

## Exhibit K-112

### I. THE CLAIMS OF THE '100 PATENT ARE INVALID UNDER 112

#### A. Indefinite

The Asserted Claims of the '100 Patent are invalid as indefinite under Section 112, ¶ 2 for failing to particularly point out and distinctly claim the subject matter which the Applicants regarded as the alleged invention. For example, as demonstrated either individually or collectively by the claim elements addressed below, the Asserted Claims fail to inform those skilled in the art about the scope of the invention with reasonable certainty, rendering the Asserted Claims (and any claims depending therefrom) invalid as indefinite:

- “a first security mechanism to enforce a security measure and form a perimeter network logically including the plurality of on board computational components” (claims 1, 9 and 17)
- “on board computational component not affected by or potentially affected by the instance of a breach of the security measure” (claims 1, 9 and 17)
- “determine whether a computational component affected by the instance of a breach of the security measure can be isolated from at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure.” (claims 1, 9 and 17)
- “isolate” / “isolation” (claims 1, 9 and 17)
- “one or more” (claims 1-3, 9-11, and 17-19)
- “and/or” (claims 1-2, 7, 9, 15, 17-18 and 23)
- “wherein the isolation is one or more of: (1) denying vehicular wireless network access to the computational component affected by the instance

## Exhibit K-112

of a breach of a security measure, (2) directing communications to and from the computational component affected by the instance of a breach of a security measure to a firewall and/or gateway to enforce a security measure, (3) blocking communications to and from the computational component affected by the instance of a breach of a security measure, and (4) activating a second security mechanism in response to the instance of a breach of a security measure” (claims 1, 9 and 17)

- “wherein the security breach instance is one or more of an instance of a virus, malware, unauthorized access, misuse, modification, denial-of-service attack, spoofing, man-in-the-middle attack, ARP poisoning, smurf attack, buffer overflow, heap overflow, format string attack, SQL injection, identity theft (or MAC spoofing), network injection, coffee latte attack, or denial of a computer network and/or network-accessible resource, wherein the network controller receives a warning signal associated with the security breach instance from a gateway, a firewall, a honeypot, a network node impacted by the security breach instance, and a network probe, and wherein the first security mechanism is one or more of: encryption, checks on MAC addresses, disabling ESSID broadcasting, isolating the vehicular network by a firewall and/or gateway, hiding the SSID (Service Set Identifier), MAC ID filtering, static IP addressing, IEEE 802.11, 802.11i, and/or 802.1x security, use of the wired equivalent privacy encryption, TKIP, EAP, LEAP, PEAP, WPAv 1, and/or WPAv2 protocols, end-to-end encryption, and RF shielding substantially surrounding an interior of the vehicle to attenuate signals and prevent wireless signals from propagating

## Exhibit K-112

outside the vehicle.” (Claim 2)

- “wherein at least one of the following is true about the isolation: communications between the at least one on board computational component in a vehicular wireless network not affected by the security breach instance and the computational component affected by the security breach instance, the communications not normally passing through a gateway and/or firewall are redirected through and filtered by the gateway and/or firewall and communications between the at least one on board computational component in a vehicular wireless network not affected by the security breach instance and the computational component affected by the security breach instance are blocked in whole or part.” (Claim 7)
- “the security breach instance” (claim 10)
- “the network controller receives a warning signal associated with the security breach instance from a gateway, a firewall, a honeypot, a network node impacted by the security breach instance, and a network probe,” (claims 2, 10 and 18)
- “security breach instance is one or more of an instance of a virus, malware, unauthorized access, misuse, modification, denial-of-service attack, spoofing, man-in-the-middle attack, ARP poisoning, smurf attack, buffer overflow, heap overflow, format string attack, SQL injection, identity theft (or MAC spoofing), network injection, coffee latte attack, or denial of a computer network and/or network-accessible resource,” (claims 2, 10 and 18)

## Exhibit K-112

- “the first security mechanism is one or more of: encryption, checks on MAC addresses, disabling ESSID broadcasting, isolating the vehicular network by a firewall and/or gateway, hiding the SSID (Service Set Identifier), MAC ID filtering, static IP addressing , IEEE 802.11, 802.11i, and/or 802.1x security, use of the wired equivalent privacy encryption, TKIP, EAP, LEAP, PEAP, WPAv 1, and/or WPAv2 protocols, end-to-end encryption, and RF shielding substantially surrounding an interior of the vehicle to attenuate signals and prevent wireless signals from propagating outside the vehicle.” (claims 2, 10 and 18)
- “wherein the at least one board computational component is one or more of an on-board sensor, processing module, software application, expansion module, critical device, non- critical device, and cellular upgrade module, and wherein the computational component affected by the security breach instance and the at least one on board computational component are both within a perimeter network of the vehicle.” (claims 3, 11 and 19)

The above limitations fail to set forth the scope of the alleged invention with reasonable certainty. The scope of these terms is not reasonably certain. One or more of these limitations is required by all Asserted Claims. Accordingly, all Asserted Claims are indefinite.

### **B. Written Description**

The Asserted Claims of the '034 Patent are also invalid for failure to comply with the written description requirement under Section 112, ¶ 1. For example, the '100 Patent does not contain written description support at least for the following claim terms, either individually or collectively, rendering the Asserted Claims in which they appear (and any claims depending therefrom) invalid for lack of written description:

## Exhibit K-112

- “a first security mechanism to enforce a security measure and form a perimeter network logically including the plurality of on board computational components” (claims 1, 9 and 17)
- “on board computational component not affected by or potentially affected by the instance of a breach of the security measure” (claims 1, 9 and 17)
- “determine whether a computational component affected by the instance of a breach of the security measure can be isolated from at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure.” (claims 1, 9 and 17)
- “isolate” / “isolation” (claims 1, 9 and 17)
- “wherein the isolation is one or more of: (1) denying vehicular wireless network access to the computational component affected by the instance of a breach of a security measure, (2) directing communications to and from the computational component affected by the instance of a breach of a security measure to a firewall and/or gateway to enforce a security measure, (3) blocking communications to and from the computational component affected by the instance of a breach of a security measure, and (4) activating a second security mechanism in response to the instance of a breach of a security measure” (claims 1, 9 and 17)
- “wherein the security breach instance is one or more of an instance of a virus, malware, unauthorized access, misuse, modification, denial-of-service attack, spoofing, man-in-the-middle attack, ARP poisoning, smurf attack, buffer overflow, heap overflow, format string attack, SQL injection,

## Exhibit K-112

identity theft (or MAC spoofing), network injection, coffee latte attack, or denial of a computer network and/or network-accessible resource, wherein the network controller receives a warning signal associated with the security breach instance from a gateway, a firewall, a honeypot, a network node impacted by the security breach instance, and a network probe, and wherein the first security mechanism is one or more of: encryption, checks on MAC addresses, disabling ESSID broadcasting, isolating the vehicular network by a firewall and/or gateway, hiding the SSID (Service Set Identifier), MAC ID filtering, static IP addressing, IEEE 802.11, 802.11i, and/or 802.1x security, use of the wired equivalent privacy encryption, TKIP, EAP, LEAP, PEAP, WPAv 1, and/or WPAv2 protocols, end-to-end encryption, and RF shielding substantially surrounding an interior of the vehicle to attenuate signals and prevent wireless signals from propagating outside the vehicle.” (Claim 2)

- “the security breach instance” (claim 10)
- “the network controller receives a warning signal associated with the security breach instance from a gateway, a firewall, a honeypot, a network node impacted by the security breach instance, and a network probe,” (claims 2, 10 and 18)
- “security breach instance is one or more of an instance of a virus, malware, unauthorized access, misuse, modification, denial-of-service attack, spoofing, man-in-the-middle attack, ARP poisoning, smurf attack, buffer overflow, heap overflow, format string attack, SQL injection, identity theft (or MAC spoofing), network injection, coffee latte attack, or denial of a

## Exhibit K-112

computer network and/or network-accessible resource,” (claims 2, 10 and 18)

- “the first security mechanism is one or more of: encryption, checks on MAC addresses, disabling ESSID broadcasting, isolating the vehicular network by a firewall and/or gateway, hiding the SSID (Service Set Identifier), MAC ID filtering, static IP addressing , IEEE 802.11, 802.11i, and/or 802.1x security, use of the wired equivalent privacy encryption, TKIP, EAP, LEAP, PEAP, WPAv 1, and/or WPAv2 protocols, end-to-end encryption, and RF shielding substantially surrounding an interior of the vehicle to attenuate signals and prevent wireless signals from propagating outside the vehicle.” (claims 2, 10 and 18)
- “wherein the at least one board computational component is one or more of an on-board sensor, processing module, software application, expansion module, critical device, non- critical device, and cellular upgrade module, and wherein the computational component affected by the security breach instance and the at least one on board computational component are both within a perimeter network of the vehicle.” (claims 3, 11 and 19)

At least under AutoConnect’s apparent interpretation and application of the Asserted Claims, the ’100 Patent does not provide sufficient written description support for the above claim terms. The specification provides insufficient support for any of the above identified limitations to describe to a person of skill in the art what has been claimed. Instead, the specification describes aspirational functionality without describing how such limitations are to be implemented in the invention. Moreover, the specification does not provide written description support for the full scope of the claims to the extent the scope of the claims is interpreted to cover the accused

## Exhibit K-112

embodiments, which are not described in the specification.

One or more of these limitations is required by all Asserted Claims. Accordingly, all Asserted Claims are invalid for lack of written description.

### C. Lack of Enablement

The Asserted Claims of the '100 Patent are also invalid for failure to comply with the enablement requirement under Section 112, ¶ 1. For example, the '100 Patent fails to provide an enabling disclosure with respect to the following claim terms, either individually or collectively, rendering the Asserted Claims in which they appear (and any claims depending therefrom) invalid for lack of enablement:

- “a first security mechanism to enforce a security measure and form a perimeter network logically including the plurality of on board computational components” (claims 1, 9 and 17)
- “on board computational component not affected by or potentially affected by the instance of a breach of the security measure” (claims 1, 9 and 17)
- “determine whether a computational component affected by the instance of a breach of the security measure can be isolated from at least one on board computational component not affected by or potentially affected by the instance of a breach of the security measure.” (claims 1, 9 and 17)
- “isolate” / “isolation” (claims 1, 9 and 17)
- “wherein the isolation is one or more of: (1) denying vehicular wireless network access to the computational component affected by the instance of a breach of a security measure, (2) directing communications to and from the computational component affected by the instance of a breach of

## Exhibit K-112

a security measure to a firewall and/or gateway to enforce a security measure, (3) blocking communications to and from the computational component affected by the instance of a breach of a security measure, and (4) activating a second security mechanism in response to the instance of a breach of a security measure” (claims 1, 9 and 17)

- “the security breach instance” (claim 10)
- “the network controller receives a warning signal associated with the security breach instance from a gateway, a firewall, a honeypot, a network node impacted by the security breach instance, and a network probe,” (claims 2, 10 and 18)
- “security breach instance is one or more of an instance of a virus, malware, unauthorized access, misuse, modification, denial-of-service attack, spoofing, man-in-the-middle attack, ARP poisoning, smurf attack, buffer overflow, heap overflow, format string attack, SQL injection, identity theft (or MAC spoofing), network injection, coffee latte attack, or denial of a computer network and/or network-accessible resource,” (claims 2, 10 and 18)
- “the first security mechanism is one or more of: encryption, checks on MAC addresses, disabling ESSID broadcasting, isolating the vehicular network by a firewall and/or gateway, hiding the SSID (Service Set Identifier), MAC ID filtering, static IP addressing, IEEE 802.11, 802.11i, and/or 802.1x security, use of the wired equivalent privacy encryption, TKIP, EAP, LEAP, PEAP, WPAv 1, and/or WPAv2 protocols, end-to-end

## Exhibit K-112

encryption, and RF shielding substantially surrounding an interior of the vehicle to attenuate signals and prevent wireless signals from propagating outside the vehicle.” (claims 2, 10 and 18)

- “wherein the at least one board computational component is one or more of an on-board sensor, processing module, software application, expansion module, critical device, non- critical device, and cellular upgrade module, and wherein the computational component affected by the security breach instance and the at least one on board computational component are both within a perimeter network of the vehicle.” (claims 3, 11 and 19)

At least under AutoConnect’s apparent interpretation and application of the Asserted Claims, the ’100 Patent does not enable the above claim terms. The specification provides insufficient support for any of the above identified limitations to enable a person of skill in the art to make and use the invention. Instead, the specification describes aspirational functionality without describing how such limitations are to be implemented in the invention.

One or more of these limitations is required by all Asserted Claims. Accordingly, all Asserted Claims are invalid for lack of enablement.