay-attack-keyless-repeaters-to-steal-cars.

[17] *See* Bettie Cross, *Car Thieves Are Hacking Key Fobs to Quickly and Quietly Steal Vehicles*, CBS AUSTIN (May 12, 2022), cbsaustin.com/news/local/car-thieves-are-hacking-key-fobs-to-quickly-and-quietly-steal-vehicles.

[18] *See* Jatara McGee, *Hackers Are Using New Tech to Steal Locked Cars Without Keys*, WLWT (May 9, 2019), www.wlwt.com/article/hackers-are-using-new-tech-to-steal-locked-cars-without-keys/27424367#.

[19] *See* Nick Bilton, *Keeping Your Car Safe From Electronic Thieves*, N.Y. TIMES (Apr. 15, 2015), www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html.

[20] *See* Sultan Khan, *Technical Advisory – Tesla BLE Phone-as-a-Key Passive Entry Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-tesla-ble-phone-as-a-key-passive-entry-vulnerable-to-relay-attacks/.

[21] BLUETOOTH SIG, PROXIMITY PROFILE 17 (2015), www.bluetooth.com/specifications/specs/proximity-profile-1-0-1/.

[22] *See* Sultan Khan, *Technical Advisory – Kwikset/Weiser BLE Proximity Authentication in Kevo Smart Locks Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-kwikset-weiser-ble-proximity-authentication-in-kevo-smart-locks-vulnerable-to-relay-attacks/.

attacks. Finally, automakers could also adopt Ultra-Wide-Band (UWB) technology, which enables a precise measurement between the vehicle and key fob and, in combination with other technologies, allows the vehicle to determine if the radio signal has been improperly amplified. Experts have suggested that UWB technology could significantly reduce the risk of relay theft.[23]

Given the recent surge in vehicle thefts and the potential security risks involved in keyless entry systems, I respectfully request that you respond in writing to the following questions by August 10, 2022:

1. Please provide the following data, as available, on thefts of vehicles manufactured by your company:

    a. How many vehicles manufactured by your company were stolen in 2019, 2020, 2021, and through the first six months of 2022?

    b. Of those vehicle thefts, how many were caused by thieves taking advantage of key fobs left in vehicles?

    c. Of those vehicle thefts, how many were caused by relay attacks?

2. Please describe the type of transponder and the technology standard that vehicles manufactured by your company use to communicate with key fobs and other devices. If vehicles manufactured by your company use different types of transponders and technology standards, please provide information on all types.

3. Please describe the testing that your company has done to assess the security of its keyless entry systems.

4. What specific steps has your company taken to reduce the vulnerability of its keyless entry system?

    a. Has your company considered making the keyless entry system motion activated?

    b. Has your company considered adopting Ultra-Wide-Band technology?

    c. Has your company considered creating mechanisms to alert owners if their key fob is left inside the vehicle?

5. Does your company plan to take any further steps to reduce any vulnerability of its keyless entry system?

Thank you for your prompt attention to these questions.

---

[23] *See e.g.,* Mridula Singh et al., *UWB with Pulse Reordering: Securing Ranging against Relay and Physical-Layer Attacks*, NETWORK AND DISTRIB. SYS, SEC. SYMP. (2019), www.ndss-symposium.org/ndss-paper/uwb-with-pulse-reordering-securing-ranging-against-relay-and-physical-layer-attacks/.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

July 20, 2022

Thomas J. Doll
President and Chief Executive Officer
Subaru of America, Inc.
One Subaru Drive
Camden, NJ 08103

Dear Mr. Doll,

I write to request information about the security of Subaru's motor vehicle keyless entry systems. Keyless entry systems — which allow users to enter a vehicle and start its engine without inserting and turning a key — likely helped reduce vehicle thefts since the 1990s, but the dramatic 30-year decline has suddenly gone into reverse. Although the exact cause of this turnaround is unclear, a growing body of evidence suggests that keyless entry systems may play a role. We therefore urge Subaru to take all necessary steps to ensure that keyless entry systems, once a security innovation that deterred thieves, do not become a security liability for them to exploit.

After their adoption in the 1990s, keyless entry systems contributed to the impressive decline in car thefts from 1990 to 2019. These systems come in different forms. Some simply allow the driver to enter a vehicle without inserting a physical key into the door lock, while others, called passive entry systems, allow the driver to start the vehicle without inserting a physical key into the ignition. In both cases, the vehicle and a key fob communicate through radio signals, and an "engine immobilizer" prevents the vehicle from starting unless the key fob is nearby.

These systems were a critical advancement in vehicle security. Old-fashioned "hotwiring" a vehicle — that is, bypassing the ignition and starting a vehicle without a key — became far more difficult; with keyless entry systems, cars would not start unless they detected, through the radio signals, the presence of the key fob. In 1995, the European Union required manufacturers to include engine immobilizers on all new vehicles within three years, and Australia and Canada passed similar laws soon thereafter. One study estimated that the EU mandate reduced vehicle thefts in the Netherlands from 1995 to 2008 by 40 percent.[1] The United States never imposed a similar requirement, but many manufacturers have voluntarily adopted keyless entry systems, and car thefts per capita decreased by two-thirds from 1990 to 2019.[2]

---

[1] Jan C. van Ours and Ben Vollaard, *The Engine Immobiliser: A Non-Starter for Car Thieves*, 126 ECON. J. 1264, 1266 (2016), https://onlinelibrary.wiley.com/doi/abs/10.1111/ecoj.12196.

[2] Crime Data Explorer, FED. BUREAU OF INVESTIGATIONS, https://crime-data-explorer.app.cloud.gov/pages/explorer/crime/crime-trend (select "1990" in "From" and "2019" in "To" and "Motor vehicle theft" in "Crime Select").

Although this decrease tracked the overall decline in violent and property crime,[3] news reports have nevertheless attributed part of the decline to the adoption of keyless ignitions.[4]

This remarkably consistent trend towards fewer vehicle thefts, however, has made a concerning U-turn since the end of 2019. According to data compiled by the Federal Bureau of Investigation (FBI), U.S. car thefts per capita increased nationally by 11.8 percent in 2020.[5] Although national data has not yet been released for 2021, news reports suggest that car thefts continued to accelerate across the country last year. For example, in 2021, the number of car thefts appears to have increased by 132 percent in Milwaukee,[6] 70 percent in Washington, DC,[7] and 60 percent in Philadelphia.[8] This trend appears to have continued into 2022. So far this year, as compared with the same period in 2021, the number of car thefts has increased 74 percent in Portland, Ore.,[9] 54 percent in Richmond, Va.,[10] and 51 percent in New York City.[11] After so many years of progress, this rapid reversal in car thefts is alarming.

The same keyless entry systems that contributed to the decline in car thefts may now be providing an opportunity for thieves. Keyless entry systems are vulnerable in two ways. First, drivers may leave their key fobs in their cars, allowing a thief to easily start and steal a vehicle.[12] Whereas drivers used to have to remove the physical key from the ignition when they exited the vehicle, no similar action is necessary when a driver need only push a button to start or stop an engine. According to the New York Police Department, roughly 40 percent of car thefts in New York City so far this year were the result of motorists leaving their vehicles running or unlocked, often with keys or a key fob inside.[13] Keyless technology has thus escalated the consequences of ordinary human error.

---

[3] *Id.* (select "All Property Crimes" or "All Violent Crimes" in "Crime Select").

[4] *See, e.g.,* Sarah Maslin Nir, *Here's Why Car Thefts Are Soaring (Hint: Check Your Cup Holder)*, N.Y. TIMES (Jan. 6, 2021), www.nytimes.com/2021/01/06/nyregion/car-thefts-nyc.html; Brad Stone, *Pinch My Ride*, Wired (Aug. 1, 2006), www.wired.com/2006/08/carkey/.

[5] Crime Data Explorer, *supra* note 3 (select "2019" in "From" and "2020" in "To" and "Motor vehicle theft" in "Crime Select").

[6] *See* Teddy Nykiel, *Over 500% Spike in Auto Thefts Troubles Downtown*, MILWAUKEE BUS. J. (Feb. 9, 2022), https://www.bizjournals.com/milwaukee/news/2022/02/09/crime-statistics-mpd-2021-car-lefts.html.

[7] *See* Bruce Leshan, *Surge in Carjackings, Car Thefts Has Police Struggling to Respond*, WUSA (Feb. 9, 2021), www.wusa9.com/article/news/crime/surge-in-carjackings-car-thefts-dc-police-form-task-force/65-8c4b0c03-e343-430e-9c77-c5d9daade558.

[8] *See* Chad Pradelli and Cheryl Mettendorf, *Action News Investigation into Rise of Dealership Auto Thefts in Philadelphia Region*, ABC ACTION NEWS (Jan. 14, 2022), 6abc.com/car-thefts-auto-dealerships-6abc-investigation-barbera-autoland/11464047/.

[9] *See* Stolen Vehicle Statistics, CITY OF PORTLAND, https://www.portlandoregon.gov/police/74369 (compare selecting Jan. – May 2022 with Jan. – May 2021 in "Filter by Reported Date of Theft").

[10] *See* Henry Graff, *Richmond Police See 54% Increase in Vehicle Thefts Over Last Year*, NBC12 (Apr. 7, 2022), www.nbc12.com/2022/04/07/richmond-police-see-54-increase-vehicle-thefts-over-last-year/.

[11] *See* Rocco Parascandola, *NYPD Reports 51% Surge in Stolen Cars This Year*, N.Y. DAILY NEWS (June 12, 2022), www.nydailynews.com/new-york/nyc-crime/ny-car-vehicle-theft-surge-careless-motorists-nypd-20220612-eojbb2hhx5a3tn34vzhilc2fdq-story.html.

[12] *See* Nathan Bomey, *Thieves strike: Auto Theft Spikes During the Pandemic as Cars Are Left Unattended*, USA TODAY (Aug. 31, 2021), usatoday.com/story/money/cars/2021/08/31/auto-theft-spikes-stolen-car-vehicle-theft-pandemic-nicb/5652615001/.

[13] Rocco Parascandola, *supra* note 11.

Second, and perhaps more worryingly, a common type of keyless entry system that allows a driver to unlock and start the vehicle without needing to touch the key — known as a passive entry system — appear to be vulnerable to a "relay attack," in which a thief uses a signal amplifier to fool the car into believing that the owner is nearby.[14] Researchers have long known that bad actors could amplify radio signals emitted from the vehicle and key, allowing them to enter and start a vehicle even if the fob is nowhere nearby.[15] In recent years, devices that enable relay attacks have become widely available,[16] and news reports have identified thefts involving relay attacks in Austin,[17] Cincinnati,[18] and Los Angeles.[19]

More recently, researchers have shown that carmakers that use Bluetooth Low Energy (BLE) entry systems — which uses Bluetooth technology to determine whether the vehicle is within a certain distance of the connected device — are also vulnerable to theft using similar relay technology, affecting manufacturers such as Tesla that have adopted BLE passive entry systems.[20] For that reason, the Bluetooth Special Interest Group, the standard-setting organization that oversees the development of Bluetooth technologies, warns that BLE "should not be used as the only protection of valuable assets."[21] Car manufacturers have only recently begun using BLE technology to determine the proximity of a key fob, so researchers have not yet confirmed any vehicles stolen through a BLE relay attack. However, as manufacturers increasingly equip devices — such as smart locks for homes[22] — with BLE passive entry systems, this vulnerability could put a broad range of critical security systems at risk.

Fortunately, researchers have also identified methods to mitigate the risk of passive entry thefts. For example, manufacturers can prevent a fob from unlocking a vehicle if the fob was not recently in motion, as typically occurs as a driver approaches a vehicle. In other words, if the fob is idle, the driver is likely not trying to unlock their own vehicle; any attempt to use the fob in that state may be a sign of a relay attack. Similarly, manufacturers could require consumers to complete an additional verification, such as inputting a PIN number, to enter the vehicle. While such systems inherently inconvenience consumers, they also are a strong defense against relay

---

[14] Rachel Wait, *Keyless Car Crime: How to Thwart the Thieves*, FORBES ADVISOR (Mar. 24, 2022), www.forbes.com/uk/advisor/car-insurance/keyless-car-crime/.

[15] *See* ARI JUELS, RFID SECURITY AND PRIVACY: A RESEARCH SURVEY 13 (2005), www.arijuels.com/wp-content/uploads/2013/09/J06a.pdf.

[16] *See* Joseph Cox, *Meet the Guy Selling Wireless Tech to Steal Luxury Cars in Seconds*, VICE NEWS (Feb. 11, 2020), www.vice.com/en/article/7kz48x/guy-selling-relay-attack-keyless-repeaters-to-steal-cars.

[17] *See* Bettie Cross, *Car Thieves Are Hacking Key Fobs to Quickly and Quietly Steal Vehicles*, CBS AUSTIN (May 12, 2022), cbsaustin.com/news/local/car-thieves-are-hacking-key-fobs-to-quickly-and-quietly-steal-vehicles.

[18] *See* Jatara McGee, *Hackers Are Using New Tech to Steal Locked Cars Without Keys*, WLWT (May 9, 2019), www.wlwt.com/article/hackers-are-using-new-tech-to-steal-locked-cars-without-keys/27424367#.

[19] *See* Nick Bilton, *Keeping Your Car Safe From Electronic Thieves*, N.Y. TIMES (Apr. 15, 2015), www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html.

[20] *See* Sultan Khan, *Technical Advisory – Tesla BLE Phone-as-a-Key Passive Entry Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-tesla-ble-phone-as-a-key-passive-entry-vulnerable-to-relay-attacks/.

[21] BLUETOOTH SIG, PROXIMITY PROFILE 17 (2015), www.bluetooth.com/specifications/specs/proximity-profile-1-0-1/.

[22] *See* Sultan Khan, *Technical Advisory – Kwikset/Weiser BLE Proximity Authentication in Kevo Smart Locks Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-kwikset-weiser-ble-proximity-authentication-in-kevo-smart-locks-vulnerable-to-relay-attacks/.

attacks. Finally, automakers could also adopt Ultra-Wide-Band (UWB) technology, which enables a precise measurement between the vehicle and key fob and, in combination with other technologies, allows the vehicle to determine if the radio signal has been improperly amplified. Experts have suggested that UWB technology could significantly reduce the risk of relay theft.[23]

Given the recent surge in vehicle thefts and the potential security risks involved in keyless entry systems, I respectfully request that you respond in writing to the following questions by August 10, 2022:

1. Please provide the following data, as available, on thefts of vehicles manufactured by your company:

    a. How many vehicles manufactured by your company were stolen in 2019, 2020, 2021, and through the first six months of 2022?

    b. Of those vehicle thefts, how many were caused by thieves taking advantage of key fobs left in vehicles?

    c. Of those vehicle thefts, how many were caused by relay attacks?

2. Please describe the type of transponder and the technology standard that vehicles manufactured by your company use to communicate with key fobs and other devices. If vehicles manufactured by your company use different types of transponders and technology standards, please provide information on all types.

3. Please describe the testing that your company has done to assess the security of its keyless entry systems.

4. What specific steps has your company taken to reduce the vulnerability of its keyless entry system?

    a. Has your company considered making the keyless entry system motion activated?

    b. Has your company considered adopting Ultra-Wide-Band technology?

    c. Has your company considered creating mechanisms to alert owners if their key fob is left inside the vehicle?

5. Does your company plan to take any further steps to reduce any vulnerability of its keyless entry system?

Thank you for your prompt attention to these questions.

---

[23] *See e.g.,* Mridula Singh et al., *UWB with Pulse Reordering: Securing Ranging against Relay and Physical-Layer Attacks*, NETWORK AND DISTRIB. SYS, SEC. SYMP. (2019), www.ndss-symposium.org/ndss-paper/uwb-with-pulse-reordering-securing-ranging-against-relay-and-physical-layer-attacks/.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

July 20, 2022

Elon Musk
Chief Executive Officer
Tesla, Inc.
13101 Harold Green Road
Austin, TX 78725

Dear Mr. Musk,

I write to request information about the security of Tesla's motor vehicle keyless entry systems. Keyless entry systems — which allow users to enter a vehicle and start its engine without inserting and turning a key — likely helped reduce vehicle thefts since the 1990s, but the dramatic 30-year decline has suddenly gone into reverse. Although the exact cause of this turnaround is unclear, a growing body of evidence suggests that keyless entry systems may play a role. We therefore urge Tesla to take all necessary steps to ensure that keyless entry systems, once a security innovation that deterred thieves, do not become a security liability for them to exploit.

After their adoption in the 1990s, keyless entry systems contributed to the impressive decline in car thefts from 1990 to 2019. These systems come in different forms. Some simply allow the driver to enter a vehicle without inserting a physical key into the door lock, while others, called passive entry systems, allow the driver to start the vehicle without inserting a physical key into the ignition. In both cases, the vehicle and a key fob communicate through radio signals, and an "engine immobilizer" prevents the vehicle from starting unless the key fob is nearby.

These systems were a critical advancement in vehicle security. Old-fashioned "hotwiring" a vehicle — that is, bypassing the ignition and starting a vehicle without a key — became far more difficult; with keyless entry systems, cars would not start unless they detected, through the radio signals, the presence of the key fob. In 1995, the European Union required manufacturers to include engine immobilizers on all new vehicles within three years, and Australia and Canada passed similar laws soon thereafter. One study estimated that the EU mandate reduced vehicle thefts in the Netherlands from 1995 to 2008 by 40 percent.[1] The United States never imposed a similar requirement, but many manufacturers have voluntarily adopted keyless entry systems, and car thefts per capita decreased by two-thirds from 1990 to 2019.[2]

---

[1] Jan C. van Ours and Ben Vollaard, *The Engine Immobiliser: A Non-Starter for Car Thieves*, 126 ECON. J. 1264, 1266 (2016), https://onlinelibrary.wiley.com/doi/abs/10.1111/ecoj.12196.

[2] Crime Data Explorer, FED. BUREAU OF INVESTIGATIONS, https://crime-data-explorer.app.cloud.gov/pages/explorer/crime/crime-trend (select "1990" in "From" and "2019" in "To" and "Motor vehicle theft" in "Crime Select").

Although this decrease tracked the overall decline in violent and property crime,[3] news reports have nevertheless attributed part of the decline to the adoption of keyless ignitions.[4]

This remarkably consistent trend towards fewer vehicle thefts, however, has made a concerning U-turn since the end of 2019. According to data compiled by the Federal Bureau of Investigation (FBI), U.S. car thefts per capita increased nationally by 11.8 percent in 2020.[5] Although national data has not yet been released for 2021, news reports suggest that car thefts continued to accelerate across the country last year. For example, in 2021, the number of car thefts appears to have increased by 132 percent in Milwaukee,[6] 70 percent in Washington, DC,[7] and 60 percent in Philadelphia.[8] This trend appears to have continued into 2022. So far this year, as compared with the same period in 2021, the number of car thefts has increased 74 percent in Portland, Ore.,[9] 54 percent in Richmond, Va.,[10] and 51 percent in New York City.[11] After so many years of progress, this rapid reversal in car thefts is alarming.

The same keyless entry systems that contributed to the decline in car thefts may now be providing an opportunity for thieves. Keyless entry systems are vulnerable in two ways. First, drivers may leave their key fobs in their cars, allowing a thief to easily start and steal a vehicle.[12] Whereas drivers used to have to remove the physical key from the ignition when they exited the vehicle, no similar action is necessary when a driver need only push a button to start or stop an engine. According to the New York Police Department, roughly 40 percent of car thefts in New York City so far this year were the result of motorists leaving their vehicles running or unlocked, often with keys or a key fob inside.[13] Keyless technology has thus escalated the consequences of ordinary human error.

---

[3] *Id.* (select "All Property Crimes" or "All Violent Crimes" in "Crime Select").

[4] *See, e.g.,* Sarah Maslin Nir, *Here's Why Car Thefts Are Soaring (Hint: Check Your Cup Holder)*, N.Y. TIMES (Jan. 6, 2021), www.nytimes.com/2021/01/06/nyregion/car-thefts-nyc.html; Brad Stone, *Pinch My Ride*, Wired (Aug. 1, 2006), www.wired.com/2006/08/carkey/.

[5] Crime Data Explorer, *supra* note 3 (select "2019" in "From" and "2020" in "To" and "Motor vehicle theft" in "Crime Select").

[6] *See* Teddy Nykiel, *Over 500% Spike in Auto Thefts Troubles Downtown*, MILWAUKEE BUS. J. (Feb. 9, 2022), https://www.bizjournals.com/milwaukee/news/2022/02/09/crime-statistics-mpd-2021-car-lefts.html.

[7] *See* Bruce Leshan, *Surge in Carjackings, Car Thefts Has Police Struggling to Respond*, WUSA (Feb. 9, 2021), www.wusa9.com/article/news/crime/surge-in-carjackings-car-thefts-dc-police-form-task-force/65-8c4b0c03-e343-430e-9c77-c5d9daade558.

[8] *See* Chad Pradelli and Cheryl Mettendorf, *Action News Investigation into Rise of Dealership Auto Thefts in Philadelphia Region*, ABC ACTION NEWS (Jan. 14, 2022), 6abc.com/car-thefts-auto-dealerships-6abc-investigation-barbera-autoland/11464047/.

[9] *See* Stolen Vehicle Statistics, CITY OF PORTLAND, https://www.portlandoregon.gov/police/74369 (compare selecting Jan. – May 2022 with Jan. – May 2021 in "Filter by Reported Date of Theft").

[10] *See* Henry Graff, *Richmond Police See 54% Increase in Vehicle Thefts Over Last Year*, NBC12 (Apr. 7, 2022), www.nbc12.com/2022/04/07/richmond-police-see-54-increase-vehicle-thefts-over-last-year/.

[11] *See* Rocco Parascandola, *NYPD Reports 51% Surge in Stolen Cars This Year*, N.Y. DAILY NEWS (June 12, 2022), www.nydailynews.com/new-york/nyc-crime/ny-car-vehicle-theft-surge-careless-motorists-nypd-20220612-eojbb2hhx5a3tn34vzhilc2fdq-story.html.

[12] *See* Nathan Bomey, *Thieves strike: Auto Theft Spikes During the Pandemic as Cars Are Left Unattended*, USA TODAY (Aug. 31, 2021), usatoday.com/story/money/cars/2021/08/31/auto-theft-spikes-stolen-car-vehicle-theft-pandemic-nicb/5652615001/.

[13] Rocco Parascandola, *supra* note 11.

Second, and perhaps more worryingly, a common type of keyless entry system that allows a driver to unlock and start the vehicle without needing to touch the key — known as a passive entry system — appear to be vulnerable to a "relay attack," in which a thief uses a signal amplifier to fool the car into believing that the owner is nearby.[14] Researchers have long known that bad actors could amplify radio signals emitted from the vehicle and key, allowing them to enter and start a vehicle even if the fob is nowhere nearby.[15] In recent years, devices that enable relay attacks have become widely available,[16] and news reports have identified thefts involving relay attacks in Austin,[17] Cincinnati,[18] and Los Angeles.[19]

More recently, researchers have shown that carmakers that use Bluetooth Low Energy (BLE) entry systems — which uses Bluetooth technology to determine whether the vehicle is within a certain distance of the connected device — are also vulnerable to theft using similar relay technology, affecting manufacturers such as Tesla that have adopted BLE passive entry systems.[20] For that reason, the Bluetooth Special Interest Group, the standard-setting organization that oversees the development of Bluetooth technologies, warns that BLE "should not be used as the only protection of valuable assets."[21] Car manufacturers have only recently begun using BLE technology to determine the proximity of a key fob, so researchers have not yet confirmed any vehicles stolen through a BLE relay attack. However, as manufacturers increasingly equip devices — such as smart locks for homes[22] — with BLE passive entry systems, this vulnerability could put a broad range of critical security systems at risk.

Fortunately, researchers have also identified methods to mitigate the risk of passive entry thefts. For example, manufacturers can prevent a fob from unlocking a vehicle if the fob was not recently in motion, as typically occurs as a driver approaches a vehicle. In other words, if the fob is idle, the driver is likely not trying to unlock their own vehicle; any attempt to use the fob in that state may be a sign of a relay attack. Similarly, manufacturers could require consumers to complete an additional verification, such as inputting a PIN number, to enter the vehicle. While such systems inherently inconvenience consumers, they also are a strong defense against relay

---

[14] Rachel Wait, *Keyless Car Crime: How to Thwart the Thieves*, FORBES ADVISOR (Mar. 24, 2022), www.forbes.com/uk/advisor/car-insurance/keyless-car-crime/.

[15] *See* ARI JUELS, RFID SECURITY AND PRIVACY: A RESEARCH SURVEY 13 (2005), www.arijuels.com/wp-content/uploads/2013/09/J06a.pdf.

[16] *See* Joseph Cox, *Meet the Guy Selling Wireless Tech to Steal Luxury Cars in Seconds*, VICE NEWS (Feb. 11, 2020), www.vice.com/en/article/7kz48x/guy-selling-relay-attack-keyless-repeaters-to-steal-cars.

[17] *See* Bettie Cross, *Car Thieves Are Hacking Key Fobs to Quickly and Quietly Steal Vehicles*, CBS AUSTIN (May 12, 2022), cbsaustin.com/news/local/car-thieves-are-hacking-key-fobs-to-quickly-and-quietly-steal-vehicles.

[18] *See* Jatara McGee, *Hackers Are Using New Tech to Steal Locked Cars Without Keys*, WLWT (May 9, 2019), www.wlwt.com/article/hackers-are-using-new-tech-to-steal-locked-cars-without-keys/27424367#.

[19] *See* Nick Bilton, *Keeping Your Car Safe From Electronic Thieves*, N.Y. TIMES (Apr. 15, 2015), www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html.

[20] *See* Sultan Khan, *Technical Advisory – Tesla BLE Phone-as-a-Key Passive Entry Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-tesla-ble-phone-as-a-key-passive-entry-vulnerable-to-relay-attacks/.

[21] BLUETOOTH SIG, PROXIMITY PROFILE 17 (2015), www.bluetooth.com/specifications/specs/proximity-profile-1-0-1/.

[22] *See* Sultan Khan, *Technical Advisory – Kwikset/Weiser BLE Proximity Authentication in Kevo Smart Locks Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-kwikset-weiser-ble-proximity-authentication-in-kevo-smart-locks-vulnerable-to-relay-attacks/.

attacks. Finally, automakers could also adopt Ultra-Wide-Band (UWB) technology, which enables a precise measurement between the vehicle and key fob and, in combination with other technologies, allows the vehicle to determine if the radio signal has been improperly amplified. Experts have suggested that UWB technology could significantly reduce the risk of relay theft.[23]

Given the recent surge in vehicle thefts and the potential security risks involved in keyless entry systems, I respectfully request that you respond in writing to the following questions by August 10, 2022:

1. Please provide the following data, as available, on thefts of vehicles manufactured by your company:

    a. How many vehicles manufactured by your company were stolen in 2019, 2020, 2021, and through the first six months of 2022?

    b. Of those vehicle thefts, how many were caused by thieves taking advantage of key fobs left in vehicles?

    c. Of those vehicle thefts, how many were caused by relay attacks?

2. Please describe the type of transponder and the technology standard that vehicles manufactured by your company use to communicate with key fobs and other devices. If vehicles manufactured by your company use different types of transponders and technology standards, please provide information on all types.

3. Please describe the testing that your company has done to assess the security of its keyless entry systems.

4. What specific steps has your company taken to reduce the vulnerability of its keyless entry system?

    a. Has your company considered making the keyless entry system motion activated?

    b. Has your company considered adopting Ultra-Wide-Band technology?

    c. Has your company considered creating mechanisms to alert owners if their key fob is left inside the vehicle?

5. Does your company plan to take any further steps to reduce any vulnerability of its keyless entry system?

Thank you for your prompt attention to these questions.

---

[23] *See e.g.,* Mridula Singh et al., *UWB with Pulse Reordering: Securing Ranging against Relay and Physical-Layer Attacks*, NETWORK AND DISTRIB. SYS, SEC. SYMP. (2019), www.ndss-symposium.org/ndss-paper/uwb-with-pulse-reordering-securing-ranging-against-relay-and-physical-layer-attacks/.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

July 20, 2022

Tetsuo "Ted" Ogawa
President and Chief Executive Officer
Toyota Motor North America, Inc.
6565 Headquarters Drive
Plano, TX 75024

Dear Mr. Ogawa,

I write to request information about the security of Toyota's motor vehicle keyless entry systems. Keyless entry systems — which allow users to enter a vehicle and start its engine without inserting and turning a key — likely helped reduce vehicle thefts since the 1990s, but the dramatic 30-year decline has suddenly gone into reverse. Although the exact cause of this turnaround is unclear, a growing body of evidence suggests that keyless entry systems may play a role. We therefore urge Toyota to take all necessary steps to ensure that keyless entry systems, once a security innovation that deterred thieves, do not become a security liability for them to exploit.

After their adoption in the 1990s, keyless entry systems contributed to the impressive decline in car thefts from 1990 to 2019. These systems come in different forms. Some simply allow the driver to enter a vehicle without inserting a physical key into the door lock, while others, called passive entry systems, allow the driver to start the vehicle without inserting a physical key into the ignition. In both cases, the vehicle and a key fob communicate through radio signals, and an "engine immobilizer" prevents the vehicle from starting unless the key fob is nearby.

These systems were a critical advancement in vehicle security. Old-fashioned "hotwiring" a vehicle — that is, bypassing the ignition and starting a vehicle without a key — became far more difficult; with keyless entry systems, cars would not start unless they detected, through the radio signals, the presence of the key fob. In 1995, the European Union required manufacturers to include engine immobilizers on all new vehicles within three years, and Australia and Canada passed similar laws soon thereafter. One study estimated that the EU mandate reduced vehicle thefts in the Netherlands from 1995 to 2008 by 40 percent.[1] The United States never imposed a similar requirement, but many manufacturers have voluntarily adopted keyless entry systems, and car thefts per capita decreased by two-thirds from 1990 to 2019.[2]

---

[1] Jan C. van Ours and Ben Vollaard, *The Engine Immobiliser: A Non-Starter for Car Thieves*, 126 ECON. J. 1264, 1266 (2016), https://onlinelibrary.wiley.com/doi/abs/10.1111/ecoj.12196.

[2] Crime Data Explorer, FED. BUREAU OF INVESTIGATIONS, https://crime-data-explorer.app.cloud.gov/pages/explorer/crime/crime-trend (select "1990" in "From" and "2019" in "To" and "Motor vehicle theft" in "Crime Select").

Although this decrease tracked the overall decline in violent and property crime,[3] news reports have nevertheless attributed part of the decline to the adoption of keyless ignitions.[4]

This remarkably consistent trend towards fewer vehicle thefts, however, has made a concerning U-turn since the end of 2019. According to data compiled by the Federal Bureau of Investigation (FBI), U.S. car thefts per capita increased nationally by 11.8 percent in 2020.[5] Although national data has not yet been released for 2021, news reports suggest that car thefts continued to accelerate across the country last year. For example, in 2021, the number of car thefts appears to have increased by 132 percent in Milwaukee,[6] 70 percent in Washington, DC,[7] and 60 percent in Philadelphia.[8] This trend appears to have continued into 2022. So far this year, as compared with the same period in 2021, the number of car thefts has increased 74 percent in Portland, Ore.,[9] 54 percent in Richmond, Va.,[10] and 51 percent in New York City.[11] After so many years of progress, this rapid reversal in car thefts is alarming.

The same keyless entry systems that contributed to the decline in car thefts may now be providing an opportunity for thieves. Keyless entry systems are vulnerable in two ways. First, drivers may leave their key fobs in their cars, allowing a thief to easily start and steal a vehicle.[12] Whereas drivers used to have to remove the physical key from the ignition when they exited the vehicle, no similar action is necessary when a driver need only push a button to start or stop an engine. According to the New York Police Department, roughly 40 percent of car thefts in New York City so far this year were the result of motorists leaving their vehicles running or unlocked, often with keys or a key fob inside.[13] Keyless technology has thus escalated the consequences of ordinary human error.

---

[3] *Id.* (select "All Property Crimes" or "All Violent Crimes" in "Crime Select").

[4] *See, e.g.,* Sarah Maslin Nir, *Here's Why Car Thefts Are Soaring (Hint: Check Your Cup Holder)*, N.Y. TIMES (Jan. 6, 2021), www.nytimes.com/2021/01/06/nyregion/car-thefts-nyc.html; Brad Stone, *Pinch My Ride*, Wired (Aug. 1, 2006), www.wired.com/2006/08/carkey/.

[5] Crime Data Explorer, *supra* note 3 (select "2019" in "From" and "2020" in "To" and "Motor vehicle theft" in "Crime Select").

[6] *See* Teddy Nykiel, *Over 500% Spike in Auto Thefts Troubles Downtown*, MILWAUKEE BUS. J. (Feb. 9, 2022), https://www.bizjournals.com/milwaukee/news/2022/02/09/crime-statistics-mpd-2021-car-lefts.html.

[7] *See* Bruce Leshan, *Surge in Carjackings, Car Thefts Has Police Struggling to Respond*, WUSA (Feb. 9, 2021), www.wusa9.com/article/news/crime/surge-in-carjackings-car-thefts-dc-police-form-task-force/65-8c4b0c03-e343-430e-9c77-c5d9daade558.

[8] *See* Chad Pradelli and Cheryl Mettendorf, *Action News Investigation into Rise of Dealership Auto Thefts in Philadelphia Region*, ABC ACTION NEWS (Jan. 14, 2022), 6abc.com/car-thefts-auto-dealerships-6abc-investigation-barbera-autoland/11464047/.

[9] *See* Stolen Vehicle Statistics, CITY OF PORTLAND, https://www.portlandoregon.gov/police/74369 (compare selecting Jan. – May 2022 with Jan. – May 2021 in "Filter by Reported Date of Theft").

[10] *See* Henry Graff, *Richmond Police See 54% Increase in Vehicle Thefts Over Last Year*, NBC12 (Apr. 7, 2022), www.nbc12.com/2022/04/07/richmond-police-see-54-increase-vehicle-thefts-over-last-year/.

[11] *See* Rocco Parascandola, *NYPD Reports 51% Surge in Stolen Cars This Year*, N.Y. DAILY NEWS (June 12, 2022), www.nydailynews.com/new-york/nyc-crime/ny-car-vehicle-theft-surge-careless-motorists-nypd-20220612-eojbb2hhx5a3tn34vzhilc2fdq-story.html.

[12] *See* Nathan Bomey, *Thieves strike: Auto Theft Spikes During the Pandemic as Cars Are Left Unattended*, USA TODAY (Aug. 31, 2021), usatoday.com/story/money/cars/2021/08/31/auto-theft-spikes-stolen-car-vehicle-theft-pandemic-nicb/5652615001/.

[13] Rocco Parascandola, *supra* note 11.

Second, and perhaps more worryingly, a common type of keyless entry system that allows a driver to unlock and start the vehicle without needing to touch the key — known as a passive entry system — appear to be vulnerable to a "relay attack," in which a thief uses a signal amplifier to fool the car into believing that the owner is nearby.[14] Researchers have long known that bad actors could amplify radio signals emitted from the vehicle and key, allowing them to enter and start a vehicle even if the fob is nowhere nearby.[15] In recent years, devices that enable relay attacks have become widely available,[16] and news reports have identified thefts involving relay attacks in Austin,[17] Cincinnati,[18] and Los Angeles.[19]

More recently, researchers have shown that carmakers that use Bluetooth Low Energy (BLE) entry systems — which uses Bluetooth technology to determine whether the vehicle is within a certain distance of the connected device — are also vulnerable to theft using similar relay technology, affecting manufacturers such as Tesla that have adopted BLE passive entry systems.[20] For that reason, the Bluetooth Special Interest Group, the standard-setting organization that oversees the development of Bluetooth technologies, warns that BLE "should not be used as the only protection of valuable assets."[21] Car manufacturers have only recently begun using BLE technology to determine the proximity of a key fob, so researchers have not yet confirmed any vehicles stolen through a BLE relay attack. However, as manufacturers increasingly equip devices — such as smart locks for homes[22] — with BLE passive entry systems, this vulnerability could put a broad range of critical security systems at risk.

Fortunately, researchers have also identified methods to mitigate the risk of passive entry thefts. For example, manufacturers can prevent a fob from unlocking a vehicle if the fob was not recently in motion, as typically occurs as a driver approaches a vehicle. In other words, if the fob is idle, the driver is likely not trying to unlock their own vehicle; any attempt to use the fob in that state may be a sign of a relay attack. Similarly, manufacturers could require consumers to complete an additional verification, such as inputting a PIN number, to enter the vehicle. While such systems inherently inconvenience consumers, they also are a strong defense against relay

---

[14] Rachel Wait, *Keyless Car Crime: How to Thwart the Thieves*, FORBES ADVISOR (Mar. 24, 2022), www.forbes.com/uk/advisor/car-insurance/keyless-car-crime/.

[15] *See* ARI JUELS, RFID SECURITY AND PRIVACY: A RESEARCH SURVEY 13 (2005), www.arijuels.com/wp-content/uploads/2013/09/J06a.pdf.

[16] *See* Joseph Cox, *Meet the Guy Selling Wireless Tech to Steal Luxury Cars in Seconds*, VICE NEWS (Feb. 11, 2020), www.vice.com/en/article/7kz48x/guy-selling-relay-attack-keyless-repeaters-to-steal-cars.

[17] *See* Bettie Cross, *Car Thieves Are Hacking Key Fobs to Quickly and Quietly Steal Vehicles*, CBS AUSTIN (May 12, 2022), cbsaustin.com/news/local/car-thieves-are-hacking-key-fobs-to-quickly-and-quietly-steal-vehicles.

[18] *See* Jatara McGee, *Hackers Are Using New Tech to Steal Locked Cars Without Keys*, WLWT (May 9, 2019), www.wlwt.com/article/hackers-are-using-new-tech-to-steal-locked-cars-without-keys/27424367#.

[19] *See* Nick Bilton, *Keeping Your Car Safe From Electronic Thieves*, N.Y. TIMES (Apr. 15, 2015), www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html.

[20] *See* Sultan Khan, *Technical Advisory – Tesla BLE Phone-as-a-Key Passive Entry Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-tesla-ble-phone-as-a-key-passive-entry-vulnerable-to-relay-attacks/.

[21] BLUETOOTH SIG, PROXIMITY PROFILE 17 (2015), www.bluetooth.com/specifications/specs/proximity-profile-1-0-1/.

[22] *See* Sultan Khan, *Technical Advisory – Kwikset/Weiser BLE Proximity Authentication in Kevo Smart Locks Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-kwikset-weiser-ble-proximity-authentication-in-kevo-smart-locks-vulnerable-to-relay-attacks/.

attacks. Finally, automakers could also adopt Ultra-Wide-Band (UWB) technology, which enables a precise measurement between the vehicle and key fob and, in combination with other technologies, allows the vehicle to determine if the radio signal has been improperly amplified. Experts have suggested that UWB technology could significantly reduce the risk of relay theft.[23]

Given the recent surge in vehicle thefts and the potential security risks involved in keyless entry systems, I respectfully request that you respond in writing to the following questions by August 10, 2022:

1. Please provide the following data, as available, on thefts of vehicles manufactured by your company:

    a. How many vehicles manufactured by your company were stolen in 2019, 2020, 2021, and through the first six months of 2022?

    b. Of those vehicle thefts, how many were caused by thieves taking advantage of key fobs left in vehicles?

    c. Of those vehicle thefts, how many were caused by relay attacks?

2. Please describe the type of transponder and the technology standard that vehicles manufactured by your company use to communicate with key fobs and other devices. If vehicles manufactured by your company use different types of transponders and technology standards, please provide information on all types.

3. Please describe the testing that your company has done to assess the security of its keyless entry systems.

4. What specific steps has your company taken to reduce the vulnerability of its keyless entry system?

    a. Has your company considered making the keyless entry system motion activated?

    b. Has your company considered adopting Ultra-Wide-Band technology?

    c. Has your company considered creating mechanisms to alert owners if their key fob is left inside the vehicle?

5. Does your company plan to take any further steps to reduce any vulnerability of its keyless entry system?

Thank you for your prompt attention to these questions.

---

[23] *See e.g.,* Mridula Singh et al., *UWB with Pulse Reordering: Securing Ranging against Relay and Physical-Layer Attacks*, NETWORK AND DISTRIB. SYS, SEC. SYMP. (2019), www.ndss-symposium.org/ndss-paper/uwb-with-pulse-reordering-securing-ranging-against-relay-and-physical-layer-attacks/.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

July 20, 2022

Scott Keogh
President and Chief Executive Officer
Volkswagen Group of America, Inc.
2200 Woodland Pointe Avenue
Herndon, VA 20171

Dear Mr. Keogh,

I write to request information about the security of Volkswagen's motor vehicle keyless entry systems. Keyless entry systems — which allow users to enter a vehicle and start its engine without inserting and turning a key — likely helped reduce vehicle thefts since the 1990s, but the dramatic 30-year decline has suddenly gone into reverse. Although the exact cause of this turnaround is unclear, a growing body of evidence suggests that keyless entry systems may play a role. We therefore urge Volkswagen to take all necessary steps to ensure that keyless entry systems, once a security innovation that deterred thieves, do not become a security liability for them to exploit.

After their adoption in the 1990s, keyless entry systems contributed to the impressive decline in car thefts from 1990 to 2019. These systems come in different forms. Some simply allow the driver to enter a vehicle without inserting a physical key into the door lock, while others, called passive entry systems, allow the driver to start the vehicle without inserting a physical key into the ignition. In both cases, the vehicle and a key fob communicate through radio signals, and an "engine immobilizer" prevents the vehicle from starting unless the key fob is nearby.

These systems were a critical advancement in vehicle security. Old-fashioned "hotwiring" a vehicle — that is, bypassing the ignition and starting a vehicle without a key — became far more difficult; with keyless entry systems, cars would not start unless they detected, through the radio signals, the presence of the key fob. In 1995, the European Union required manufacturers to include engine immobilizers on all new vehicles within three years, and Australia and Canada passed similar laws soon thereafter. One study estimated that the EU mandate reduced vehicle thefts in the Netherlands from 1995 to 2008 by 40 percent.[1] The United States never imposed a similar requirement, but many manufacturers have voluntarily adopted keyless entry systems, and car thefts per capita decreased by two-thirds from 1990 to 2019.[2]

---

[1] Jan C. van Ours and Ben Vollaard, *The Engine Immobiliser: A Non-Starter for Car Thieves*, 126 ECON. J. 1264, 1266 (2016), https://onlinelibrary.wiley.com/doi/abs/10.1111/ecoj.12196.

[2] Crime Data Explorer, FED. BUREAU OF INVESTIGATIONS, https://crime-data-explorer.app.cloud.gov/pages/explorer/crime/crime-trend (select "1990" in "From" and "2019" in "To" and "Motor vehicle theft" in "Crime Select").

Although this decrease tracked the overall decline in violent and property crime,[3] news reports have nevertheless attributed part of the decline to the adoption of keyless ignitions.[4]

This remarkably consistent trend towards fewer vehicle thefts, however, has made a concerning U-turn since the end of 2019. According to data compiled by the Federal Bureau of Investigation (FBI), U.S. car thefts per capita increased nationally by 11.8 percent in 2020.[5] Although national data has not yet been released for 2021, news reports suggest that car thefts continued to accelerate across the country last year. For example, in 2021, the number of car thefts appears to have increased by 132 percent in Milwaukee,[6] 70 percent in Washington, DC,[7] and 60 percent in Philadelphia.[8] This trend appears to have continued into 2022. So far this year, as compared with the same period in 2021, the number of car thefts has increased 74 percent in Portland, Ore.,[9] 54 percent in Richmond, Va.,[10] and 51 percent in New York City.[11] After so many years of progress, this rapid reversal in car thefts is alarming.

The same keyless entry systems that contributed to the decline in car thefts may now be providing an opportunity for thieves. Keyless entry systems are vulnerable in two ways. First, drivers may leave their key fobs in their cars, allowing a thief to easily start and steal a vehicle.[12] Whereas drivers used to have to remove the physical key from the ignition when they exited the vehicle, no similar action is necessary when a driver need only push a button to start or stop an engine. According to the New York Police Department, roughly 40 percent of car thefts in New York City so far this year were the result of motorists leaving their vehicles running or unlocked, often with keys or a key fob inside.[13] Keyless technology has thus escalated the consequences of ordinary human error.

---

[3] *Id.* (select "All Property Crimes" or "All Violent Crimes" in "Crime Select").

[4] *See, e.g.,* Sarah Maslin Nir, *Here's Why Car Thefts Are Soaring (Hint: Check Your Cup Holder)*, N.Y. TIMES (Jan. 6, 2021), www.nytimes.com/2021/01/06/nyregion/car-thefts-nyc.html; Brad Stone, *Pinch My Ride*, Wired (Aug. 1, 2006), www.wired.com/2006/08/carkey/.

[5] Crime Data Explorer, *supra* note 3 (select "2019" in "From" and "2020" in "To" and "Motor vehicle theft" in "Crime Select").

[6] *See* Teddy Nykiel, *Over 500% Spike in Auto Thefts Troubles Downtown*, MILWAUKEE BUS. J. (Feb. 9, 2022), https://www.bizjournals.com/milwaukee/news/2022/02/09/crime-statistics-mpd-2021-car-lefts.html.

[7] *See* Bruce Leshan, *Surge in Carjackings, Car Thefts Has Police Struggling to Respond*, WUSA (Feb. 9, 2021), www.wusa9.com/article/news/crime/surge-in-carjackings-car-thefts-dc-police-form-task-force/65-8c4b0c03-e343-430e-9c77-c5d9daade558.

[8] *See* Chad Pradelli and Cheryl Mettendorf, *Action News Investigation into Rise of Dealership Auto Thefts in Philadelphia Region*, ABC ACTION NEWS (Jan. 14, 2022), 6abc.com/car-thefts-auto-dealerships-6abc-investigation-barbera-autoland/11464047/.

[9] *See* Stolen Vehicle Statistics, CITY OF PORTLAND, https://www.portlandoregon.gov/police/74369 (compare selecting Jan. – May 2022 with Jan. – May 2021 in "Filter by Reported Date of Theft").

[10] *See* Henry Graff, *Richmond Police See 54% Increase in Vehicle Thefts Over Last Year*, NBC12 (Apr. 7, 2022), www.nbc12.com/2022/04/07/richmond-police-see-54-increase-vehicle-thefts-over-last-year/.

[11] *See* Rocco Parascandola, *NYPD Reports 51% Surge in Stolen Cars This Year*, N.Y. DAILY NEWS (June 12, 2022), www.nydailynews.com/new-york/nyc-crime/ny-car-vehicle-theft-surge-careless-motorists-nypd-20220612-eojbb2hhx5a3tn34vzhilc2fdq-story.html.

[12] *See* Nathan Bomey, *Thieves strike: Auto Theft Spikes During the Pandemic as Cars Are Left Unattended*, USA TODAY (Aug. 31, 2021), usatoday.com/story/money/cars/2021/08/31/auto-theft-spikes-stolen-car-vehicle-theft-pandemic-nicb/5652615001/.

[13] Rocco Parascandola, *supra* note 11.

Second, and perhaps more worryingly, a common type of keyless entry system that allows a driver to unlock and start the vehicle without needing to touch the key — known as a passive entry system — appear to be vulnerable to a "relay attack," in which a thief uses a signal amplifier to fool the car into believing that the owner is nearby.[14] Researchers have long known that bad actors could amplify radio signals emitted from the vehicle and key, allowing them to enter and start a vehicle even if the fob is nowhere nearby.[15] In recent years, devices that enable relay attacks have become widely available,[16] and news reports have identified thefts involving relay attacks in Austin,[17] Cincinnati,[18] and Los Angeles.[19]

More recently, researchers have shown that carmakers that use Bluetooth Low Energy (BLE) entry systems — which uses Bluetooth technology to determine whether the vehicle is within a certain distance of the connected device — are also vulnerable to theft using similar relay technology, affecting manufacturers such as Tesla that have adopted BLE passive entry systems.[20] For that reason, the Bluetooth Special Interest Group, the standard-setting organization that oversees the development of Bluetooth technologies, warns that BLE "should not be used as the only protection of valuable assets."[21] Car manufacturers have only recently begun using BLE technology to determine the proximity of a key fob, so researchers have not yet confirmed any vehicles stolen through a BLE relay attack. However, as manufacturers increasingly equip devices — such as smart locks for homes[22] — with BLE passive entry systems, this vulnerability could put a broad range of critical security systems at risk.

Fortunately, researchers have also identified methods to mitigate the risk of passive entry thefts. For example, manufacturers can prevent a fob from unlocking a vehicle if the fob was not recently in motion, as typically occurs as a driver approaches a vehicle. In other words, if the fob is idle, the driver is likely not trying to unlock their own vehicle; any attempt to use the fob in that state may be a sign of a relay attack. Similarly, manufacturers could require consumers to complete an additional verification, such as inputting a PIN number, to enter the vehicle. While such systems inherently inconvenience consumers, they also are a strong defense against relay

---

[14] Rachel Wait, *Keyless Car Crime: How to Thwart the Thieves*, FORBES ADVISOR (Mar. 24, 2022), www.forbes.com/uk/advisor/car-insurance/keyless-car-crime/.

[15] *See* ARI JUELS, RFID SECURITY AND PRIVACY: A RESEARCH SURVEY 13 (2005), www.arijuels.com/wp-content/uploads/2013/09/J06a.pdf.

[16] *See* Joseph Cox, *Meet the Guy Selling Wireless Tech to Steal Luxury Cars in Seconds*, VICE NEWS (Feb. 11, 2020), www.vice.com/en/article/7kz48x/guy-selling-relay-attack-keyless-repeaters-to-steal-cars.

[17] *See* Bettie Cross, *Car Thieves Are Hacking Key Fobs to Quickly and Quietly Steal Vehicles*, CBS AUSTIN (May 12, 2022), cbsaustin.com/news/local/car-thieves-are-hacking-key-fobs-to-quickly-and-quietly-steal-vehicles.

[18] *See* Jatara McGee, *Hackers Are Using New Tech to Steal Locked Cars Without Keys*, WLWT (May 9, 2019), www.wlwt.com/article/hackers-are-using-new-tech-to-steal-locked-cars-without-keys/27424367#.

[19] *See* Nick Bilton, *Keeping Your Car Safe From Electronic Thieves*, N.Y. TIMES (Apr. 15, 2015), www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html.

[20] *See* Sultan Khan, *Technical Advisory – Tesla BLE Phone-as-a-Key Passive Entry Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-tesla-ble-phone-as-a-key-passive-entry-vulnerable-to-relay-attacks/.

[21] BLUETOOTH SIG, PROXIMITY PROFILE 17 (2015), www.bluetooth.com/specifications/specs/proximity-profile-1-0-1/.

[22] *See* Sultan Khan, *Technical Advisory – Kwikset/Weiser BLE Proximity Authentication in Kevo Smart Locks Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-kwikset-weiser-ble-proximity-authentication-in-kevo-smart-locks-vulnerable-to-relay-attacks/.

attacks. Finally, automakers could also adopt Ultra-Wide-Band (UWB) technology, which enables a precise measurement between the vehicle and key fob and, in combination with other technologies, allows the vehicle to determine if the radio signal has been improperly amplified. Experts have suggested that UWB technology could significantly reduce the risk of relay theft.[23]

Given the recent surge in vehicle thefts and the potential security risks involved in keyless entry systems, I respectfully request that you respond in writing to the following questions by August 10, 2022:

1. Please provide the following data, as available, on thefts of vehicles manufactured by your company:

    a. How many vehicles manufactured by your company were stolen in 2019, 2020, 2021, and through the first six months of 2022?

    b. Of those vehicle thefts, how many were caused by thieves taking advantage of key fobs left in vehicles?

    c. Of those vehicle thefts, how many were caused by relay attacks?

2. Please describe the type of transponder and the technology standard that vehicles manufactured by your company use to communicate with key fobs and other devices. If vehicles manufactured by your company use different types of transponders and technology standards, please provide information on all types.

3. Please describe the testing that your company has done to assess the security of its keyless entry systems.

4. What specific steps has your company taken to reduce the vulnerability of its keyless entry system?

    a. Has your company considered making the keyless entry system motion activated?

    b. Has your company considered adopting Ultra-Wide-Band technology?

    c. Has your company considered creating mechanisms to alert owners if their key fob is left inside the vehicle?

5. Does your company plan to take any further steps to reduce any vulnerability of its keyless entry system?

Thank you for your prompt attention to these questions.

---

[23] *See e.g.,* Mridula Singh et al., *UWB with Pulse Reordering: Securing Ranging against Relay and Physical-Layer Attacks*, NETWORK AND DISTRIB. SYS, SEC. SYMP. (2019), www.ndss-symposium.org/ndss-paper/uwb-with-pulse-reordering-securing-ranging-against-relay-and-physical-layer-attacks/.

Sincerely,

Edward J. Markey
United States Senator

United States Senate

July 20, 2022

Anders Gustafsson
President and Chief Executive Officer
Volvo Car USA
1800 Volvo Place
Mahwah, NJ 07430

Dear Mr. Gustafsson,

I write to request information about the security of Volvo's motor vehicle keyless entry systems. Keyless entry systems — which allow users to enter a vehicle and start its engine without inserting and turning a key — likely helped reduce vehicle thefts since the 1990s, but the dramatic 30-year decline has suddenly gone into reverse. Although the exact cause of this turnaround is unclear, a growing body of evidence suggests that keyless entry systems may play a role. We therefore urge Volvo to take all necessary steps to ensure that keyless entry systems, once a security innovation that deterred thieves, do not become a security liability for them to exploit.

After their adoption in the 1990s, keyless entry systems contributed to the impressive decline in car thefts from 1990 to 2019. These systems come in different forms. Some simply allow the driver to enter a vehicle without inserting a physical key into the door lock, while others, called passive entry systems, allow the driver to start the vehicle without inserting a physical key into the ignition. In both cases, the vehicle and a key fob communicate through radio signals, and an "engine immobilizer" prevents the vehicle from starting unless the key fob is nearby.

These systems were a critical advancement in vehicle security. Old-fashioned "hotwiring" a vehicle — that is, bypassing the ignition and starting a vehicle without a key — became far more difficult; with keyless entry systems, cars would not start unless they detected, through the radio signals, the presence of the key fob. In 1995, the European Union required manufacturers to include engine immobilizers on all new vehicles within three years, and Australia and Canada passed similar laws soon thereafter. One study estimated that the EU mandate reduced vehicle thefts in the Netherlands from 1995 to 2008 by 40 percent.[1] The United States never imposed a similar requirement, but many manufacturers have voluntarily adopted keyless entry systems, and car thefts per capita decreased by two-thirds from 1990 to 2019.[2]

---

[1] Jan C. van Ours and Ben Vollaard, *The Engine Immobiliser: A Non-Starter for Car Thieves*, 126 ECON. J. 1264, 1266 (2016), https://onlinelibrary.wiley.com/doi/abs/10.1111/ecoj.12196.

[2] Crime Data Explorer, FED. BUREAU OF INVESTIGATIONS, https://crime-data-explorer.app.cloud.gov/pages/explorer/crime/crime-trend (select "1990" in "From" and "2019" in "To" and "Motor vehicle theft" in "Crime Select").

Although this decrease tracked the overall decline in violent and property crime,[3] news reports have nevertheless attributed part of the decline to the adoption of keyless ignitions.[4]

This remarkably consistent trend towards fewer vehicle thefts, however, has made a concerning U-turn since the end of 2019. According to data compiled by the Federal Bureau of Investigation (FBI), U.S. car thefts per capita increased nationally by 11.8 percent in 2020.[5] Although national data has not yet been released for 2021, news reports suggest that car thefts continued to accelerate across the country last year. For example, in 2021, the number of car thefts appears to have increased by 132 percent in Milwaukee,[6] 70 percent in Washington, DC,[7] and 60 percent in Philadelphia.[8] This trend appears to have continued into 2022. So far this year, as compared with the same period in 2021, the number of car thefts has increased 74 percent in Portland, Ore.,[9] 54 percent in Richmond, Va.,[10] and 51 percent in New York City.[11] After so many years of progress, this rapid reversal in car thefts is alarming.

The same keyless entry systems that contributed to the decline in car thefts may now be providing an opportunity for thieves. Keyless entry systems are vulnerable in two ways. First, drivers may leave their key fobs in their cars, allowing a thief to easily start and steal a vehicle.[12] Whereas drivers used to have to remove the physical key from the ignition when they exited the vehicle, no similar action is necessary when a driver need only push a button to start or stop an engine. According to the New York Police Department, roughly 40 percent of car thefts in New York City so far this year were the result of motorists leaving their vehicles running or unlocked, often with keys or a key fob inside.[13] Keyless technology has thus escalated the consequences of ordinary human error.

---

[3] *Id.* (select "All Property Crimes" or "All Violent Crimes" in "Crime Select").

[4] *See, e.g.*, Sarah Maslin Nir, *Here's Why Car Thefts Are Soaring (Hint: Check Your Cup Holder)*, N.Y. TIMES (Jan. 6, 2021), www.nytimes.com/2021/01/06/nyregion/car-thefts-nyc.html; Brad Stone, *Pinch My Ride*, Wired (Aug. 1, 2006), www.wired.com/2006/08/carkey/.

[5] Crime Data Explorer, *supra* note 3 (select "2019" in "From" and "2020" in "To" and "Motor vehicle theft" in "Crime Select").

[6] *See* Teddy Nykiel, *Over 500% Spike in Auto Thefts Troubles Downtown*, MILWAUKEE BUS. J. (Feb. 9, 2022), https://www.bizjournals.com/milwaukee/news/2022/02/09/crime-statistics-mpd-2021-car-lefts.html.

[7] *See* Bruce Leshan, *Surge in Carjackings, Car Thefts Has Police Struggling to Respond*, WUSA (Feb. 9, 2021), www.wusa9.com/article/news/crime/surge-in-carjackings-car-thefts-dc-police-form-task-force/65-8c4b0c03-e343-430e-9c77-c5d9daade558.

[8] *See* Chad Pradelli and Cheryl Mettendorf, *Action News Investigation into Rise of Dealership Auto Thefts in Philadelphia Region*, ABC ACTION NEWS (Jan. 14, 2022), 6abc.com/car-thefts-auto-dealerships-6abc-investigation-barbera-autoland/11464047/.

[9] *See* Stolen Vehicle Statistics, CITY OF PORTLAND, https://www.portlandoregon.gov/police/74369 (compare selecting Jan. – May 2022 with Jan. – May 2021 in "Filter by Reported Date of Theft").

[10] *See* Henry Graff, *Richmond Police See 54% Increase in Vehicle Thefts Over Last Year*, NBC12 (Apr. 7, 2022), www.nbc12.com/2022/04/07/richmond-police-see-54-increase-vehicle-thefts-over-last-year/.

[11] *See* Rocco Parascandola, *NYPD Reports 51% Surge in Stolen Cars This Year*, N.Y. DAILY NEWS (June 12, 2022), www.nydailynews.com/new-york/nyc-crime/ny-car-vehicle-theft-surge-careless-motorists-nypd-20220612-eojbb2hhx5a3tn34vzhilc2fdq-story.html.

[12] *See* Nathan Bomey, *Thieves strike: Auto Theft Spikes During the Pandemic as Cars Are Left Unattended*, USA TODAY (Aug. 31, 2021), usatoday.com/story/money/cars/2021/08/31/auto-theft-spikes-stolen-car-vehicle-theft-pandemic-nicb/5652615001/.

[13] Rocco Parascandola, *supra* note 11.

Second, and perhaps more worryingly, a common type of keyless entry system that allows a driver to unlock and start the vehicle without needing to touch the key — known as a passive entry system — appear to be vulnerable to a "relay attack," in which a thief uses a signal amplifier to fool the car into believing that the owner is nearby.[14] Researchers have long known that bad actors could amplify radio signals emitted from the vehicle and key, allowing them to enter and start a vehicle even if the fob is nowhere nearby.[15] In recent years, devices that enable relay attacks have become widely available,[16] and news reports have identified thefts involving relay attacks in Austin,[17] Cincinnati,[18] and Los Angeles.[19]

More recently, researchers have shown that carmakers that use Bluetooth Low Energy (BLE) entry systems — which uses Bluetooth technology to determine whether the vehicle is within a certain distance of the connected device — are also vulnerable to theft using similar relay technology, affecting manufacturers such as Tesla that have adopted BLE passive entry systems.[20] For that reason, the Bluetooth Special Interest Group, the standard-setting organization that oversees the development of Bluetooth technologies, warns that BLE "should not be used as the only protection of valuable assets."[21] Car manufacturers have only recently begun using BLE technology to determine the proximity of a key fob, so researchers have not yet confirmed any vehicles stolen through a BLE relay attack. However, as manufacturers increasingly equip devices — such as smart locks for homes[22] — with BLE passive entry systems, this vulnerability could put a broad range of critical security systems at risk.

Fortunately, researchers have also identified methods to mitigate the risk of passive entry thefts. For example, manufacturers can prevent a fob from unlocking a vehicle if the fob was not recently in motion, as typically occurs as a driver approaches a vehicle. In other words, if the fob is idle, the driver is likely not trying to unlock their own vehicle; any attempt to use the fob in that state may be a sign of a relay attack. Similarly, manufacturers could require consumers to complete an additional verification, such as inputting a PIN number, to enter the vehicle. While such systems inherently inconvenience consumers, they also are a strong defense against relay

---

[14] Rachel Wait, *Keyless Car Crime: How to Thwart the Thieves*, FORBES ADVISOR (Mar. 24, 2022), www.forbes.com/uk/advisor/car-insurance/keyless-car-crime/.

[15] *See* ARI JUELS, RFID SECURITY AND PRIVACY: A RESEARCH SURVEY 13 (2005), www.arijuels.com/wp-content/uploads/2013/09/J06a.pdf.

[16] *See* Joseph Cox, *Meet the Guy Selling Wireless Tech to Steal Luxury Cars in Seconds*, VICE NEWS (Feb. 11, 2020), www.vice.com/en/article/7kz48x/guy-selling-relay-attack-keyless-repeaters-to-steal-cars.

[17] *See* Bettie Cross, *Car Thieves Are Hacking Key Fobs to Quickly and Quietly Steal Vehicles*, CBS AUSTIN (May 12, 2022), cbsaustin.com/news/local/car-thieves-are-hacking-key-fobs-to-quickly-and-quietly-steal-vehicles.

[18] *See* Jatara McGee, *Hackers Are Using New Tech to Steal Locked Cars Without Keys*, WLWT (May 9, 2019), www.wlwt.com/article/hackers-are-using-new-tech-to-steal-locked-cars-without-keys/27424367#.

[19] *See* Nick Bilton, *Keeping Your Car Safe From Electronic Thieves*, N.Y. TIMES (Apr. 15, 2015), www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html.

[20] *See* Sultan Khan, *Technical Advisory – Tesla BLE Phone-as-a-Key Passive Entry Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-tesla-ble-phone-as-a-key-passive-entry-vulnerable-to-relay-attacks/.

[21] BLUETOOTH SIG, PROXIMITY PROFILE 17 (2015), www.bluetooth.com/specifications/specs/proximity-profile-1-0-1/.

[22] *See* Sultan Khan, *Technical Advisory – Kwikset/Weiser BLE Proximity Authentication in Kevo Smart Locks Vulnerable to Relay Attacks*, NCC GROUP (May 15, 2022), research.nccgroup.com/2022/05/15/technical-advisory-kwikset-weiser-ble-proximity-authentication-in-kevo-smart-locks-vulnerable-to-relay-attacks/.

attacks. Finally, automakers could also adopt Ultra-Wide-Band (UWB) technology, which enables a precise measurement between the vehicle and key fob and, in combination with other technologies, allows the vehicle to determine if the radio signal has been improperly amplified. Experts have suggested that UWB technology could significantly reduce the risk of relay theft.[23]

Given the recent surge in vehicle thefts and the potential security risks involved in keyless entry systems, I respectfully request that you respond in writing to the following questions by August 10, 2022:

1. Please provide the following data, as available, on thefts of vehicles manufactured by your company:

    a. How many vehicles manufactured by your company were stolen in 2019, 2020, 2021, and through the first six months of 2022?

    b. Of those vehicle thefts, how many were caused by thieves taking advantage of key fobs left in vehicles?

    c. Of those vehicle thefts, how many were caused by relay attacks?

2. Please describe the type of transponder and the technology standard that vehicles manufactured by your company use to communicate with key fobs and other devices. If vehicles manufactured by your company use different types of transponders and technology standards, please provide information on all types.

3. Please describe the testing that your company has done to assess the security of its keyless entry systems.

4. What specific steps has your company taken to reduce the vulnerability of its keyless entry system?

    a. Has your company considered making the keyless entry system motion activated?

    b. Has your company considered adopting Ultra-Wide-Band technology?

    c. Has your company considered creating mechanisms to alert owners if their key fob is left inside the vehicle?

5. Does your company plan to take any further steps to reduce any vulnerability of its keyless entry system?

Thank you for your prompt attention to these questions.

---

[23] *See e.g.*, Mridula Singh et al., *UWB with Pulse Reordering: Securing Ranging against Relay and Physical-Layer Attacks*, NETWORK AND DISTRIB. SYS, SEC. SYMP. (2019), www.ndss-symposium.org/ndss-paper/uwb-with-pulse-reordering-securing-ranging-against-relay-and-physical-layer-attacks/.

Sincerely,

Edward J. Markey
United States Senator