

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION**

SOFTEX LLC, Plaintiff, vs. ABSOLUTE SOFTWARE CORPORATION AND ABSOLUTE SOFTWARE, INC., Defendants.	Civil Action No. 1:22-cv-01308-DAE JURY TRIAL DEMANDED
SOFTEX LLC, Plaintiff, vs. DELL TECHNOLOGIES INC. AND DELL INC., Defendants.	Civil Action No. 1:22-cv-01309-DAE JURY TRIAL DEMANDED
SOFTEX LLC, Plaintiff, vs. HP INC., Defendant.	Civil Action No. 1:22-cv-01311-DAE JURY TRIAL DEMANDED

DEFENDANTS’ INITIAL INVALIDITY CONTENTIONS

Defendants Absolute Software Corporation and Absolute Software, Inc. (“Absolute”), Dell Technologies Inc. and Dell Inc. (“Dell”), and HP Inc. (“HP”) (collectively, “Defendants”) hereby submit the following Initial Invalidity Contentions to Plaintiff Softex LLC (“Softex” or “Plaintiff”) regarding claims 1-3, 5-14, and 16-27 of U.S. Patent No. 7,590,837 (the “’837 Patent” or “’837”); claims 1-8, 11-21, and 23 of U.S. Patent No. 8,128,710 (the “’710 Patent” or “’710”); claims 1-4,

7-11, and 14-20 of U.S. Patent No. 8,137,410 (the “’410 Patent” or “’410”); claims 1-19 of U.S. Patent No. 8,145,892 (the “’892 Patent” or “’892”); claims 1-4, 10-14, and 18-20 of U.S. Patent No. 8,287,603 (the “’603 Patent” or “’603”); claims 1, 7, 9, and 15 of U.S. Patent No. 8,506,649 (the “’649 Patent” or “’649”); and claims 1-21 of U.S. Patent No. 8,516,235 (the “’235 Patent” or “’235”) (collectively, the “Asserted Claims” of the “Asserted Patents”).¹

The following contentions are based on Defendants’ current understanding of the Asserted Claims as applied in Plaintiff’s Preliminary Infringement Contentions, served on May 4, 2023 without the benefit of claim construction and with generalized discovery not yet open in the present litigation. Claim construction discovery in this action has not yet commenced, and Defendants will provide their claim construction positions at the appropriate time pursuant to the parties’ Corrected Joint Rule 26(f) Reports.² Accordingly, these Initial Invalidity Contentions may reflect various potential and alternative positions regarding claim construction and scope. To the extent these contentions reflect or suggest a particular interpretation or reading of any claim element, Defendants do not adopt or agree to any such interpretation or reading. Defendants’ contentions therefore should not be relied upon as a statement of Defendants’ claim interpretations and should not be relied upon as any admission regarding the proper scope of the claims. Defendants’ claim construction positions will be provided at a later appropriate time in this case, as noted above.

Nor do these Initial Invalidity Contentions constitute any admission by Defendants that any accused products, including any current or past versions of those products, are covered by any

¹ Absolute, HP, and Dell each individually serve these Initial Invalidity Contentions on Plaintiff. Service of identical contentions, in a consolidated format, does not constitute an admission that Defendants believe their actions with Plaintiff should be consolidated. Defendants HP and Dell maintain that a stay is warranted in their respective cases, as evidenced by consistent invalidity theories with Absolute at this stage.

² D.I. 33, 1:22-cv-01308-DAE; D.I. 45, 1:22-cv-01309-DAE; D.I. 44, 1:22-cv-01311-DAE.

Asserted Claim, including but not limited to the disclosure of Absolute products or functionality pre-dating August 2003 as prior art in these Invalidity Contentions. Defendants do not take any position herein regarding the proper scope or construction of the Asserted Claims.

These Invalidity Contentions try to take into account and apply Plaintiff's apparent interpretations of the Asserted Claims. Accordingly, any assertion herein that a particular limitation is disclosed by a prior art reference or references may be based in part on Plaintiff's apparent interpretation and is not intended to be, and is not, an admission by Defendants that any such construction is supportable or correct. To the extent the following contentions reflect constructions of claim limitations consistent with or implicit in Plaintiff's Infringement Contentions, no inference is intended, nor should any be drawn, that Defendants agree with or concede those claim constructions. Defendants expressly do not do so and reserve their right to contest them.

To the extent that prior art cited for a particular limitation discloses functionality that is the same or similar in some respects to the alleged functionality in the accused products and/or services as set forth in Plaintiff's Infringement Contentions, Defendants do not concede that those limitations are in fact met by those accused functionalities. However, to the extent Plaintiff accuses the same or similar functionality as that disclosed in the prior art, Defendants contend such functionality is evidence of invalidity.

Defendants further reserve the right to supplement and amend these disclosures and associated document production based on further investigation, analysis, and discovery, Defendants' consultation with experts and others, and contentions or court rulings on relevant issues such as claim construction and priority dates. For example, since generalized fact discovery has not yet begun, deposing the alleged inventors may reveal information that affects the

disclosures and contentions herein. Furthermore, in its Infringement Contentions Plaintiff has asserted that the alleged inventions of the Asserted Patents are entitled to a priority date of “[n]o later than August 23, 2003.”³ Defendants have relied on this assertion in identifying and selecting prior art in connection with these Invalidity Contentions. Thus, Defendants reserve the right to amend these Invalidity Contentions and/or modify their selection of prior art references if Plaintiff is permitted to allege any date of alleged conception and corroborating evidence prior to the date identified above, or if Plaintiff is unable to prove that any of the Asserted Claims are entitled to the August 23, 2003 priority claim. Defendants also reserve the right to amend these Invalidity Contentions and/or to modify its selection of prior art references in the event that Plaintiffs serve supplemental or modified infringement contentions.

Because Defendants are continuing their analysis of relevant prior art, and as generalized fact discovery (including third party discovery) has not yet opened, Defendants reserve the right to revise, amend, and/or supplement the information provided herein, including identifying, charting, and/or relying upon additional prior art references, relevant disclosures, and bases for Invalidity Contentions. Additional prior art, disclosures, and invalidity defects, whether cited in this disclosure and whether known to Defendants, may become relevant as investigation, analysis, and discovery continue, and following claim construction proceedings in this case. Defendants are currently unaware of the extent, if any, to which Plaintiff will contend that limitations of the Asserted Claims are not disclosed in the prior art identified by Defendants. To the extent that such an issue arises, Defendants reserve the right to identify and rely upon other references or portions of references regarding the allegedly missing limitation(s).

³ Preliminary Infringement Contentions, at 2.

Additionally, Defendants reserve the right to present additional prior art references and/or disclosures under 35 U.S.C. §§ 102(a), (b), (e), (f), and/or (g), and/or § 103, located during the course of such discovery or further investigation, and to assert invalidity under 35 U.S.C. §§ 102(c), (d), or (f) to the extent that such discovery or investigation yields information forming the basis for such invalidity.

Additionally, Defendants reserve the right to use these disclosures as well as further discovery and disclosures relating to the alleged utility and advantages of the Asserted Claims over old modes and devices for purposes of any damages issues in the case.

Furthermore, to the extent Plaintiff asserts the doctrine of equivalents, a “doctrine of equivalents theory cannot be asserted if it will encompass or ‘ensnare’ the prior art.” *Jang v. Boston Sci. Corp.*, 872 F.3d 1275, 1285 (Fed. Cir. 2017). To the extent Plaintiff asserts the doctrine of equivalents for any of the claimed limitations, they would ensnare the prior art for the reasons and based on the evidence discussed below and in the accompanying charts. Defendants reserve the right to use these disclosures as well as further discovery and disclosures for purposes of noninfringement.

I. The Asserted Claims are Invalid under 35 U.S.C. §§ 102 and 103⁴

A. The Asserted Claims of the ’837 Patent

The non-provisional application leading to issuance of the ’837 Patent was filed on August 23, 2004. While the ’837 Patent is matured from a provisional application (No. 60/497,182) filed on August 23, 2003, it is not presumptively entitled to claim priority to that application. It is Plaintiff’s burden to establish that all of the elements of the Asserted Claims of the ’837 Patent

⁴ References throughout to 35 U.S.C. §§ 101 *et al.* refer to pre-AIA versions of those statutes.

have both written description and enablement support in the pre-August 23, 2004 application should Plaintiff seek to predate that date for purposes of the prior art.

B. The Asserted Claims of the '710 Patent

The non-provisional application leading to issuance of the '710 Patent was filed on October 30, 2007. While the '710 Patent is a continuation to the non-provisional application leading to the issuance of U.S. Patent No. 7,590,837, filed on August 23, 2004, it is not presumptively entitled to claim priority to that application or its underlying provisional application, No. 60/497,182. It is Plaintiff's burden to establish that all of the elements of the Asserted Claims of the '710 Patent have both written description and enablement support in the pre-October 30, 2007 application(s) should it seek to predate that date for purposes of the prior art.

C. The Asserted Claims of the '410 Patent

The non-provisional application leading to issuance of the '410 Patent was filed on July 2, 2008. While the '410 Patent is a divisional to the non-provisional application leading to the issuance of U.S. Patent No. 7,590,837, filed on August 23, 2004, it is not presumptively entitled to claim priority to that application or its underlying provisional application, No. 60/497,182. It is Plaintiff's burden to establish that all of the elements of the Asserted Claims of the '410 Patent have both written description and enablement support in the pre-July 2, 2008 application(s) should it seek to predate that date for purposes of the prior art.

D. The Asserted Claims of the '892 Patent

The non-provisional application leading to issuance of the '892 Patent was filed on October 30, 2007. While the '892 Patent is a continuation to the non-provisional application leading to the issuance of U.S. Patent No. 7,590,837, filed on August 23, 2004, it is not presumptively entitled to claim priority to that application or its underlying provisional application, No. 60/497,182. It is

Plaintiff's burden to establish that all of the elements of the Asserted Claims of the '892 Patent have both written description and enablement support in the pre-October 30, 2007 application(s) should it seek to predate that date for purposes of the prior art.

E. The Asserted Claims of the '603 Patent

The non-provisional application leading to issuance of the '603 Patent was filed on August 7, 2009. While the '603 Patent is a divisional to the non-provisional application leading to the issuance of U.S. Patent No. 7,590,837, filed on August 23, 2004, it is not presumptively entitled to claim priority to that application or its underlying provisional application, No. 60/497,182. It is Plaintiff's burden to establish that all of the elements of the Asserted Claims of the '603 Patent have both written description and enablement support in the pre-August 7, 2009 application(s) should it seek to predate that date for purposes of the prior art.

F. The Asserted Claims of the '649 Patent

The non-provisional application leading to issuance of the '649 Patent was filed on July 11, 2006. While the '649 Patent is a divisional to the non-provisional application leading to the issuance of U.S. Patent No. 7,590,837, filed on August 23, 2004, it is not presumptively entitled to claim priority to that application or its underlying provisional application, No. 60/497,182. It is Plaintiff's burden to establish that all of the elements of the Asserted Claims of the '649 Patent have both written description and enablement support in the pre-July 11, 2006 application(s) should it seek to predate that date for purposes of the prior art.

G. The Asserted Claims of the '235 Patent

The non-provisional application leading to issuance of the '235 Patent was filed on October 30, 2007. While the '235 Patent is a continuation to the non-provisional application leading to the issuance of U.S. Patent No. 7,590,837, filed on August 23, 2004, it is not presumptively entitled

to claim priority to that application or its underlying provisional application, No. 60/497,182. It is Plaintiff's burden to establish that all of the elements of the Asserted Claims of the '235 Patent have both written description and enablement support in the pre-October 30, 2007 application(s) should it seek to predate that date for purposes of the prior art.

H. Identity of Each Item of Prior Art

Subject to Defendants' reservation of rights, Defendants identify each item of prior art that anticipates or renders obvious one or more of the Asserted Claims in the attached Prior Art Index submitted herewith. (*See Appendix A, infra.*) To the extent that the references listed in **Appendix A** are not identified as items of prior art that anticipate and/or render obvious an Asserted Claim, Defendants intend to rely on these references as background and as evidence of the state of the art at the time of Plaintiff's alleged invention and/or as demonstrating inherency in the prior art.

Additionally, several of the prior art references are related patent applications and issued patents that contain substantially the same subject matter (e.g., published U.S. patent applications, and issued U.S. Patents, foreign applications and issued patents). Any citation to or quotation from any of these patent applications or patents, therefore, should be understood as encompassing any parallel citation to the same subject matter in other related to corresponding applications or patents. Defendants also reserve the right to later rely upon all references or portions of references provided in **Appendix A** to supplement or amend its disclosures contained herein. Also, to the extent not expressly mentioned herein, Defendants incorporate by reference any and all prior art contained or identified in documents that will be produced or should be produced by Plaintiff to Defendants in this case.

Each disclosed item of prior art is evidence of a prior invention by another under 35 U.S.C. § 102(g), as evidenced by the named inventors, authors, organizations, and publishers involved

with each such reference. Defendants further intend to rely on admissions of the named inventors concerning the prior art, including statements found in the Asserted Patents, their prosecution histories, related patents and/or patent applications, any testimony, and the papers filed and evidence submitted by Plaintiff in conjunction with this litigation.

I. Whether Prior Art Anticipates or Renders Obvious the Asserted Claims

Subject to Defendants' reservation of rights, Defendants identify in the attached **Exhibits A-1 through A-26, B-1 through B-27, C-1 through C-44, D-1 through D-26, E-1 through E-31, F-1 through F-45, and G-1 through G-41**, identified in **Appendix B** ("Prior Art Invalidity Charts") prior art references that anticipate the Asserted Claims under at least 35 U.S.C. §§ 102(a), (b), (e), and/or (g), either expressly or inherently, and/or render obvious the Asserted Claims under 35 U.S.C. § 103 either alone or in combination with other references. Each Asserted Claim is anticipated by, and/or obvious in view of, one or more items of prior art identified in these disclosures, alone or in combination.⁵ Tables identifying exemplary ways in which the prior art references cited herein anticipate and/or render obvious the Asserted Claims are provided in Section I.A.iv below.

Much of the art identified in the attached Prior Art Invalidity Charts reflects common knowledge and the state of the art at the time of alleged priority date of the Asserted Patents. Defendants may rely on additional citations, references, expert testimony, and other material to provide context or to aid in understanding the cited portions of the references and/or cited features of the systems. Defendants may also rely on expert testimony explaining relevant portions of references, relevant systems, relevant calculations and measurements, and other discovery regarding relevant subject matter. Additionally, Defendants may rely on other portions of any prior

⁵ Although Plaintiff has not asserted claims 2 and 10 of the '649 Patent against Absolute, Exhibits F-1 through F-45 nevertheless address the invalidity of these claims for completeness.

art reference for purposes of explaining the background and general technical subject area of the reference.

Where an individual reference is cited with respect to all elements of an Asserted Claim, Defendants contend that the reference anticipates the claim under 35 U.S.C. §§ 102(a), (b), (e), and/or (g) and also renders obvious the claim under 35 U.S.C. § 103, both by itself in view of the knowledge of a person of ordinary skill in the art and in combination with the other cited references to the extent the reference is not found to disclose one or more claim elements. A single prior art reference, for example, can establish obviousness where the differences between the disclosures within the reference and the claimed invention would have been obvious to one of ordinary skill in the art. For instance, “[c]ombining two embodiments disclosed adjacent to each other in a prior art patent does not require a leap of inventiveness.” *Boston Sci. Scimed, Inc. v. Cordis Corp.*, 554 F.3d 982, 991 (Fed. Cir. 2009). To the extent Plaintiff contends that an embodiment within a particular item of prior art does not fully disclose all limitations of a claim, Defendants accordingly reserve their right to rely on other embodiments in that prior art reference, or other information, to show single reference obviousness under 35 U.S.C. § 103(a).

Where an individual reference is cited with respect to fewer than all elements of an Asserted Claim, Defendants contend that the reference renders obvious the claim under 35 U.S.C. § 103(a) in view of each other reference and combination of references that discloses the remaining claim element(s), as indicated in the Prior Art Invalidity Claim Charts submitted herewith and as more fully discussed below. “Under § 103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved. Against this background, the obviousness or nonobviousness of the subject matter is determined.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398,

406 (2007), quoting *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17-18 (1966). Exemplary motivations to combine references are discussed below. Defendants reserve the right to rely upon any references or assertions identified herein in connection with Defendants' contention that each Asserted Claim is invalid under 35 U.S.C. § 103 and to rely upon expert testimony addressing such references and assertions.

The fact that prior art is identified to anticipate the Asserted Claims presents no obstacle in also relying on that reference as a basis for invalidity based on obviousness. It is established that "a rejection for obviousness under § 103 can be based on a reference which happens to anticipate the claimed subject matter." *In re Meyer*, 599 F.2d 1026, 1031 (C.C.P.A. 1979). To the extent any prior art item listed in **Appendix A** may not fully disclose a limitation of an Asserted Claim or is alleged by Plaintiff to lack disclosure of the limitation, such limitation is present and identified in another prior art item as shown in the attached Prior Art Invalidity Claim Charts.

Many of the references cited in the Prior Art Invalidity Claim Charts cite or relate to additional references and/or products, systems, or services. Defendants may rely upon such additional references and copies or exemplars of such products or systems. Defendants will produce or make available for inspection any such cited references that they intend to rely upon. Defendants may also rely upon the disclosures of the references cited and/or discussed during the prosecution of the Asserted Patents and/or the assertions presented regarding those references. Defendants reserve the right to further streamline and reduce the number of anticipation or obviousness references relied upon with respect to a given Asserted Claim and to exchange or otherwise modify the specific references relied upon for anticipation and within each obviousness combination for each Asserted Claim.

Each limitation of the Asserted Claims was well-known to those of ordinary skill in the art before the alleged priority dates of the Asserted Patents, as detailed below and described in the accompanying Prior Art Invalidity Charts. As explained more fully below and throughout these Invalidity Contentions, the Asserted Claims of the Asserted Patents are anticipated and/or obvious in view of the prior art references listed in **Appendix A**.

A. Obviousness and Motivations to Combine

Each prior art reference may be combined with one or more other prior art references to render obvious the Asserted Claims in combination, as explained in more detail below. The disclosures of these references also may be combined with information known to persons skilled in the art at the time of the alleged invention, and understood and supplemented in view of the common sense of persons skilled in the art at the time of alleged invention, including any statements in the intrinsic record of the Asserted Patents and related applications.

A person of ordinary skill in the art would have been motivated to combine the prior art references in **Appendix A** based on the nature of the problem to be solved, the teachings of the prior art, and the knowledge of persons of ordinary skill in the art. The identified prior art references, including portions cited in the Prior Art Invalidity Charts submitted herewith, address the same or similar technical issues and suggest the same or similar solutions to those issues at the Asserted Claims. On an element-by-element basis, Defendants expressly intend to combine one or more prior art items identified in **Appendix A** with each other to address any contentions from Plaintiff that a particular prior art item supposedly lacks one or more elements of an Asserted Claim. In other words, Defendants contend that each charted prior art item can be combined with other charted prior art items when a particular prior art item lacks or does not explicitly disclose an element or feature of an Asserted Claim. The suggested obviousness combinations described

below are not to be construed to suggest that any reference included in the combinations is not anticipatory. Further, to the extent Plaintiff contends that any of the anticipatory prior art fails to disclose one or more limitations of the Asserted Claims, Defendants reserve the right to identify other prior art references that, when combined with the anticipatory prior art, would render the claims obvious despite an allegedly missing limitation. Defendants will further specify the motivations to combine the prior art, including through reliance on expert testimony, at the appropriate later stage of this litigation.

A person of ordinary skill in the art would have been motivated to combine the prior art items identified in **Appendix A** and/or described in the Prior Art Invalidity Charts. As the Supreme Court held in *KSR International Company v. Teleflex, Inc.*: “The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results.” 550 U.S. at 416. The Supreme Court further held that, “[w]hen a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one. If a person of ordinary skill can implement a predictable variation, § 103 likely bars its patentability. For the same reason, if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill.” *Id.* at 417.

Moreover, “in many cases a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle.” *Id.* at 420. It is sufficient that a combination of elements was “obvious to try” holding that, “[w]hen there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp. If

this leads to the anticipated success, it is likely the product not of innovation but of ordinary skill and common sense.” *Id.* at 421. “In that instance the fact that a combination was obvious to try might show that it was obvious under § 103.” *Id.* Finally, the Supreme Court recognized that “[g]ranting patent protection to advances that would occur in the ordinary course without real innovation retards progress and may, in the case of patents combining previously known elements, deprive prior inventions of their value or utility.” *Id.* at 419. All of the following rationales recognized in *KSR* support a finding of obviousness:

- 1) Combining prior art elements according to known methods to yield predictable results;
- 2) Simple substitution of one known element for another to obtain predictable results;
- 3) Use of known techniques to improve similar devices (methods or products) in the same way;
- 4) Applying a known technique to a known device (method or product) ready for improvement to yield predictable results;
- 5) “Obvious to try”—choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success;
- 6) Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art; and

7) Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

Certain of these rationales are discussed more specifically below. The fact that others are not discussed more specifically should not be interpreted as an admission or concession that it does not apply. To the contrary, the discussion below simply provides more explanation of these specific rationales.

Defendants further contend that the prior art identified in these Initial Invalidity Contentions is evidence of simultaneous or near-simultaneous independent invention by others of the alleged invention as recited in one or more of the Asserted Claims. Defendants reserve their right to rely on the simultaneous or near-simultaneous independent invention by others as further evidence of the obviousness of the Asserted Claims.

Each limitation of the Asserted Claims was well-known to those of ordinary skill in the art before the alleged priority date of the Asserted Patents, as detailed below and in the attached Prior Art Invalidity Charts. The elements recited in the Asserted Claims are mere combinations and modifications of these well-known elements. A person of ordinary skill in the art would have been able and motivated to improve the existing technology in the same or similar manner by combining or modifying the individual elements that were already known in the art to yield predictable results.

Subject to the foregoing, Defendants identify the following exemplary reasons that skilled artisans would have combined elements of the prior art to render obvious the Asserted Claims. The fact that others are not discussed more specifically should not be interpreted as an admission or concession that they do not apply. To the contrary, the discussion below simply provides more explanation of these specific rationales.

i. Motivations Identified During Prosecution

Defendants hereby expressly incorporate by reference any statements and reasons set forth by the Examiner during prosecution of the Asserted Patents and related patent applications as to why it would have been obvious to modify or combine references to achieve the limitations of the Asserted Claims.

ii. Combinations of References Through Citations

Numerous prior art references cite to, discuss, or build upon other references. Where one reference cites or discusses another reference, a person of ordinary skill in the art would have been motivated to consider their teachings in combination, as they would be understood to provide related teachings in a similar field.

In some instances, multiple prior art publications and/or physical references discuss or address the same or substantially similar underlying system, software, or other project, such as commercial software products and successive versions thereof, or multiple publications discussing the same subject matter. Where multiple references discuss or relate to the same or related underlying projects, systems, or other subject matter, it was obvious to combine the discussions and disclosures of the references as they would be understood to describe features or potential features of the underlying project, system, technique, or other subject matter. Similarly, where one reference cites or discusses other references or their teachings, or references have one or more authors in common and a related area of subject matter, it would have been obvious to consider the teachings of the references in combination with each other due to the express relationships and commonalities between the references.

Further, for each set of references that together refer to or describe the same system and/or potential improvements to the same system, it would have been obvious to combine such

references. In particular, to the extent the items are commonly owned, they would be within the knowledge of the same company, and the company would be motivated to use elements from one reference to improve another seeking to solve the same or similar problems.

iii. Obviousness Combination Groups and Further Motivations to Combine

In addition to combinations of references and motivations to combine identified elsewhere herein, including within claim charts, Defendants identify combinations and motivations to combine based on references grouped by subject matter, in the manner approved by district courts regarding invalidity contentions. *See, e.g., Avago Techs. Gen IP PTE Ltd. v. Elan Microelectronics Corp.*, No. C04-05385 JW (HRL), 2007 WL 951818, at *3-4 (N.D. Cal. Mar. 28, 2007) (organizing prior art references into “groups” and identifying combinations as a set of references “and/or” another set of references); *Keithley v. Homestore.com, Inc.*, 553 F. Supp. 2d 1148, 1150 (N.D. Cal. 2008) (following *Avago* – “Apple’s grouping method is permissible under the Local Rules”); *see also Multimedia Patent Tr. v. Apple Inc.*, Case No. 3:10-cv-02618-H (KSC), 2012 WL 12868250 (S.D. Cal. Nov. 5, 2012); *High Point Sarl v. Sprint Nextel Corp.*, No. 09-2269-CM-DJW, 2011 WL 4526770, at *8-9 (D. Kan. Sept. 28, 2011).

Defendants identify references in groups below, based on common subject matter relevant to the Asserted Claims, for the purpose of disclosing obviousness combinations and further disclosing motivations to combine.

The absence of a particular reference from a group is not an admission or suggestion that the reference does not disclose or suggest any particular claim limitations. In some instances, a reference may fully disclose and/or suggest the obviousness of a claim limitation but not be identified within the applicable group for purposes of defining groups of references for purposes of disclosing obviousness combinations for these contentions.

a. Application Component References

The Asserted Claims recite functionality for an application component executing within an operating system environment that determines if an electronic device has been reported stolen based on information received from a server system, and in some instances, (1) is connected and in communication with a non-viewable component, (2) notifies a BIOS component that the electronic device has been reported stolen; and (3) assists in tracking/locating the electronic device. *See, e.g.*, '837, cl. 1 (“an application component to execute within the OS environment... wherein said application component is configured to determine whether the electronic device has been reported stolen, based on information received from the server system ... wherein the application component is configured to notify the BIOS security component that the electronic device has been reported stolen, in response to determining that the electronic device has been reported stolen”); '710, cl. 1 (“(b) an application component... that executes within an operating system environment, ... (d) a server system capable of communicating through a secure medium with the application component”); '410, cl. 1 (“wherein the disk drive comprises An application component associated with tracking and locating the electronic device.”); '892, cl. 1 (“an application component that is connected to the non-viewable component, that is capable of communicating with the non-viewable component, that executes within an operating system environment, and that is capable of communicating through a secure medium with a server system”); '603, cl. 1 (“executing, on the electronic device, an application component, wherein the application component is configured to automatically ascertain whether the electronic device has been reported stolen, based on information received from a server system”); '235, cl. 1 (“an application component connected to the non-viewable component and capable of executing within an operating system environment and of communicating with the non-viewable component.”). At

the time of the invention, the concept of an application component communicating with an external server to determine whether an electronic device had been reported stolen was well-known. Likewise, the state of the art was already well-developed for application components that enable tracking, tracing, and/or otherwise locating an electronic device. And persons of ordinary skill already knew that these tracking application components could be connected to and in communication with non-viewable components of the electronic device. As the attached claim charts demonstrate, use of an application component executing within an operating system environment to determine whether an electronic device has been reported stolen based on information received from a server system is disclosed in at least: Angelo Publication, Choi, Computrace, Cotichini, Isikoff, Morriss, Solymar, Tait, TheftGuard, zTrace.

Persons of ordinary skill in the art would have been motivated to combine the teachings of the Application Component references with any system that seeks to incorporate electronic device theft-prevention techniques and/or device tracking technology. The implementation of an application component associated with tracking and capable of communication with a server system and/or non-viewable component of the electronic device would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. For example, references disclose the following motivations to combine:

- An application component is an obvious choice to implement within small, portable devices because it provides a “very cost effective” way to monitor those devices

and requires only “inexpensive modifications to software or hardware” to the device to implement. *See* Cotichini, 2:55-67.

- An application component, in most (if not all) instances, is implemented within electronic devices in such a way that it is transparent to the end-user, making it less likely that the end-user can detect and attempt to disable the component, thereby increasing the likelihood for locating and recovering the device. *See, e.g.,* Cotichini, 2:55-67 (“[N]o physical alteration is necessary or apparent to a thief. The existence of the security device is well cloaked and thus it cannot be readily located or disabled even if the possibility of its existence is suspected”); Solymar, 2:27-32 (“The agent hides within the software/firmware/hardware of the electronic device, and operates without interfering with the regular operation of the device. The agent is designed to evade detection and resist attempts to disable it by an unauthorized user.”); Choi, [0030] (“[I]t is impossible for another person who picks up the information system or a robber to delete the security and management unit from the information system or stop the operation of it.”). As explained generally in Morriss, these devices can be “quite expensive” and often “contain confidential or personal information of their users” so “the development of [] measures to prevent the loss of a wireless communication device or to secure its recovery in the event of a loss is of great importance in today’s wireless environment.” Morriss, [0003].

Defendants reserve the right to amend, supplement, and/or modify this disclosure upon further information, discovery, and analysis as the case progresses.

b. Non-Viewable Component References

The Asserted Claims recite functionality for a non-viewable component within an electronic device that is connected to the application component and determines if the application component has been tampered with. *See, e.g.*, '837, cl. 1 (“a non-viewable security component in the electronic device, wherein the non-viewable security component comprises a validator module capable of determining whether the application component is present and whether the application component has been tampered with”); '710, cl. 1 (“(a) a non-viewable component... wherein the non-viewable component is configured to determine whether the application component is present and whether the application component has been tampered with.”); '410, cl. 1 (“wherein the hidden partition comprises a non-viewable component associated with tracking and locating the electronic device ... performing, with the non-viewable component, operations comprising: automatically determining whether the application component operated correctly during last power-up of the electronic device”); '892, cl. 1 (“wherein the system includes a non-viewable component ... wherein the nonviewable component is configured to determine whether the application component is present and whether the application component has been tampered with”); '235, cl. 1 (“a non-viewable component ... wherein the non-viewable component is configured to determine whether the application component is present and whether the application component has been tampered with.”). Use of a non-viewable component was well-known at the time of invention. As the attached claim charts demonstrate, use of a non-viewable component in an electronic device is disclosed in at least: Angelo '729, Cheston, Computrace, Dayan, Hamilton, Miller, Pearson, Stevens, TheftGuard, zTrace.

Persons of ordinary skill in the art would have been motivated to combine the teachings of the Non-Viewable Component references with any system that seeks to improve resilience against unauthorized attempts to remove or tamper with anti-theft security features. The implementation

of a non-viewable component would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try.

For example, references disclose the following motivations to combine:

- A non-viewable component implemented in software allows for “convenience and flexibility,” for the same reasons mentioned above with respect to the application component. Pearson, 1:54-62.
- A non-viewable component is difficult for an end-user to locate and disable, which enhances the security of the device because the non-viewable component will continue to ensure that only trusted programs (i.e., programs that have not been tampered with) are running on the device. *See, e.g.*, Miller, 15:26-37 (“The user cannot inadvertently delete or alter the detection software... [n]or can a virus access the partition.”); Cheston, 2:16-19 (“[T]he hidden partition is preferably inaccessible to the operating system thereby decreasing the probability of code stored therein being corrupted”); Dayan, [0008] (“The designated partition may be invisible to the operating system and resistant to modification by any programs running under the operating system.”); Pearson, 2:46-58 (“The trusted module or component... is preferably immune to unauthorized modification or inspection of internal data”).
- A non-viewable component can be a “trusted module,” which was a well-known type of module for validating the integrity of hardware and software within devices. There were standards and specifications for such trusted modules developed at the time of the Asserted Patents. *See, e.g.*, Cromer ’464, 1:26-39 (“The open alliance,

known as the Trusted Computing Platform Alliance (TCPA), has proposed a standard... so PC manufacturers can provide a more trusted and secure PC platform based on common industry standards, the details of which are provided in the TCPA PC Specific Implementation Specification, Version 1.00 RC1 (Aug. 16, 2001)"); Pearson, 2:46-58 ("Methods of building trusted modules are, per se, well known to those skilled in the art.").

Defendants reserve the right to amend, supplement, and/or modify this disclosure upon further information, discovery, and analysis as the case progresses.

c. Non-Modifiable Memory Area References

The Asserted Claims recite functionality for an area of memory that cannot be modified by a user of an electronic device. *See, e.g.*, '649, cl. 1 ("the non-volatile memory comprises...a system area that cannot be modified by the user"). It was well-known at the time of the invention that there were many ways of protecting portions of memory in a computer from modification by a user. As the attached claim charts demonstrate, use of a non-modifiable area of memory is disclosed in at least: Andrews, Bean, BlackBerry, Bonnett, Cheston, Computrace, Cotichini, Dayan, Flanigan, Hamilton, Hayward, Howard, Isikoff, Markkanen, Miller, Pearson, Solymar, Stevens, TheftGuard, zTrace.

Persons of ordinary skill in the art would have been motivated to combine the teachings of the Non-Modifiable Memory Area references with any system that seeks to improve resilience against unauthorized attempts to remove or tamper with anti-theft security features. The implementation of a non-modifiable memory area would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique

to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. For example, references disclose the following motivations to combine:

- A non-modifiable memory area prevents users from disabling or deleting any programs stored in that area, which can be used to protect critical programs from alteration and improves the reliability and resilience of programs designed for computer security. *See, e.g.*, Bonnett, [0036] (“hidden partition 206b operates to store at least a portion 225b of program 225 that a program designer desires to be made inaccessible to a user of appliance 200.”); Flanigan, 5:8-12 (“The host protected area may be used to store virus scan instructions, instructions to predict a disk drive failure, a portion of a host BIOS start up/reset initialization code, emergency boot instructions, and the like”); Cotichini, 24:10-12 (“Attempts to read or write to the location where the Agent has been installed are deflected in order to prevent discovery of the agent.”); Miller, 15:26-37 (“The user cannot inadvertently delete or alter the detection software... [n]or can a virus access the partition.”); Cheston, 2:16-19 (“[T]he hidden partition is preferably inaccessible to the operating system thereby decreasing the probability of code stored therein being corrupted”); Dayan, [0008] (“The designated partition may be invisible to the operating system and resistant to modification by any programs running under the operating system.”); Pearson, 2:46-58 (“The trusted module or component... is preferably immune to unauthorized modification or inspection of internal data”).

Defendants reserve the right to amend, supplement, and/or modify this disclosure upon further information, discovery, and analysis as the case progresses.

d. BIOS Component References

The Asserted Claims recite functionality for a BIOS component capable of determining whether a non-viewable component, and in some instances, an application component, of an electronic device have been tampered with. *See, e.g.*, '837, cl. 1 (“a basic input/output (BIOS) security component stored in the secure area”); '710, cl. 1 (“(c) a Basic Input/Output System (BIOS) component connected to the non-viewable component, ... wherein the BIOS component is configured to determine whether the non-viewable component is present and whether the non-viewable component has been tampered with”); '410, cl. 15 (“wherein the electronic device comprises a disk drive and a basic input/output system (BIOS) component associated with tracking and locating the electronic device ... performing, with the BIOS component, operations comprising: automatically determining whether the application component operated correctly during last power-up of the electronic device”); '892, cl. 1 (“a Basic Input/Output System (BIOS) component connected to the non-viewable component, wherein the BIOS component is configured to determine whether the non-viewable component is present and whether the non-viewable component has been tampered with”); '603, cl. 1 (“a basic input/output system (BIOS) component”); '235, cl. 1 (“a BIOS component connected to the non-viewable component, wherein the BIOS component is configured to determine whether the non-viewable component is present and whether the non-viewable component has been tampered with.”). BIOS components with such diagnostic capabilities were fundamental to computer systems and had been for decades at the time of the invention. As the attached claim charts demonstrate, use of a BIOS component is disclosed in at least: AMIBIOS, Andrews, Angelo '729, Barrus, Cheston, Cromer '464, Dayan, Flanigan, Hamilton, Howard, Isikoff, Miller, Pearson, PhoenixBIOS, Phoenix FirstWare, Stevens.

Persons of ordinary skill in the art would have been motivated to combine the teachings of the BIOS Component references with any system that seeks to incorporate diagnostics and tamper-

resistant anti-theft technology into an electronic device. The implementation of a BIOS component would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. For example, references disclose the following motivations to combine:

- A BIOS component is a fundamental piece of firmware integrated into devices with operating systems. *See, e.g.*, Barrus, 6:55-67 (“As is known in the art, the Basic Input/Output System (BIOS) is firmware that controls a computer’s bootup sequence.”); Miller, 1:15-26 (“A PC also has lower level software known as the Basic Input/Output System (BIOS) contained in Read Only Memory (ROM) on the system board... The BIOS performs a set of diagnostic routines called Power On Self Test (POST) and if completed successfully, proceeds to locate and boot up the OS.”); Stevens, [0004] (“The BIOS is a firmware program that is typically stored in nonvolatile memory (flash memory), and which brings up (initializes) a computer system when it is powered on.”). It would have therefore been obvious – and possibly even necessarily – to implement a BIOS component within *any* device that includes an operating system. The BIOS component ensures that the operating system, hardware and software within the device are operating properly after the device is powered on.
- A BIOS component is known to perform integrity checks of hardware and software during the device’s boot up sequence to ensure that the hardware and software running on the device is free from viruses and/or tampering. *Id.*; *see also* Miller,

15:26-37 (“[T]he present invention performs all virus detection checks before the computer system is booted for user operations.”). Therefore, a BIOS component already fundamentally performs some of the same (or similar) functions recited in the Asserted Claims.

- As explained in the claim charts for the AMIBIOS and Phoenix FirstWare system references, a person of ordinary skill in the art would have been motivated to integrate computer security/tracking application functionality with BIOS and non-viewable-component functionality described in the claim charts for the AMIBIOS and Phoenix FirstWare in view of Phoenix’s and AMIBIOS’s advances in BIOS and non-viewable component security, extensibility, and customizability. For example, Phoenix’s cME and FirstWare functionality enabled application developers to partner with Phoenix and easily access Phoenix’s pre-defined diagnostics and self-healing capabilities, internet access, and recovery utilities operated from system BIOSs and non-viewable components.

Defendants reserve the right to amend, supplement, and/or modify this disclosure upon further information, discovery, and analysis as the case progresses.

e. Check Integrity References

The asserted claims of the ’837, ’710, ’410, ’892, ’603, and ’235 Patents recite additional functionality for the BIOS component involving checking the integrity / correct operation of the application component during a previous power-up of an electronic device. *See, e.g.*, ’837, cl. 1 (“the BIOS security component configured to check integrity of the application component during a boot process for the electronic device”); ’710, cl. 1 (“wherein the BIOS component is configured to check integrity of the application component during a boot process for the electronic device”);

'410, cl. 1 (“automatically determining whether the application component operated correctly during last power-up of the electronic device”); '892, cl. 1 (“wherein the BIOS component is configured to check integrity of the application component during a boot process for the electronic device”); '603, cl. 1 (“automatically determining whether the application component is operating correctly”); '235, cl. 1 (“wherein the BIOS component is configured to check integrity of the application component during a boot process for the electronic device”). The principle of checking data, files, and components to ensure their correct operation was well-known and had been implemented in computer systems decades before the time of the invention. As the attached claim charts demonstrate, use of an application component within an operating system environment to determine whether an electronic device has been reported stolen based on information received from a server system is disclosed in at least: AMIBIOS, Angelo '729, Assaf, Cheston, Cromer '464, Hamilton, Kesler, Miller, Pearson, PhoenixBIOS, Phoenix FirstWare.

Persons of ordinary skill in the art would have been motivated to combine the teachings of the Check Integrity references with any system that seeks to incorporate diagnostics that permit the system to identify tampering, file corruption, or other vulnerabilities in an electronic device. The implementation of functionality to check the integrity and/or proper operation of components in an electronic device would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. For example, references disclose the following motivations to combine:

- Checking the integrity of hardware, software and other components of a device was already a well-known function of the BIOS component implemented within devices

with operating systems; therefore, it would have been a natural extension of the BIOS component (or any component running during boot up) to check the integrity or operation of a specific applications or programs during bootup to ensure that those applications or programs are free from tampering, corruption or other unintended modifications to their original format. *See* above.

- Integrity checking, in general, was well known in the art at the time of the Asserted Patents. *See, e.g.*, Pearson, 2:46-58 (describing a “trusted module” for performing integrity checks, where “[m]ethods of building trusted modules are, per se, well known to those skilled in the art” and the “crypto methods” used as part of the trusted modules were also “well known to those skilled in the art of security”); Cromer ’464, 1:26-39 (identifying standards and specifications developed at the time of the Asserted Patents for building trusted modules, which perform integrity checks).
- Integrity checking is an important layer in device security because it ensures that the applications and programs running on the device are free from tampering, corruption or other vulnerabilities that could potentially compromise the device and the data contained therein. *See, e.g.*, Miller, 2:21-50 (“While many computer viruses are relatively benign, computer viruses can be hostile, clandestine and created specifically to cause undesirable results on the computer, such as destroy software and data, or cause peculiar computer operation, ...”); Miller, 1:61-2:4 (“Huge amounts of money are invested by companies in purchasing software and even more money is expended on developing the information contained in the electronic data files such as documents, spreadsheets and drawings. Protecting

these resources is therefore an important concern.”); Morriss, [0003] (“[S]uch devices can be quite expensive... such devices may contain confidential or personal information of their users the development of other measures to prevent the loss of a wireless communication device or to secure its recovery in the event of a loss is of great importance in today’s wireless environment.”).

- As explained in the claim charts for the AMIBIOS and Phoenix FirstWare system references, a person of ordinary skill in the art would have been motivated to integrate computer security/tracking application functionality with BIOS and non-viewable-component functionality described in the claim charts for the AMIBIOS and Phoenix FirstWare in view of Phoenix’s and AMIBIOS’s advances in BIOS and non-viewable component security, extensibility, and customizability. For example, Phoenix’s cME and FirstWare functionality enabled application developers to partner with Phoenix and easily access Phoenix’s pre-defined diagnostics and self-healing capabilities, internet access, and recovery utilities operated from system BIOSs and non-viewable components.

Defendants reserve the right to amend, supplement, and/or modify this disclosure upon further information, discovery, and analysis as the case progresses.

f. Restore Integrity References

The asserted claims of the ’837, ’710, ’410, ’892, ’603, and ’235 Patents also recite that the BIOS component will restore the integrity of an application component if the application component returns a negative integrity check. *See, e.g.,* ’837, cl. 1 (“wherein the BIOS security component is configured to automatically cause the electronic device to restore the integrity of the application component, in response to a negative integrity check for the application component”);

'710, cl. 1 (“wherein the BIOS component is configured to automatically cause the electronic device to restore the integrity of the application component, in response to a negative integrity check of the application component”); '410, cl. 1 (“in response to determination that the application component did not operate correctly during last power-up of the electronic device, automatically restoring the application component from a backup fileset”); '892, cl. 1 (“wherein the BIOS component is configured to automatically cause the electronic device to restore the integrity of the application component, in response to a negative integrity check of the application component”); '235, cl. 1 (“wherein the BIOS component is configured to automatically cause the electronic device to restore the integrity of the application component in response to a negative integrity check of the application component”). At the time of the invention, the concept of an application component communicating with an external server to determine whether an electronic device had been reported stolen was well-known. Likewise, the state of the art was already well-developed for application components that enable tracking, tracing, and/or otherwise locating an electronic device. And persons of ordinary skill already knew that these tracking application components could be connected to and in communication with non-viewable components of the electronic device. As the attached claim charts demonstrate, use of an application component within an operating system environment to determine whether an electronic device has been reported stolen based on information received from a server system is disclosed in at least: AMIBIOS, Angelo '978, Assaf, Dayan, Hamilton, Phoenix FirstWare.

Persons of ordinary skill in the art would have been motivated to combine the teachings of the Restore Integrity references with any system that seeks to self-administer corrective actions to address identified vulnerabilities and ensure the correct operation of the system. The implementation of functionality in the BIOS component to restore the integrity of compromised

application components would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. For example, references disclose the following motivations to combine:

- Restoring a resource (such as a program or component) is a “quick[] and eas[y]” process that can be performed with minimal interruptions to the device operation. Angelo ’978, 6:28-49 (describing “functionality to quickly and easily restore the resources on the faulted computer [].”). For example, a program or component can be restored from a backup copy of that program or component stored locally on the device or downloaded from a server providing a security service. *See, e.g.,* Angelo ’978, 6:1-27. In the latter implementation, the server can provide the device with the most up to date version of that program or component so the device has the most up to date protection. *See, e.g.,* Angelo ’978, 1:55-67, 3:38-51.
- Restoring the integrity of a program or component would be an obvious next step after a negative integrity check to maintain the security of the device. If the program or component were allowed to run after a negative integrity check, it could compromise the device and the data stored therein. *See* Miller, 2:21-50 (“While many computer viruses are relatively benign, computer viruses can be hostile, clandestine and created specifically to cause undesirable results on the computer, such as destroy software and data, or cause peculiar computer operation”); Miller, 1:61-2:4 (“Huge amounts of money are invested by companies in purchasing software and even more money is expended on developing the

information contained in the electronic data files such as documents, spreadsheets and drawings. Protecting these resources is therefore an important concern.”); Morriss, [0003] (“[S]uch devices can be quite expensive ... such devices may contain confidential or personal information of their users.... the development of other measures to prevent the loss of a wireless communication device or to secure its recovery in the event of a loss is of great importance in today’s wireless environment”).

- As explained in the claim charts for the AMIBIOS and Phoenix FirstWare system references, a person of ordinary skill in the art would have been motivated to integrate computer security/tracking application functionality with BIOS and non-viewable-component functionality described in the claim charts for the AMIBIOS and Phoenix FirstWare in view of Phoenix’s and AMIBIOS’s advances in BIOS and non-viewable component security, extensibility, and customizability. For example, Phoenix’s cME and FirstWare functionality enabled application developers to partner with Phoenix and easily access Phoenix’s pre-defined diagnostics and self-healing capabilities, internet access, and recovery utilities operated from system BIOSs and non-viewable components.

Defendants reserve the right to amend, supplement, and/or modify this disclosure upon further information, discovery, and analysis as the case progresses.

g. Disable References

The asserted claims of the ’837, ’410, ’603, ’649, and ’235 Patents recite disabling the electronic device when certain conditions are met. *See, e.g.*, ’837, cl. 1 (“wherein the BIOS security component is configured to prevent the electronic device from booting to the OS, in

response to receiving notification that the electronic device has been reported stolen”); ’410, cl. 17 (“automatically disabling the electronic device in response to a determination that the number of device power-ups has been reached”); ’603, cl. 4 (“The method of claim 3, wherein the one or more actions include at least one action from the group consisting of disabling the electronic device and erasing a hard disk drive in the electronic device.”); ’649, cl.1 (“in response to receiving the notification, automatically disabling at least one user function of the mobile electronic device while still allowing the mobile electronic device to communicate with the security service”); ’235, cl. 6 (“The method of claim 1, wherein the BIOS component is configured to prevent the electronic device from booting to an operating system of the electronic device, in response to receiving notification that the electronic device has been reported stolen.”). At the time of the invention, the concept of disabling an electronic device after it has been reported stolen, or a certain number of unauthorized access attempts, was well-known. As the attached claim charts demonstrate, this disabling functionality is disclosed in at least: Andrews, Angelo Publication, Barrus, Bean, BlackBerry, Britt, Choi, Computrace, CyberAngel, Dailey, Hamilton, Hariprasad, Hayward, Helle, Henrie, Howard, Isikoff, Kesler, Levi, Markkanen, Morriss, TheftGuard, Windows, zTrace.⁶

Persons of ordinary skill in the art would have been motivated to combine the teachings of the Disable references with any system that seeks to prevent unauthorized use of a stolen electronic device. The implementation of disabling functionality in an electronic device would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application

⁶ Andrews, Bean, BlackBerry, Hayward, Helle, Howard, Markkanen, and Windows are charted against the ’649 Patent only but their respective disable disclosures would apply equally to parallel disclosures in the asserted claims of the remaining Asserted Claims.

of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. For example, references disclose the following motivations to combine:

- The ability to remotely disable a portable device was a well-known way of protecting sensitive data at the time of the Asserted Patents. *See* Morriss, [0004] (“Various wireless device loss detection and response approaches presently exist. Such approaches focus primarily on remotely programming the lost device over-the-air (OTA) to (i) prohibit the device from performing certain operations”); Choi, [0039] ([F]unction for disabling of operation can be controlled remotely to make the use of data within the lost or stolen information system impossible... Such remote control of the lost or stolen information system can protect the information stored therein and prevent illegal use of the information.”); Britt, 1:22-39 (“[D]isabling a lost or stolen data processing device to thereby prevent unauthorized access to sensitive information stored thereon”). It was also a quick and temporary solution (as opposed to the permanency of erasing data or device destruction) that allowed owners to reactivate and continue use of the device after recovery. *See, e.g.*, Britt, 5:36-6:23 (describing deactivating “in software” such as the “operating system-level” and reactivating “using a particular password”).
- The ability to remotely disable a portable device can be achieved using the “basic communications hardware” within the device and therefore is a relatively cost-effective way to “protect the integrity of the data contained on the machine ...”

Isikoff, 2:60-3:4. In one exemplary reference, a simple command is sent to and executed by the device to disable certain functions. *See* Barrus, 5:31-34, 5:44-59.

- Disabling certain functions while still allowing communications to commence increases the likelihood that the device will be returned to the rightful owner and data will be recovered. *See, e.g.*, Morriss, [0011] (describing placing the device in a “restrictive operating mode” which “increases the chances of the device owner or his or her wireless service provider being contacted in the event that the wireless device is lost or stolen”), [0066] (same).

Defendants reserve the right to amend, supplement, and/or modify this disclosure upon further information, discovery, and analysis as the case progresses.

h. Boot Prevention References

As a specific example of disabling an electronic device, the asserted claims of the '837, '603, and '235 Patents recite BIOS functionality to prevent an electronic device from booting when certain conditions are met. *See, e.g.*, '837, cl. 1 (“wherein the BIOS security component is configured to prevent the electronic device from booting to the OS, in response to receiving notification that the electronic device has been reported stolen”); '603, cl. 1 (“during a subsequent boot process for the electronic device, automatically preventing the electronic device from completing the boot process if the BIOS component does not find the information from the application component indicating that the application component was operating correctly.”); '235, cl. 6 (“The method of claim 1, wherein the BIOS component is configured to prevent the electronic device from booting to an operating system of the electronic device, in response to receiving notification that the electronic device has been reported stolen.”). Computer systems at the time of the invention had long used BIOS functionality to prevent booting to an operating

system when either a device was reported stolen or an application failed an integrity check. As the attached claim charts demonstrate, this additional functionality in a BIOS component is disclosed in at least: AMIBIOS, Barrus, Britt, Choi, Cromer '464, Hamilton, Isikoff, Phoenix FirstWare.

Persons of ordinary skill in the art would have been motivated to combine the teachings of the Boot Prevention references with any system that seeks to prevent unauthorized use of a stolen electronic device. The implementation of BIOS functionality that prevents booting to an operating system after a reported theft of the electronic device, or a failed integrity check for an application, would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. For example, references disclose the following motivations to combine:

- Preventing a portable device from booting was a well-known way of protecting sensitive data at the time of the Asserted Patents. Barrus, 6:12-44 (“The locked computer is [] useless to the thief.”). A disabled device could be prevented from booting, therefore, the same analysis provided in the previous section applies here. *See, e.g.,* Morriss, [0004] (“Various wireless device loss detection and response approaches presently exist. Such approaches focus primarily on remotely programming the lost device over-the-air (OTA) to (i) prohibit the device from performing certain operations”); Choi, [0039] ([F]unction for disabling of operation can be controlled remotely to make use of data within the lost or stolen information system impossible... Such remote control of the lost or stolen

information system can protect the information stored therein and prevent illegal use of the information.”); Britt, 1:22-39 (“[D]isabling a lost or stolen data processing device to thereby prevent unauthorized access to sensitive information stored thereon.”). Likewise, this was also a quick and temporary solution (as opposed to the permanency of erasing data or device destruction) that allowed owners to reactivate and continue use of the device after recovery. *See, e.g.*, Britt, 5:36-6:23 (describing deactivating “in software” such as the “operating system-level” and reactivating “using a particular password”), 6:12-44 (describing “reactivation” of a locked computer disabled during the boot process).

- As explained in the claim charts for the AMIBIOS and Phoenix FirstWare system references, a person of ordinary skill in the art would have been motivated to integrate computer security/tracking application functionality with BIOS and non-viewable-component functionality described in the claim charts for the AMIBIOS and Phoenix FirstWare in view of Phoenix’s and AMIBIOS’s advances in BIOS and non-viewable component security, extensibility, and customizability. For example, Phoenix’s cME and FirstWare functionality enabled application developers to partner with Phoenix and easily access Phoenix’s pre-defined diagnostics and self-healing capabilities, internet access, and recovery utilities operated from system BIOSs and non-viewable components.

Defendants reserve the right to amend, supplement, and/or modify this disclosure upon further information, discovery, and analysis as the case progresses.

i. Data Destruction References

The asserted claims of the '710, '603, and '649 Patents recite functionality for erasing user data from an electronic device after a report has been received that the electronic device has been stolen. *See, e.g.*, '710, cl. 1 (“after receiving the report that the electronic device has been stolen, causing the electronic device to erase the non-volatile storage device”); '603, cl. 4 (“The method of claim 3, wherein the one or more actions include at least one action from the group consisting of disabling the electronic device and erasing a hard disk drive in the electronic device.”); '649, cl. 7 (“A mobile electronic device according to claim 1, wherein the operations the security application is operable to perform further comprise: after the at least some user data has been copied from the mobile electronic device to at least one of the servers, causing at least some of the user data to be deleted from the mobile electronic device.”). At the time of the invention, the concept of erasing user data on an electronic device in response to a reported theft of an electronic device was well-known and understood. As the attached claim charts demonstrate, data destruction on an electronic device after receiving a report it was stolen is disclosed in at least: Andrews, Barrus, BlackBerry, Britt, Choi, Computrace, Geluc, Isikoff, Hayward, Markkanen, TheftGuard, Windows, zTrace.⁷

Persons of ordinary skill in the art would have been motivated to combine the teachings of the Data Destruction references with any system that seeks to incorporate electronic device theft-prevention techniques and safeguard sensitive information on a user’s electronic device. The implementation of this data destruction functionality would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique

⁷ Andrews, BlackBerry, Hayward, Markkanen, and Windows are charted against the '649 Patent only but their respective data destruction disclosures would apply equally to parallel disclosures in the asserted claims of the '710 and '603 Patents.

to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. For example, references disclose the following motivations to combine:

- Erasing data from a device was a well-known way of protecting sensitive data at the time of the Asserted Patents. *See* Pearson, 15:47-60 (“Techniques relevant to tamper-resistance are well known to those skilled in the art of security. These techniques include... methods for eliminating data when tampering is detected.”); Choi, [0039] (“[F]unction for deleting particular data.. make[s] the use of data within the lost or stolen information system impossible... Such remote control of the lost or stolen information system can protect the information stored therein and prevent illegal use of the information.”)
- The ability to remotely destroy data on a portable device can be achieved using the “basic communications hardware” within the device and therefore is a relatively cost-effective way to “protect the integrity of the data contained on the machine ...” Isikoff, 2:60-3:4. In one exemplary reference, a simple command is sent to and executed by the device to destroy data. *See* Barrus, 5:31-34, 5:44-59.

Defendants reserve the right to amend, supplement, and/or modify this disclosure upon further information, discovery, and analysis as the case progresses.

j. Data Copying References

The asserted claims of the ’603 and ’649 Patents recite functionality for copying user data from an electronic device reported stolen to another server. *See, e.g.*, ’603, cl. 3 (“if the response indicates that the electronic device is reported stolen, automatically performing one or more actions, based on user selected service options for protecting the electronic device from unauthorized utilization.”); ’649, cl. 1 (“automatically causing at least some user data to be copied

from the mobile electronic device to at least one of the servers”). At the time of the invention, the concept of copying user data from a compromised electronic device to another server was well-known. As the attached claim charts demonstrate, data copying from an electronic device to a server is disclosed in at least: Andrews, BlackBerry, Choi, Computrace, Cotichini, Isikoff, Hayward, Helle, Howard, Markkanen, Solymar, TheftGuard, Windows, zTrace.⁸

Persons of ordinary skill in the art would have been motivated to combine the teachings of the Data Copying references with any system that seeks to preserve sensitive user data as a theft countermeasure when an electronic device is reported stolen. The implementation data copying from a compromised electronic device to another server would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. For example, references disclose the following motivations to combine:

- Backing up data in general was a well-known concept at the time of the Asserted Patents. *See, e.g.*, Isikoff, 7:46-67 (describing backing up data in “non-emergency situations” such as “back up all word processing documents every three days automatically”).
- Backing up data is a quick and cost-effective way to recover data in the event the device is lost or stolen. *See* Isikoff, 2:56-3:4 (“The transceiver... is also configured as described further below for data recovery... in which case it operates to... transmit important data to the rightful owner... This operation substantially

⁸ Andrews, BlackBerry, Hayward, Helle, Howard, Markkanen, and Windows are charted against the ’649 Patent only but their respective data copying disclosures would apply equally to parallel disclosures in the asserted claims of the ’603 Patent.

enhances value, yet is achieved at little additional premium over the cost of the basic communications hardware.”).

- Backing up data is also an obvious step before attempting to erase data on a device that is lost or stolen, as it preserves data that will otherwise be permanently erased from the device. *See, e.g.*, Britt, 6:11-23 (“Prior to erasing the data, the service may perform a backup to preserve the user data on the service 100.”).

Defendants reserve the right to amend, supplement, and/or modify this disclosure upon further information, discovery, and analysis as the case progresses.

k. Hardware References

The Asserted Claims recite general computer hardware components—*e.g.*, processors, non-volatile memory, storage media, expansion buses—that are used to execute the well-known security and tracking functionality described in the claims. *See, e.g.*, ’837, cl. 20 (“a central processing unit; a memory array coupled to said central processing unit; an expansion bus coupled to said central processing unit and said memory array, said expansion bus capable of interfacing peripheral devices; a basic input/output system (BIOS) memory ... a hard disk drive coupled to said expansion bus”); ’710, cl. 19 (“a non-transitory machine accessible storage medium ... a non-volatile storage device”); ’410, cl. 8 (“a non-transitory machine-readable storage medium; ... wherein the electronic device comprises a disk drive”); ’892, cl. 11 (“an electronic device comprising hardware and software components”); ’603, cl. 18 (“a processing unit; a non-transitory machine-readable medium responsive to the processing unit”); ’649, cl. 1 (“a processor; one or more non-transitory machine-readable storage media responsive to the processor”); ’235, cl. 15 (“a memory, and a processor”). Use of general computer hardware components in security and tracking systems was ubiquitous at the time of the invention, if not

fundamental to *any* computer system seeking to provide this functionality. As the attached claim charts demonstrate, use of hardware components in security and tracking systems for electronic devices is disclosed in at least: AlertPC, Andrews, Angelo '729, Angelo Publication, Barrus, Bean, BlackBerry, Bonnett, Choi, Computrace, Cotichini, CyberAngel, Dailey, Dayan, Flanigan, Hamilton, Hayward, Helle, Henrie, Howard, Isikoff, Levi, Markkanen, Miller, Morriss, Pearson, PC PhoneHome, Solymar, Stevens, TheftGuard, zTrace.⁹

The use of hardware in security, monitoring, and tracking systems for electronic devices would have been obvious to a person of ordinary skill in the art at least because doing so would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. Moreover, a person of ordinary skill in the art would have readily appreciated the well-known, widespread, and necessary use of general hardware in computer systems, and the associated benefits and advantages of its use. Persons of ordinary skill in the art would have been motivated to combine the teachings of the Hardware references with any computer system or electronic device, including security, tracking, and/or monitoring systems for electronic devices.

Defendants reserve the right to amend, supplement, and/or modify this disclosure upon further information, discovery, and analysis as the case progresses.

I. Server References

⁹ Dailey and Levi are charted against the '603 and '649 Patents only but their respective hardware disclosures would apply equally to parallel disclosures in the remaining Asserted Claims. Similarly, Andrews, Bean, BlackBerry, Bonnett, Flanigan, Hayward, Helle, Howard, and Markkanen are charted against the '649 Patent only but their respective hardware disclosures would apply equally to parallel disclosures in the remaining Asserted Claims.

The asserted claims of the '837, '710, '892, '603, '649, and '235 Patents recite a server system of a security service that may include functionality to record electronic device theft reports, receive identifying information from an electronic device, notify an electronic device whether it has been reported stolen, and send remote commands to the electronic device to perform various actions (*e.g.*, disable, copy data, erase data). *See, e.g.*, '837, cl. 1 (“an electronic device operable to support an operating system (OS) environment and operable to communicate with a server system”); '710, cl. 1 (“(d) a server system capable of communicating through a secure medium with the application component”); '892, cl. 1 (“an application component ... that is capable of communicating through a secure medium with a server system”); '603, cl. 1 (“wherein the application component is configured to automatically ascertain whether the electronic device has been reported stolen, based on information received from a server system”); '649, cl.1 (“enabling an owner of the mobile electronic device to register the mobile electronic device with a security service residing at least partially on one or more servers”); '235, cl. 4 (“The method of claim 1, wherein the electronic device is operable to support the operating system environment and operable to communicate with a server system.”). At the time of the invention, servers were in ubiquitous use for security services in electronic device monitoring, security, and/or tracking systems. As the attached claim charts demonstrate, use of a server system in an electronic device security and tracking system is disclosed in at least: AlertPC, Andrews, BlackBerry, Britt, Choi, Computrace, Cotichini, CyberAngel, Dailey, Hamilton, Hayward, Helle, Henrie, Howard, Kesler, Levi, Markkanen, Morriss, PC PhoneHome, Solymar, TheftGuard, Windows, zTrace.¹⁰

The implementation of servers to render these security services would have involved the combination of prior art elements according to known methods to yield predictable results, the

¹⁰ Dailey, Kesler, and Levi are charted against the '603 and '649 Patents only but their respective server disclosures would apply equally to parallel disclosures in the remaining Asserted Claims.

simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. Persons of ordinary skill in the art would have been motivated to combine the teachings of the Server references with any system that seeks to implement electronic device security and tracking, and to integrate remote anti-theft countermeasures after the electronic device is reported stolen.

Defendants reserve the right to amend, supplement, and/or modify this disclosure upon further information, discovery, and analysis as the case progresses.

m. Startup File References

Claims 5 and 25 of the '837 Patent recite that the application component is comprised of startup files, an application file, and a dynamic link library (DLL) that are interconnected. *See* '837, cls. 5, 25. The recited composition of the claimed application component was commonplace at the time of invention. As the attached claim charts demonstrate, application components comprising interconnected startup files, an application file, and a DLL is disclosed in at least: Computrace, Solymar, Tait, TheftGuard, zTrace.

The implementation of an application component with interconnected startup files, an application file, and a DLL in security, monitoring, and tracking systems for electronic devices would have been obvious to a person of ordinary skill in the art at least because doing so would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield

Similarly, Andrews, BlackBerry, Hayward, Helle, Howard, Markkanen, and Windows are charted against the '649 Patent only but their respective server disclosures would apply equally to parallel disclosures in the remaining Asserted Claims.

predictable results, and/or would have been obvious to try. Moreover, a person of ordinary skill in the art would have readily appreciated the well-known and widespread use of application components with interconnected startup files, an application file, and a DLL, and the associated benefits and advantages of their use. Persons of ordinary skill in the art would have been motivated to combine the teachings of the Startup File references with any computer system or electronic device that implements applications, including security, tracking, and/or monitoring systems for electronic devices.

Defendants reserve the right to amend, supplement, and/or modify this disclosure upon further information, discovery, and analysis as the case progresses.

n. PowerUp References

Claim 17 of the '410 Patent recites functionality related to corrective actions (*e.g.*, user authentication, disabling) taken when an electronic device has reached a number of power-ups, after determining that an application component was not operating correctly. *See, e.g.*, '410, cl. 17. Corrective actions, such as user password authentication and device disabling, in response to multiple device powerups were well-known security features in electronic devices at the time of invention. As the attached claim charts demonstrate, use of corrective actions in response to number of device power-ups is disclosed in at least: AMIBIOS, Brammick, Britt, McLaughlin, Phoenix FirstWare, Watson.

Persons of ordinary skill in the art would have been motivated to combine the teachings of the PowerUp references with any system that seeks to provide additional layers of security to prevent unauthorized user access to an electronic device. The implementation of corrective actions related to the number of device powerups after a negative integrity check for an application would have involved the combination of prior art elements according to known methods to yield

predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. For example, references disclose the following motivations to combine:

- As explained in the claim charts for the AMIBIOS and Phoenix FirstWare system references, a person of ordinary skill in the art would have been motivated to integrate computer security/tracking application functionality with BIOS and non-viewable-component functionality described in the claim charts for the AMIBIOS and Phoenix FirstWare in view of Phoenix's and AMIBIOS's advances in BIOS and non-viewable component security, extensibility, and customizability. For example, Phoenix's cME and FirstWare functionality enabled application developers to partner with Phoenix and easily access Phoenix's pre-defined diagnostics and self-healing capabilities, internet access, and recovery utilities operated from system BIOSs and non-viewable components.

Defendants reserve the right to amend, supplement, and/or modify this disclosure upon further information, discovery, and analysis as the case progresses.

o. Tracking References

The asserted claims of the '837 and '603 Patents recite functionality related to tracking an electronic device. *See, e.g.*, '837, cl. 10 ("The electronic device security and tracking system of claim 1, wherein the non-viewable security component, the application component, the BIOS security component, and the server system are operably arranged to provide for locating and disabling the electronic device"); '603, cl. 3 ("if the response indicates that the electronic device is reported stolen, automatically performing one or more actions, based on user selected

service options for protecting the electronic device from unauthorized utilization.”). At the time of the invention, the electronic device tracking was well-known and ubiquitous within security technologies—indeed, GPS tracking for vehicles and other objects had been commercially available since at least the 1980s. As the attached claim charts demonstrate, electronic device tracking is disclosed in at least: AlertPC, Angelo Publication, Barrus, Choi, Computrace, Cotichini, CyberAngel, Hamilton, Henrie, Isikoff, Kesler, Levi, Morriss, PC PhoneHome, Solymar, TheftGuard, zTrace.¹¹

Persons of ordinary skill in the art would have been motivated to combine the teachings of the Tracking References with any system that seeks to incorporate tracking technology into electronic device theft-prevention systems. The implementation of electronic device tracking would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. For example, references disclose the following motivations to combine:

- Many mobile device at the time of the Asserted Patents included global position system (GPS) capabilities; therefore, it would have been obvious to harness the already on-board GPS capabilities of the device to determine the location of the device for recovery purposes. *See, e.g.,* Geluc, [0157] (“[GPS] can be activated to

¹¹ Kesler and Levi are charted against the ’603 Patent but their respective server disclosures would apply equally to parallel disclosures in the ’837 Patent.

enable the tracking of it by transmitting coordinates describing the systems position. A typical example is a mobile phone or a vehicle with a GPS.”).

- Because the need “to secure [the device’s] recovery in the event of a loss is of great importance in today’s wireless environment,” it would have been obvious to implement technology within the device that allowed the device to be located or tracked so recovery is possible. Morriss, [0003]; *see also, id.*, [0059] (disclosing that the location of the device can be provided to “the wireless service provider, device owner and/or law enforcement authorities [to assist] in locating the device.”); Isikoff, 2:60-3:40 (“tracking of the computer after a theft... expedite[s] return of the stolen computer... assist[s] in the capture of the thief[] and [] serve[s] as a deterrent against theft.”).

Defendants reserve the right to amend, supplement, and/or modify this disclosure upon further information, discovery, and analysis as the case progresses.

p. Encrypted Messaging References

The asserted claims of the ’837 and ’603 Patents recite functionality encrypting communications between components in a security and tracking system for electronic devices. *See, e.g.*, ’837, cl. 2 (“the server system is capable of communicating through a secure medium with the non-viewable security component”); ’603, cl. 2 (“in response to successfully contacting the primary server, automatically sending an encrypted message to the primary server, wherein the encrypted message includes data to identify the electronic device”). Electronic communications encryption was a well-established and ubiquitous security practice in computer technology at the time of invention. As the attached claim charts demonstrate, use of encrypted

messaging between an electronic device and a server is disclosed in at least: Choi, Computrace, Cotichini, Kesler, Levi, Pearson, Solymar, TheftGuard, zTrace.¹²

Persons of ordinary skill in the art would have been motivated to combine the teachings of the Encrypted Messaging references with any system that seeks to ensure secure communication between components, including in a security, tracking, and/or monitoring system for electronic devices. The implementation of encrypted messaging between components was ubiquitous technology at the time of invention, and in the implementation described in the Asserted Claims would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. For example, references disclose the following motivations to combine:

- The use of cryptographic methods “to provide authenticity, integrity, [and] confidentiality” was well known in the art at the time of the Asserted Patents. Pearson, 2:46-58. Encryption is one type of cryptograph. It would have been obvious to use this well-known technique to provide secure communications between the device and server as well as to provide a straight-forward way of authenticating any messages transmitted from the device so that an authorized user can be identified quickly and efficiently.

Defendants reserve the right to amend, supplement, and/or modify this disclosure upon further information, discovery, and analysis as the case progresses.

q. Interval Messaging References

¹² Kesler and Levi are charted against the '603 Patent but their respective server disclosures would apply equally to parallel disclosures in the '837 Patent.

The asserted claims of the '603 and '649 Patents recite functionality where an electronic device automatically and periodically sends messages to a server at certain intervals. *See, e.g.*, '603, cl. 3 (“if the response indicates that the electronic device is not reported stolen, automatically waiting a random interval and then sending another encrypted message to the primary server in response to the response indicating that the electronic device is not reported stolen”), '649, cl. 1 (“after the owner has registered the mobile electronic device with the security service, causing the mobile electronic device to periodically communicate with the security service”). At the time of the invention, it was well-known that electronic device can message, notify, or “ping” an external server for various purposes, including tracking, device health, security status, and other reasons. As the attached claim charts demonstrate, this periodic communication with a server from an electronic device is disclosed in at least: AlertPC, Andrews, BlackBerry, Choi, Computrace, Cotichini, CyberAngel, Dailey, Hayward, Helle, Henrie, Howard, Isikoff, Kesler, Levi, Markkanen, Solymar, TheftGuard, Windows, zTrace.¹³

Persons of ordinary skill in the art would have been motivated to combine the teachings of the Interval Messaging references with any system that seeks to incorporate electronic device theft-prevention techniques and/or device tracking technology. The implementation of periodic communication between an electronic device and a server would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or

¹³ Andrews, BlackBerry, Hayward, Helle, Howard, Markkanen, and Windows are charted against the '649 Patent only but their respective interval messaging disclosures would apply equally to parallel disclosures in the asserted claims of the '603 Patent.

would have been obvious to try. For example, references disclose the following motivations to combine:

- Interval messaging would be an obvious safety feature in an automated system/service that could be used to determine if a device is stolen or tampered with. For example, if a messaging interval is missed, this could indicate that something is wrong with the device and certain steps need to be taken to protect the device and the data thereon without any human interaction required. *See, e.g.,* Cotichini, 17:16-36 (“If the system time has been backdated, a modal change from active to alert will occur. This feature safeguards against a thief disabling the agent by backdating the client so that the agent does not call the host for a long period of time.”).

Defendants reserve the right to amend, supplement, and/or modify this disclosure upon further information, discovery, and analysis as the case progresses.

r. Activation References

The asserted claims of the ’892 Patent recite functionality that provides a user with an interface to request activation of a security service. *See, e.g.,* ’892, cl. 1 (“providing to a user of an electronic device, a user interface which allows the user to request activation of a security service for the electronic device, the security service to provide security and tracking for the electronic device”). At the time of invention, the concept that a user would activate a security service through opting in via a user interface was well-established, commonplace, and generally practiced within the device security industry. As the attached claim charts demonstrate, opt-in

activation of a security service via a user interface was disclosed in at least: Britt, Choi, Cotichini, Henrie, Morriss, zTrace, TheftGuard, Computrace, AlertPC, CyberAngel, PC PhoneHome.

Persons of ordinary skill in the art would have been motivated to combine the teachings of the Activation references with any system that seeks to provide electronic device tracking, security, and/or monitoring technology. The implementation of opt-in activation of a security service via a user interface would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. Exemplary motivations to combine for the Activation references parallel those of the Registration references.

Defendants reserve the right to amend, supplement, and/or modify this disclosure upon further information, discovery, and analysis as the case progresses.

s. Registration References

Similar to the Activation references, the asserted claims of the '649 Patent recite registering a mobile electronic device with a security service residing on a server that provides various security-related features, *e.g.*, device monitoring, tracking, remote control. *See, e.g.*, '649, cl. 1 (“enabling an owner of the mobile electronic device to register the mobile electronic device with a security service residing at least partially on one or more servers”). Mobile electronic device registration for security services residing on a server was well-established in the art at the time of the invention. As the attached claim charts demonstrate, use of an application component within an operating system environment to determine whether an electronic device has been reported stolen based on information received from a server system is disclosed in at least: Andrews, AlertPC, Bean, BlackBerry, Britt, Choi, Computrace, CyberAngel, Dailey, Hamilton, Hayward,

Helle, Henrie, Howard, Kesler, Levi, Markkanen, Morriss, Pearson, PC PhoneHome, TheftGuard, Windows, zTrace.

Persons of ordinary skill in the art would have been motivated to combine the teachings of the Registration References with any system that seeks to incorporate electronic device theft-prevention techniques and/or device tracking technology. The implementation of mobile device registration with a security service on a server would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. For example, references disclose the following motivations to combine:

- Registration is a logical first step in acquiring any service for a device. Registration is a means for collecting information about the device and its user so that the company providing the service has all the information necessary to perform the service. For example, user and device information can be used to authenticate the user/device during messaging/transmissions. *See* Choi, [0037] (“For registration, a user inputs personal information... the owner of the information system can be confirmed through verification of the inputted information.”); Levi, 5:58-6:25 (“The sign-up process is initiated and performed by a user 45 in order to contract for monitoring service from a remote device monitoring system 10.”)

Defendants reserve the right to amend, supplement, and/or modify this disclosure upon further information, discovery, and analysis as the case progresses.

t. Automatic Detection / Contact References

The asserted claims of the '603 Patent recite an electronic device automatically detecting an Internet connection and attempting to contact a server. *See, e.g.*, '603, cl. 2 (“automatically detecting an Internet connection on the electronic device; automatically attempting to contact a primary server from the electronic device”). This automatic detection and contact technology was well-known at the time of invention. As the attached claim charts demonstrate, automatic detection of an Internet connection, and attempting to contact a server, is disclosed in at least: AlertPC, Choi, Computrace, Cotichini, CyberAngel, Dailey, Kesler, Morriss, PC PhoneHome, Solymar, TheftGuard, zTrace.

Persons of ordinary skill in the art would have been motivated to combine the teachings of the Automatic Detection / Contact references with any system that seeks to clandestinely establish contact with an outside server without user intervention, *e.g.*, in an electronic device security and tracking system. The implementation of functionality in an electronic device to automatically detect an Internet connection and then attempt contact with a server would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. For example, references disclose the following motivations to combine:

- Automatic detection / contact would have been an obvious safety feature in an automated system because it would allow the security system to communicate with a server in the background without alerting an unauthorized user. *See, e.g.*, Solymar (such a “feature enables the security system to initiate a call to the host monitoring system even when the client is simultaneously running a different Internet

application,” unlike previous systems which would cause “interference” and “could alert the user to the presence of the security system.”) In other words, this automated functionality enables the security system to remain undetected by an unauthorized user. *See, e.g.*, Dailey, 5:31-45 (referring to its security system that automatically “check[s]-in” with the service server as “stealth”).

- Such automatic detection / contact would have been straight-forward to implement as it would have only required a mere modification to code.

Defendants reserve the right to amend, supplement, and/or modify this disclosure upon further information, discovery, and analysis as the case progresses.

u. Automatic Identification References

The asserted claims of the '710, '603, and '647 Patents recite functionality where an electronic device automatically sends identifying information to a server associated with a security service after establishing a connection with the server. *See, e.g.*, '710, cl. 4 (“The method of claim 1, further comprising: sending an electronic mail containing location identification information of the electronic device.”); '603, cl. 2 (“in response to successfully contacting the primary server, automatically sending an encrypted message to the primary server, wherein the encrypted message includes data to identify the electronic device”); '649, cl. 1 (“causing the mobile electronic device to automatically send identifying information for the mobile electronic device to the security service”). At the time of the invention, persons of ordinary skill already knew that electronic devices could automatically send identifying information to servers after establishing an Internet connection with the server. As the attached claim charts demonstrate, automatic transmission of identifying information from an electronic device to a server is disclosed in at least: Andrews, AlertPC, BlackBerry, Choi, Cotichini, Computrace, CyberAngel, Dailey, Isikoff, Hayward, Helle,

Henrie, Howard, Kesler, Levi, Markkanen, Morriss, PC PhoneHome, Solymar, TheftGuard, Windows, zTrace.¹⁴

Persons of ordinary skill in the art would have been motivated to combine the teachings of the Automatic Identification references with any system that seeks to incorporate electronic device theft-prevention techniques and/or device tracking technology. Automatic transmission of identifying information from an electronic device to a server would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. For example, a person of ordinary skill would have been motivated to combine for at least the following reasons:

- Automatic Identification would have been an obvious safety feature in an automated system for the same reasons discussed above for Automatic Detection / Contact. After contact is established, it would allow the security system to verify or authenticate itself to the server as a background process without alerting an unauthorized user. *See, e.g.,* Solymar (such a “feature enables the security system to initiate a call to the host monitoring system even when the client is simultaneously running a different Internet application,” unlike previous systems which would cause “interference” and “could alert the user to the presence of the security system.”) In other words, this automated functionality enables the security

¹⁴ Dailey, Isikoff, Kesler, and Levi are charted against the '603 and '649 Patents but their respective automatic identification disclosures would apply equally to claims 4, 8, and 21 of the '710 Patent. Similarly, Andrews, BlackBerry, Hayward, Helle, Howard, Markkanen, and Windows are charted against the '649 Patent only but their respective automatic identification disclosures would apply equally to parallel disclosures in the asserted claims of the '603 and '710 Patents.

system to remain undetected by an unauthorized user. *See, e.g.,* Dailey, 5:31-45 (referring to its security system that automatically “check[s]-in” with the service server as “stealth”).

- Such automatic detection / contact would have been straight-forward to implement as it would have only required a mere modification to code.

Defendants reserve the right to amend, supplement, and/or modify this disclosure upon further information, discovery, and analysis as the case progresses.

v. BIOS Modification References

The asserted claims of the '235 Patent recite functionality related to modifying the BIOS of an electronic device. *See, e.g.,* '235, cl. 1 (“opening a BIOS modification application; opening a target BIOS binary image of the electronic device within the BIOS modification application; and adding an electronic security and tracking system and method (ESTSM) ROM image to the target BIOS binary image”). At the time of the invention, BIOS modification applications that permitted adding ROM images (including for electronic security and tracking) to an existing BIOS image were known and even implemented in commercial systems from major BIOS developers, *e.g.,* Phoenix Technologies. As the attached claim charts demonstrate, the claimed functionality of a BIOS modification application is disclosed in at least: AMIBIOS, Gharda, Phoenix FirstWare, Stevens.

Persons of ordinary skill in the art would have been motivated to combine the teachings of the BIOS Modification references with any system that seeks to incorporate theft-prevention security measures into the low-level code and/or firmware of an electronic device to minimize the tampering risks from unauthorized users. The implementation of a BIOS modification application capable of adding electronic security and tracking-related ROM images to an existing target BIOS

image would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. For example, references disclose the following motivations to combine:

- “Flashing” was a well-known technique for updating a BIOS program on a BIOS ROM. *See* Gharda, 1:46-55 (“BIOS is not provided in high-end PCs in these Flash ROM chips, providing new advantages, such as an ability to address system bugs in the field. BIOS can hence be ‘re-flashed’ in the field to provide a new version...”). A backend application would be an obvious choice for creating the “updated” BIOS program that is to be “flashed” to the BIOS ROM. *See* Gharda, 2:25-35 (“[W]hat is provided by the present invention is a BIOS system that allows third parties to add to and to customize a BIOS ROM (BIOS extensions) without having to deal with all of the detailed characteristics of the chip and code stored on the chip. In such a system, OEMs, for example, may quickly, easily, and inexpensively... add BIOS plug-ins for other functions that may provide added value if performed during pre-boot operations and the like.”).
- As explained in the claim charts for the AMIBIOS and Phoenix FirstWare system references, a person of ordinary skill in the art would have been motivated to integrate computer security/tracking application functionality with BIOS and non-viewable-component functionality described in the claim charts for the AMIBIOS and Phoenix FirstWare in view of Phoenix’s and AMIBIOS’s advances in BIOS and non-viewable component security, extensibility, and customizability. For

example, Phoenix's cME and FirstWare functionality enabled application developers to partner with Phoenix and easily access Phoenix's pre-defined diagnostics and self-healing capabilities, internet access, and recovery utilities operated from system BIOSs and non-viewable components.

Defendants reserve the right to amend, supplement, and/or modify this disclosure upon further information, discovery, and analysis as the case progresses.

w. Option ROM References

The asserted claims of the '235 Patent recite additional functionality within the BIOS modification application, where option ROM (*e.g.*, BIOS extension files) nodes within the BIOS modification application can be expanded and a determination be made as to whether any option ROM images are present under the expanded node or there is space to include one. *See, e.g.*, '235, cl. 2 ("expanding an option ROM node within the BIOS modification application; and determining if an option ROM image is present under the option ROM node and if there is space in the target BIOS binary image for an ESTSM ROM image,"), cl. 3 ("determining if there are no option ROM images present under the option ROM node.")). At the time of the invention, the state of the art was already well-developed for BIOS modification applications that included this additional functionality to determine whether an option ROM image existed or could be added to a target BIOS image. As the attached claim charts demonstrate, use of a BIOS modification application with this added functionality is disclosed in at least: AMIBIOS , Cheston, Gharda, Miller, Phoenix BIOS, Phoenix FirstWare, Stevens.

Persons of ordinary skill in the art would have been motivated to combine the teachings of the Option ROM references with any system that seeks to improve the functionality and user friendliness of an existing BIOS modification application, including to easily assess whether a

target BIOS image has or can accommodate additional option ROM images. The implementation of this additional functionality in the BIOS modification application would have involved the combination of prior art elements according to known methods to yield predictable results, the simple substitution of one known element for another to obtain predictable results, the application of a known technique to a known device ready for improvement to yield predictable results, and/or would have been obvious to try. For example, references disclose the following motivations to combine:

- Option ROMs were well known components within computing devices at the time of the Asserted Patents, as evidenced by the charts for Cheston, Gharda, Miller, Phoenix BIOS, Stevens. Option ROMs were known to include BIOS extensions that could be implemented as part of a BIOS boot process. *See, e.g.*, Cheston, 3:42-64 (describing an “Option ROM, physically located on [an] adapter, that contains the adapter’s BIOS extension code”); Gharda, 2:25-35 (describing a “BIOS system that allows third parties to add to and to customize a BIOS ROM (BIOS extensions)”).
- As explained in the claim charts for the AMIBIOS and Phoenix FirstWare system references, a person of ordinary skill in the art would have been motivated to integrate computer security/tracking application functionality with BIOS and non-viewable-component functionality described in the claim charts for the AMIBIOS and Phoenix FirstWare in view of Phoenix’s and AMIBIOS’s advances in BIOS and non-viewable component security, extensibility, and customizability. For example, Phoenix’s cME and FirstWare functionality enabled application developers to partner with Phoenix and easily access Phoenix’s pre-defined

diagnostics and self-healing capabilities, internet access, and recovery utilities operated from system BIOSs and non-viewable components.

Defendants reserve the right to amend, supplement, and/or modify this disclosure upon further information, discovery, and analysis as the case progresses.

iv. Anticipation Prior Art and Obviousness Combinations

Defendants disclose the anticipating prior art and combinations of references in the below chart based on references identified in **Appendix A** and the Prior Art Invalidity Claim Charts submitted herewith. As demonstrated above, a skilled artisan would have had ample motivation to combine the references in the manner described herein, and would have had a reasonable expectation that such combinations would have been successful. The below combinations and anticipatory references are exemplary and non-limiting.

'837 Asserted Claims	Application of Prior Art
Claims 1, 7, 8, 17, 18	Obvious over the combination of each reference within the following combination groups: • Each Application Component reference with one or more of the following: ○ Non-Viewable Component and/or ○ BIOS Component and/or ○ Check Integrity and/or ○ Restore Integrity and/or ○ Server and/or ○ Boot Prevention references. • Each Non-Viewable Component reference with one or more of the following: ○ Application Component and/or ○ BIOS Component and/or ○ Check Integrity and/or ○ Restore Integrity and/or

'837 Asserted Claims	Application of Prior Art
	○ Server and/or ○ Boot Prevention references. • Each BIOS Component reference with one or more of the following: ○ Application Component and/or ○ Non-Viewable Component and/or ○ Check Integrity and/or ○ Restore Integrity and/or ○ Server and/or ○ Boot Prevention references. • Each Check Integrity reference with one or more of the following: ○ Application Component and/or ○ Non-Viewable Component and/or ○ BIOS Component and/or ○ Restore Integrity and/or ○ Server and/or ○ Boot Prevention references. • Each Restore Integrity reference with one or more of the following: ○ Application Component and/or ○ Non-Viewable Component and/or ○ BIOS Component and/or ○ Check Integrity and/or ○ Server and/or ○ Boot Prevention references. • Each Server reference with one or more of the following: ○ Application Component and/or ○ Non-Viewable Component and/or ○ BIOS Component and/or ○ Check Integrity and/or

'837 Asserted Claims	Application of Prior Art
	○ Restore Integrity and/or ○ Boot Prevention references. • Each Boot Prevention reference with one or more of the following: ○ Application Component and/or ○ Non-Viewable Component and/or ○ BIOS Component and/or ○ Check Integrity and/or ○ Restore Integrity and/or ○ Server references.
Claims 2, 13	Obvious over the combination of each reference within the following combination groups: • Each reference combination cited for Claim 1. • Each reference combination cited for Claim 1 with one or more Tracking references and with one or more Encrypted Message references.
Claims 3, 14	Obvious over the combination of each reference within the following combination groups: • Each reference combination cited for Claim 1. • Each reference combination cited for Claim 1 with one or more Encrypted Message references.
Claim 5	Obvious over the combination of each reference within the following combination groups: • Each reference combination cited for Claim 1. • Each reference combination cited for Claim 1 with one or more Startup File references.
Claims 6, 16	Obvious over the combination of each reference within the following combination groups: • Each reference combination cited for Claim 1. • Each reference combination cited for Claim 1 with one or more Restore Integrity references.
Claims 9, 19	Obvious over the combination of each reference within the following combination groups: • Each reference combination cited for Claim 8.

'837 Asserted Claims	Application of Prior Art
	Each reference combination cited for Claim 8 with one or more of the following references: Angelo '729, Barrus, Dayan, Hamilton, Isikoff, Pearson, PhoenixBIOS.
Claims 10-12	Obvious over the combination of each reference within the following combination groups: - Each reference combination cited for Claim 1. - Each reference combination cited for Claim 1 with one or more Tracking references and one or more Disable references.
Claims 20, 24, 27	Obvious over the combination of each reference within the following combination groups: - Each reference combination cited for Claim 1. - Each reference combination cited for Claim 1 with one or more Hardware references.
Claims 21, 22	Obvious over the combination of each reference within the following combination groups: - Each reference combination cited for Claim 20. - Each reference combination cited for Claim 20 with one or more Encrypted Message references.
Claim 23, 26	Obvious over the combination of each reference within the following combination groups: - Each reference combination cited for Claim 20. - Each reference combination cited for Claim 20 with one or more Check Integrity references and one or more Restore Integrity references.
Claim 25	Obvious over the combination of each reference within the following combination groups: - Each reference combination cited for Claim 20. - Each reference combination cited for Claim 20 with one or more Startup File references.

'710 Asserted Claims	Application of Prior Art
Claims 1, 2, 5, 6, 11-19, 23	Obvious over the combination of each reference within the following combination groups: • Each Application Component reference with one or more of the following: ○ Non-Viewable Component and/or ○ BIOS Component and/or ○ Server and/or ○ Check Integrity and/or ○ Restore Integrity and/or ○ Data Destruction references. • Each Non-Viewable Component reference with one or more of the following: ○ Application Component and/or ○ BIOS Component and/or ○ Server and/or ○ Check Integrity and/or ○ Restore Integrity and/or ○ Data Destruction references. • Each BIOS Component reference with one or more of the following: ○ Application Component and/or ○ Non-Viewable Component and/or ○ Server and/or ○ Check Integrity and/or ○ Restore Integrity and/or ○ Data Destruction references. • Each Server reference with one or more of the following: ○ Application Component and/or ○ Non-Viewable Component and/or ○ BIOS Component and/or

'710 Asserted Claims	Application of Prior Art
	○ Check Integrity and/or ○ Restore Integrity and/or ○ Data Destruction references. • Each Check Integrity reference with one or more of the following: ○ Application Component and/or ○ Non-Viewable Component and/or ○ BIOS Component and/or ○ Server and/or ○ Restore Integrity and/or ○ Data Destruction references. • Each Restore Integrity reference with one or more of the following: ○ Application Component and/or ○ Non-Viewable Component and/or ○ BIOS Component and/or ○ Server and/or ○ Check Integrity and/or ○ Data Destruction references. • Each Data Destruction reference with one or more of the following: ○ Application Component and/or ○ Non-Viewable Component and/or ○ BIOS Component and/or ○ Server and/or ○ Check Integrity and/or ○ Restore Integrity references.
Claims 3, 7, 20	Obvious over the combination of each reference within the following combination groups: • Each reference combination cited for Claim 1. • Each reference combination cited for Claim 1 with one or more Tracking references.

'710 Asserted Claims	Application of Prior Art
Claims 4, 8, 21	Obvious over the combination of each reference within the following combination groups: • Each reference combination cited for Claim 1. • Each reference combination cited for Claim 1 with one or more Automatic Identification references.

'410 Asserted Claims	Application of Prior Art
Claims 1-4, 7-11, 14-20	Obvious over the combination of each reference within the following combination groups: • Each Application Component reference with one or more of the following: ○ Non-Viewable Component and/or ○ BIOS Component and/or ○ Check Integrity and/or ○ Restore Integrity and/or ○ PowerUp references. • Each Non-Viewable Component reference with one or more of the following: ○ Application Component and/or ○ BIOS Component and/or ○ Check Integrity and/or ○ Restore Integrity and/or ○ PowerUp references. • Each BIOS Component reference with one or more of the following: ○ Application Component and/or ○ Non-Viewable Component and/or ○ Check Integrity and/or ○ Restore Integrity and/or ○ PowerUp references. • Each Check Integrity reference with one or more of the following:

'410 Asserted Claims	Application of Prior Art
	○ Application Component and/or ○ Non-Viewable Component and/or ○ BIOS Component and/or ○ Restore Integrity and/or ○ PowerUp references. ● Each Restore Integrity reference with one or more of the following: ○ Application Component and/or ○ Non-Viewable Component and/or ○ BIOS Component and/or ○ Check Integrity and/or ○ PowerUp references. ● Each PowerUp reference with one or more of the following: ○ Application Component and/or ○ Non-Viewable Component and/or ○ BIOS Component and/or ○ Check Integrity and/or ○ Restore Integrity references.

'892 Asserted Claims	Application of Prior Art
Claims 1-19	Obvious over the combination of each reference within the following combination groups: ● Each Application Component reference with one or more of the following: ○ Non-Viewable Component and/or ○ BIOS Component and/or ○ Check Integrity and/or ○ Restore Integrity and/or ○ Server and/or ○ Activation references.

'892 Asserted Claims	Application of Prior Art
	• Each Non-Viewable Component reference with one or more of the following: ○ Application Component and/or ○ BIOS Component and/or ○ Check Integrity and/or ○ Restore Integrity and/or ○ Server and/or ○ Activation references. • Each BIOS Component reference with one or more of the following: ○ Application Component and/or ○ Non-Viewable Component and/or ○ Check Integrity and/or ○ Restore Integrity and/or ○ Server and/or ○ Activation references. • Each Check Integrity reference with one or more of the following: ○ Application Component and/or ○ Non-Viewable Component and/or ○ BIOS Component and/or ○ Restore Integrity and/or ○ Server and/or ○ Activation references. • Each Restore Integrity reference with one or more of the following: ○ Application Component and/or ○ Non-Viewable Component and/or ○ BIOS Component and/or ○ Check Integrity and/or ○ Server and/or ○ Activation references.

'892 Asserted Claims	Application of Prior Art
	• Each Server reference with one or more of the following: ○ Application Component and/or ○ Non-Viewable Component and/or ○ BIOS Component and/or ○ Check Integrity and/or ○ Restore Integrity and/or ○ Activation references. • Each Activation reference with one or more of the following: ○ Application Component and/or ○ Non-Viewable Component and/or ○ BIOS Component and/or ○ Check Integrity and/or ○ Restore Integrity and/or ○ Server references.

'603 Asserted Claims	Application of Prior Art
Claims 1, 12, 18	Obvious over the combination of each reference within the following combination groups: • Each Application Component reference with one or more of the following: ○ Non-Viewable Component and/or ○ BIOS Component and/or ○ Check Integrity and/or ○ Server and/or ○ Boot Prevention references. • Each Non-Viewable Component reference with one or more of the following: ○ Application Component and/or ○ BIOS Component and/or

'603 Asserted Claims	Application of Prior Art
	○ Check Integrity and/or ○ Server and/or ○ Boot Prevention references. • Each BIOS Component reference with one or more of the following: ○ Application Component and/or ○ Non-Viewable Component and/or ○ Check Integrity and/or ○ Server and/or ○ Boot Prevention references. • Each Check Integrity reference with one or more of the following: ○ Application Component and/or ○ Non-Viewable Component and/or ○ BIOS Component and/or ○ Server and/or ○ Boot Prevention references. • Each Server reference with one or more of the following: ○ Application Component and/or ○ Non-Viewable Component and/or ○ BIOS Component and/or ○ Check Integrity and/or ○ Boot Prevention references. • Each Boot Prevention reference with one or more of the following: ○ Application Component and/or ○ Non-Viewable Component and/or ○ BIOS Component and/or ○ Check Integrity and/or ○ Server references.

'603 Asserted Claims	Application of Prior Art
Claims 2, 13	Obvious over the combination of each reference within the following combination groups: • Each reference combination cited for Claim 1. • Each reference combination cited for Claim 1 with one or more Automatic Detection / Contact references and one or more Encrypted Message references.
Claims 3, 19	Obvious over the combination of each reference within the following combination groups: • Each reference combination cited for Claim 2. • Each reference combination cited for Claim 2 with one or more Interval Messaging references and one or more Tracking references. • Each reference combination cited for Claim 2 with one or more Interval Messaging references and one or more Disable references. • Each reference combination cited for Claim 2 with one or more Interval Messaging references and one or more Boot Prevention references. • Each reference combination cited for Claim 2 with one or more Interval Messaging references and one or more Data Destruction references. • Each reference combination cited for Claim 2 with one or more Interval Messaging references and one or more Data Copying References.
Claims 4, 14, 20	Obvious over the combination of each reference within the following combination groups: • Each reference combination cited for Claim 1. • Each reference combination cited for Claim 1 with one or more Data Destruction references. • Each reference combination cited for Claim 1 with one or more Data Copying references.
Claim 10	Obvious over the combination of each reference within the following combination groups: • Each reference combination cited for Claim 1. • Each reference combination cited for Claim 1 with one or more Check Integrity references.

'603 Asserted Claims	Application of Prior Art
Claim 11	Obvious over the combination of each reference within the following combination groups: • Each reference combination cited for Claim 1. • Each reference combination cited for Claim 1 with one or more of the following references; Pearson, Cromer '464.

'649 Asserted Claims	Application of Prior Art
Claims 1, 9	Obvious over the combination of each reference within the following combination groups: • Each Hardware reference with one or more of the following: ○ Registration and/or ○ Automatic Identification and/or ○ Interval Messaging and/or ○ Disable and/or ○ Data Copying and/or ○ Server and/or ○ Non-Modifiable Memory Area and/or ○ BIOS Component references. • Each Registration reference with one or more of the following: ○ Hardware and/or ○ Automatic Identification and/or ○ Interval Messaging and/or ○ Disable and/or ○ Data Copying and/or ○ Server and/or ○ Non-Modifiable Memory Area and/or ○ BIOS Component references. • Each Automatic Identification reference with one or more of the following:

'649 Asserted Claims	Application of Prior Art
	○ Hardware and/or ○ Registration and/or ○ Interval Messaging and/or ○ Disable and/or ○ Data Copying and/or ○ Server and/or ○ Non-Modifiable Memory Area and/or ○ BIOS Component references. ● Each Interval Messaging reference with one or more of the following: ○ Hardware and/or ○ Registration and/or ○ Automatic Identification and/or ○ Disable and/or ○ Data Copying and/or ○ Server and/or ○ Non-Modifiable Memory Area and/or ○ BIOS Component references. ● Each Disable reference with one or more of the following: ○ Hardware and/or ○ Registration and/or ○ Automatic Identification and/or ○ Interval Messaging and/or ○ Data Copying and/or ○ Server and/or ○ Non-Modifiable Memory Area and/or ○ BIOS Component references. ● Each Data Copying reference with one or more of the following: ○ Hardware and/or ○ Automatic Identification and/or

'649 Asserted Claims	Application of Prior Art
	○ Interval Messaging and/or ○ Disable and/or ○ Server and/or ○ Non-Modifiable Memory Area and/or ○ BIOS Component references. ● Each Server reference with one or more of the following: ○ Hardware and/or ○ Automatic Identification and/or ○ Interval Messaging and/or ○ Disable and/or ○ Data Copying and/or ○ Non-Modifiable Memory Area and/or ○ BIOS Component references. ● Each BIOS Component reference with one or more of the following: ○ Hardware and/or ○ Registration and/or ○ Automatic Identification and/or ○ Interval Messaging and/or ○ Disable and/or ○ Data Copying and/or ○ Non-Modifiable Memory Area and/or ○ Server references. ● Each Non-Modifiable Memory Area reference with one or more of the following: ○ Hardware and/or ○ Registration and/or ○ Automatic Identification and/or ○ Interval Messaging and/or ○ Disable and/or ○ Data Copying and/or

'649 Asserted Claims	Application of Prior Art
	○ Server references.
Claims 7, 15	Obvious over the combination of each reference within the following combination groups: • Each reference combination cited for Claim 1. • Each reference combination cited for Claim 1 with one or more Data Destruction references.

'235 Asserted Claims	Application of Prior Art
Claims 1, 8, 15	Obvious over the combination of each reference within the following combination groups: • Each Application Component reference with one or more of the following: ○ Non-Viewable Component and/or ○ BIOS Component and/or ○ Check Integrity and/or ○ Restore Integrity and/or ○ BIOS Modification references. • Each Non-Viewable Component reference with one or more of the following: ○ Application Component and/or ○ BIOS Component and/or ○ Check Integrity and/or ○ Restore Integrity and/or ○ BIOS Modification references. • Each BIOS Component reference with one or more of the following: ○ Application Component and/or ○ Non-Viewable Component and/or ○ Check Integrity and/or ○ Restore Integrity and/or ○ BIOS Modification references.

'235 Asserted Claims	Application of Prior Art
	• Each Check Integrity reference with one or more of the following: ○ Application Component and/or ○ Non-Viewable Component and/or ○ BIOS Component and/or ○ Restore Integrity and/or ○ BIOS Modification references. • Each Restore Integrity reference with one or more of the following: ○ Application Component and/or ○ Non-Viewable Component and/or ○ BIOS Component and/or ○ Check Integrity and/or ○ BIOS Modification references. • Each BIOS Modification reference with one or more of the following: ○ Application Component and/or ○ Non-Viewable Component and/or ○ BIOS Component and/or ○ Check Integrity and/or ○ Restore Integrity references.
Claims 2, 3, 9, 10, 16, 17	Obvious over the combination of each reference within the following combination groups: • Each reference combination cited for Claim 1. • Each reference combination cited for Claim 1 with one or more Option ROM references.
Claims 4, 7, 11, 14, 18, 21	Obvious over the combination of each reference within the following combination groups: • Each reference combination cited for Claim 1. • Each reference combination cited for Claim 1 with one or more Application Component references and one or more Server references.
Claims 5, 12, 19	Obvious over the combination of each reference within the following combination groups:

'235 Asserted Claims	Application of Prior Art
	• Each reference combination cited for Claim 1. • Each reference combination cited for Claim 1 with one or more Non-Viewable Component references.
Claims 6, 13, 20	Obvious over the combination of each reference within the following combination groups: • Each reference combination cited for Claim 1. • Each reference combination cited for Claim 1 with one or more Boot Prevention references.

Defendants also reserve the right to rely on any combination of references describing the systems listed in **Appendix A**, *infra.*, in order to establish obviousness of the Asserted Claims. Such references would have been regarded as readily combinable by one of ordinary skill in the art because they address common problems and describe the similar underlying systems, among other things (*see* discussion above).

B. Claim Charts

Subject to Defendants' reservation of rights, attached hereto as **Exhibits A-1 through A-26, B-1 through B-27, C-1 through C-44, D-1 through D-26, E-1 through E-31, F-1 through F-45, and G-1 through G-41**, and identified in **Appendix B**, incorporated by reference, are claim charts providing a limitation-by-limitation analysis of where specifically in each prior art item each limitation of the Asserted Claims of the Asserted Patents is found. Any reference to a figure in cited text incorporates by reference the figure itself, and any citation to a figure incorporates by reference any description of that figure in a reference.

As noted above, these claim charts are based on Defendants' understanding of the claim terms as interpreted by Plaintiff in its Preliminary Infringement Contentions—even though Defendants do not necessarily agree with those constructions and reserve the right to dispute them—and/or Defendants' potential constructions. Defendants reserve the right to supplement or

modify these Invalidity Contentions in conjunction with the Court's rulings on claim construction. To the extent any limitation is deemed not be met exactly by an item of prior art, Defendants contend that the difference would have been obvious to a person of ordinary skill in the art and within the knowledge of one skilled in the art at the time of the alleged invention, so that the claimed invention would have been obvious both in light of the single reference alone and/or in light of combined references. Defendants do not admit or concede that the element is not expressly or inherently disclosed by the reference at issue.

As a general matter, all portions of each prior art item are relied upon to support the disclosure of each patent claim limitation, as all portions provide general support. Supporting citations are nevertheless provided, but do not necessarily represent every location where a particular claim term may be found in the prior art item. Defendants reserve the right to rely on additional, or different, portions of the prior art items other than those specifically cited in these claim charts, and to supplement and/or amend these charts.

C. Secondary Considerations

Plaintiff bears the burden of establishing the existence of secondary considerations and the requisite nexus to the claimed inventions. To date, Plaintiff has not disclosed that any secondary considerations support any alleged non-obviousness of the Asserted Claims. To the extent that Plaintiff subsequently discloses any contention that any secondary considerations support a conclusion that any of the Asserted Claims are not obvious, Defendants reserve the right to respond, including to amend and/or supplement these Invalidity Contentions. Moreover, as these Invalidity Contentions demonstrate, none of the Asserted Claims address any need that was either long felt or unmet, nor were their results unexpected. To the contrary, the extensive invalidating prior art detailed above and in the claim charts show that before the patents-in-suit, the prior art techniques, designs, and systems were widely accepted, understood, and available. Finally,

although secondary considerations may be relevant to the obviousness analysis, secondary considerations of nonobviousness cannot overcome the strong prima facie case of obviousness set forth in these Invalidity Contentions.

II. The Asserted Claims are Invalid under 35 U.S.C. § 102(g)(2)

Under pre-AIA 35 U.S.C. § 102(g)(2), a patent is invalid where “the invention was made in this country by another inventor who had not abandoned, suppressed, or concealed it.” This section “ensures that a patent is awarded only to the ‘first’ inventor in law.” *Apotex USA, Inc. v. Merck & Co., Inc.*, 254 F.3d 1031, 1035 (Fed. Cir. 2001). Prior invention may be established by a challenger demonstrating “(1) it reduced its invention to practice first ... or (2) it was the first party to conceive of the invention and then exercised reasonable diligence in reducing that invention to practice.” *Fox Grp., Inc. v. Cree, Inc.*, 700 F.3d 1300, 1304 (Fed. Cir. 2012) (quoting *Mycogen Plant Sci., Inc. v. Monsanto Co.*, 243 F.3d 1316, 1332 (Fed. Cir. 2001)). While “§ 102(g) prior art must be somehow made available to the public in order to defeat another patent, a § 102(g) prior inventor is under no obligation to file a patent application.” *Apotex*, 254 F.3d at 1039. Commercialization and use in printed publications are two other non-limiting examples of proving public disclosure. *Fox Grp.*, 700 F.3d at 1306; *Dow Chem. Co. v. Astro-Valcour, Inc.*, 267 F.3d 1334, 1343 (Fed. Cir. 2001).

Each Defendant contends, in their respective case, that the Accused Products do not infringe any of the Asserted Claims. However, based on Plaintiff’s overbroad interpretation and application of the Asserted Claims in its Preliminary Infringement Contentions against Defendants, Absolute first conceived the inventions recited in the Asserted Patents. Conception of the purported invention of the Asserted Patents occurred several years prior to August 2003, and Absolute diligently developed these ideas, discussing its proposed security and tracking technology with Phoenix Technologies during this period. Absolute continued efforts to reduce

to practice its security and tracking technology that culminated in the incorporation of additional functionality to its CompuTrace products.

III. The Asserted Claims are Invalid under 35 U.S.C. § 112 For Indefiniteness, Lack of Written Description, and/or Lack of Enablement

To be valid, a patent claim must “particularly point [] out and distinctly claim[] the subject matter which the inventor . . . regards as the invention.” 35 U.S.C. § 112(2). The Supreme Court has held that the proper standard for indefiniteness is as follows: “[A] patent is invalid for indefiniteness if its claims, read in light of the specification delineating the patent, and the prosecution history, fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention” *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 901 (2014). The Supreme Court further explained that “a patent must be precise enough to afford clear notice of what is claimed, thereby apprising the public of what is still open to them.” *Id.* at 909.

To uphold claims that do not clearly define the scope of the invention would thwart the ultimate purpose of the patent laws: to “promote the Progress of Science and useful Arts.” *Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co.*, 535 U.S. 722, 730 (2002) (quoting U.S. Const. art. I, § 8, cl. 8). As the Supreme Court explained in *Festo*, a patent claim “is a property right; and like any property right, its boundaries should be clear. This clarity is essential to promote progress, because it enables efficient investment in innovation. A patent holder should know what he owns, and the public should know what he does not.” *Id.* The identified claim terms of Plaintiff’s Asserted Claims “fall[] within the innovation-discouraging ‘zone of uncertainty’ against which the Supreme Court has warned.” *Interval Licensing LLC v. AOL, Inc.*, 766 F. 3d 1364, 1374 (Fed. Cir. 2014), quoting *Nautilus*, 572 U.S. at 911 (cleaned up).

This principle may also apply where a single claim covers both an apparatus and a method of use, as it “does not apprise a person of ordinary skill in the art of its scope, and it is invalid under section 112, paragraph 2.” *IPXL Holdings, L.L.C. v. Amazon.com, Inc.*, 430 F.3d 1377, 1384 (Fed. Cir. 2005). For example, “as a result of the combination of two separate statutory classes of invention, a manufacturer or seller ... would not know from the claim whether it might also be liable for contributory infringement because a buyer or user of the apparatus later performs the claimed method of using the apparatus.” *Id.* (citing *Ex parte Lyell*, 17 U.S.P.Q.2d 1548, 1550 (B.P.A.I. 1990)). Such a claim “is not sufficiently precise to provide competitors with an accurate determination of the ‘metes and bounds’ of protection involved.” *Lyell*, 17 U.S.P.Q.2d at 1550-51; *see also In re Katz Interactive Call Processing Patent Litig.*, 639 F.3d 1303, 1318 (Fed. Cir. 2011) (observing under *IPXL* that “it [is] unclear ‘whether infringement ... occurs when one creates a system that allows the user [to use the input means], or whether infringement occurs when the user actually uses the input means.’”). Numerous of the Asserted Claims, identified below, cover both a system and method of use and fail to provide sufficient clarity as to what constitutes infringement.

The Asserted Claims suffer from similar defects that may render them indefinite, at least under Plaintiff’s apparent view of the claim scope. Plaintiff’s Preliminary Infringement Contentions further indicate that Plaintiff may interpret the claims in a manner that further renders them indefinite, particularly in view of the absence of sufficient supporting disclosure in the intrinsic evidence.

Defendants also note that the attached claim charts identify disclosures in the prior art that correspond to limitations of the Asserted Claims; in some cases, Defendants have identified prior art disclosures corresponding to limitations separately identified below as being potentially

indefinite. The identification of corresponding disclosures in the prior art for such limitations should not be construed as a concession that Defendants believe those limitations fulfill the definiteness requirement, or inform persons of ordinary skill in the art of the metes-and-bounds of the full scope of the alleged invention with reasonable certainty. Rather, Defendants' prior art disclosures are based on their best understanding (without the benefit of claim construction by the Court) informed by the Infringement Contentions served by Plaintiff, and in some cases, were chosen because they most closely mirror exemplary embodiments in the specifications of the Asserted Patents (and thus are likely to meet the disputed claim limitations in the event they are not adjudged to be indefinite).

In view of the foregoing, Defendants identify below potential grounds of invalidity for indefiniteness, which Defendants reserve the right to present during claim construction proceedings and/or summary judgment proceedings in this action. Defendants provide these contentions without the benefit of upcoming claim construction discovery and other ongoing discovery. Defendants may provide proposed claim constructions to be adopted in the alternative to the extent certain claim terms and elements are not determined to be indefinite. Where a certain claim term or limitation in one claim is identified as indefinite, Defendants contend that the same claim term or limitation is indefinite in every instance the term or limitation is recited throughout the Asserted Claims. Where Defendants have identified a phrase as indefinite, Defendants also contend that the subparts of the phrase are indefinite within the context recited in the claim.

For the written description requirement, "the test for sufficiency is whether the disclosure of the application relied upon reasonably conveys to those skilled in the art that the inventor had possession of the claimed subject matter as of the filing date." *Ariad Pharms., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010) (en banc). Possession requires a "show[ing] that the

inventor actually invented the invention claimed.” *Id.* The “level of detail required to satisfy the written description requirement varies depending on the nature and scope of the claims and on the complexity and predictability of the relevant technology.” *Id.* “[T]he purpose of the written description requirement is to ‘ensure that the scope of the right to exclude, as set forth in the claims, does not overreach the scope of the inventor’s contribution to the field of art as described in the patent specification.’” *ICU Med., Inc. v. Alaris Med. Sys., Inc.*, 558 F.3d 1368, 1376-79 (Fed. Cir. 2009) (citations omitted).

The Asserted Claims are invalid for lack of written description where indicated below, including under the reasoning of precedent such as *Ariad, ICU Medical, Synthes USA, LLC v. Spinal Kinetics, Inc.*, 734 F.3d 1332, 1341-45 (Fed. Cir. 2013), *LizardTech, Inc. v. Earth Resource Mapping, Inc.*, 424 F.3d 1336, 1343-48 (Fed. Cir. 2005), *Liebel-Flarsheim Co. v. Medrad, Inc.*, 358 F.3d 898, 905-914 (Fed. Cir. 2004), and other case law, because the specification does not contain a written description of the claimed subject matter.

For example, in *LizardTech*, the claim was directed to a method of compressing digital images using seamless discrete wavelet transformation (“DWT”). The court found that the claim covered all ways of performing DWT-based compression processes that lead to a seamless DWT because there were no limitations as to how the seamless DWT was to be accomplished. However, the specification provided only one method for creating a seamless DWT, and there was no evidence that the specification contemplated a more generic way of creating a seamless array of DWT coefficients. Therefore, the written description requirement was not satisfied in this case because the specification did not provide sufficient evidence that the inventor invented the generic claim. “[T]he description of one method for creating a seamless DWT does not entitle the inventor . . . to claim any and all means for achieving that objective.” *LizardTech*, 424 F.3d at 1346.

Similarly, in *ICU Medical*, the written description described the use of valves with a spike, but the patent applicant later prosecuted claims with a “spikeless” claim scope that “do not require a spike.” *ICU Med.*, 558 F.3d at 1377. As the Federal Circuit explained:

ICU’s asserted spikeless claims are broader than its asserted spike claims because they do not include a spike limitation; these spikeless claims thus refer to medical valves generically—covering those valves that operate with a spike and those that operate without a spike. But the specification describes only medical valves with spikes. *See supra* Part I. We reject ICU’s contention that the figures and descriptions that include spikes somehow demonstrate that the inventor possessed a medical valve that operated without a spike. Based on this disclosure, a person of skill in the art would not understand the inventor of the ‘509 and ‘592 patents to have invented a spikeless medical valve.

Id. at 1378. Because the specification did not disclose subject matter that operated without a spike, the Federal Circuit affirmed summary judgment of invalidity for failure to satisfy the written description requirement. *Id.* at 1379.

In *Synthes USA*, as further illustration, the written description described only certain subject matter including “a plurality of grooves and a plurality of channels, but did not describe ‘openings’ generally.” *Synthes USA*, 734 F.3d at 1341. The applicant broadened the claim scope during prosecution to a more general claim scope, in an attempt to read the claims on a competitor’s product. *Id.* A jury found invalidity for lack of written description, and the Federal Circuit affirmed. The Federal Circuit found that the evidence supported a finding that “the as-filed disclosure did not demonstrate possession of an intervertebral implant that employed *any sort* of openings *anywhere* on the cover plates.” *Id.* (emphasis in original). The Federal Circuit noted that the written description “never discloses anything broader than using grooves to anchor the fiber system to the cover plates.” *Id.* at 1342.

The “enablement requirement is satisfied when one skilled in the art, after reading the specification, could practice the claimed invention without undue experimentation.” *Auto. Techs. Int’l, Inc. v. BMW of N. Am.*, 501 F.3d 1274, 1282 (Fed. Cir. 2007). A claimed invention may be

invalid under § 112 for lack of written description and non-enablement even if it was disclosed in the prior art: “[i]t is the specification, not the knowledge of one skilled in the art, that must supply the novel aspects of an invention in order to constitute adequate enablement.” *Genentech, Inc. v. Novo Nordisk*, 108 F.3d 1361, 1366 (Fed. Cir. 1997). The patentee is “required to provide an adequate enabling disclosure in the specification; it cannot simply rely on the knowledge of a person of ordinary skill to serve as a substitute for the missing information in the specification.” *Alza Corp. v. Andrx Pharms., LLC*, 603 F.3d 935, 940-41 (Fed. Cir. 2010). “A patentee who chooses broad claim language must make sure the broad claims are fully enabled.” *Sitrick v. Dreamworks, LLC*, 516 F.3d 993, 999-1000 (Fed. Cir. 2008). As the Federal Circuit has explained:

Enablement serves the dual function in the patent system of ensuring adequate disclosure of the claimed invention and of preventing claims broader than the disclosed invention. This important doctrine prevents both inadequate disclosure of an invention and overbroad claiming that might otherwise attempt to cover more than was actually invented. Thus, a patentee chooses broad claim language at the peril of losing any claim that cannot be enabled across its full scope of coverage.

MagSil Corp. v. Hitachi Global Storage Techs., Inc., 687 F.3d 1377, 1380-81 (Fed. Cir. 2012). “The specification must contain sufficient disclosure to enable an ordinarily skilled artisan to make and use the entire scope of the claimed invention at the time of filing.” *Id.* at 1381-82.

The claims are invalid for lack of enablement because the written descriptions do not enable the full scope of the claimed subject matter. *Liebel-Flarsheim Co. v. Medrad, Inc.*, 481 F.3d 1371 (Fed. Cir. 2007); *Automotive Techs.*, 501 F.3d at 1284-85; *Sitrick*, 516 F.3d at 999-1000; *MagSil*, 687 F.3d at 1380-81. In *Liebel-Flarsheim*, for example, the claimed invention was a front-loading fluid injector system with a replaceable syringe capable of withstanding high pressure for delivering a contrast agent to a patient. *Liebel-Flarsheim*, 481 F.3d at 1373. The claims were construed to cover systems with or without a pressure jacket, but the written description failed to enable “both injector systems with and without a pressure jacket.” *Automotive Techs.*, 501 F.3d

at 1285 (citation omitted).

Similarly, in *Automotive Techs.*, the claims covered “both mechanical and electronic side impact sensors,” but the specification failed to enable the full scope: “in order to fulfill the enablement requirement, the specification must enable the full scope of the claims that includes both electronic and mechanical side impact sensors, which the specification fails to do.” *Id.*

In *Sitrick*, the claims were broad enough to cover integrating signals into pre-existing media: “[b]ecause the asserted claims are broad enough to cover both movies and video games; the patents must enable both embodiments.” *Sitrick*, 516 F.3d at 999-1000. The specification failed to enable embodiments using movies: “one skilled in the art could not take the disclosure in the specification with respect to substitution or integration of user images in video games and substitute a user image for a pre-existing character image in movies without undue experimentation.” *Id.* at 1000. *See also, e.g., MagSil*, 687 F.3d at 1381-84 (the claims covered a broad range of resistive charge that the written description did not enable); *Alza*, 603 F.3d at 940-943 (“ALZA’s patent specification does not enable the full scope of the claims, namely non-osmotic oral dosage forms with ascending release rates”).

In view of the foregoing, Defendants identify below the following grounds of invalidity under § 112. Defendants provide these contentions without the benefit of upcoming claim construction discovery and other ongoing discovery. These § 112 contentions reflect that Plaintiff’s apparent asserted scope of the claim language as reflected in Plaintiff’s Preliminary Infringement Contentions suggests a broader scope than the specification sufficiently supports, though at this stage Plaintiff has not yet disclosed its claim construction positions to be disclosed in upcoming claim construction discovery. Discovery has not yet opened, and Defendants’ analysis and investigation continues. Defendants accordingly reserve the right to amend these

disclosures in view of further discovery, information, and/or analysis.

Where a certain claim term or limitation in one claim is identified as being subject to a § 112 invalidity defect, Defendants contends that the same claim term or limitation, and each constituent phrase and term containing substantially the same claim limitation, is subject to the same defect in every instance the term or limitation is recited throughout the Asserted Claims. Furthermore, each ground of invalidity under § 112 for any identified claim also applies to any asserted claim that depends from it.

As explained in the table below, the Asserted Claims are invalid for lack of enablement and/or lack of written description, and potentially indefinite, at least for the reasons below.

Claim(s)	Limitation / Term	Grounds of § 112 Invalidity Challenge
'837, cls. 1, 2, 7, 10, 12, 13, 17, 20, 21, 27; '710, cls. 1, 2, 6, 18, 19, 23; '410, cls. 1, 8, 15; '892, cls. 1, 11, 12, 15; '235, cls. 1, 5, 8, 12, 15, 19	"non-viewable"	Indefinite. The term "non-viewable" is subjective, lacks an exact meaning, and relies on the view of the person interpreting a term. Moreover, whether a component is "viewable" or "non-viewable" depends on the expertise and ability of the user, which the specification fails to provide. The intrinsic record provides no guidance to hem in the flexible and shifting character of this term, and a person of ordinary skill would not have understood the objective meaning of the term with reasonable certainty under <i>Nautilus</i> and its progeny.
'837, cls. 1, 12, 20; '892, cls. 11, 12	"support an operating system environment"	Deficient written description and/or enablement, and indefinite. A person of ordinary skill would not have understood with reasonable certainty the full scope of the term "support an operating system environment" under <i>Nautilus</i> , as what constitutes "support" is unclear and/or ambiguous. In addition, nowhere in the intrinsic record does the patent describe this term or define the metes and bounds of its scope.
'837, cls. 1, 12, 20; '710,	"tampered with"	Deficient written description and/or enablement, and indefinite. A person of

Claim(s)	Limitation / Term	Grounds of § 112 Invalidity Challenge
cls. 1, 2, 19; '892, cls. 1, 11, 12, 15; '235, cl. 8		ordinary skill would not have understood with reasonable certainty the full scope of the term “tampered with” under <i>Nautilus</i> , as what constitutes “tampering” is unclear and/or ambiguous. In addition, nowhere in the intrinsic record does the patent describe this term or define the metes and bounds of its scope.
'837, cls. 1, 12, 20; '710, cls. 1, 2; '892, cls. 1, 11, 12; '235, 8, 15	“substantially distinct”	Indefinite. The term “substantially distinct” is subjective, lacks an exact meaning, and relies on the view of the person interpreting a term. The intrinsic record provides no guidance to hem in the flexible and shifting character of this term, and a person of ordinary skill would not have understood the objective meaning of the term with reasonable certainty under <i>Nautilus</i> and its progeny.
'410, cls. 1, 8, 15, 17; '603, cls. 1, 12, 18	“operate[d] correctly” / “operating correctly”	Deficient written description and/or enablement, and indefinite. The term “correctly” is subjective, lacks an exact meaning, and relies on the view of the person interpreting a term. Specifically, “operate correctly” lacks sufficient disclosure within the specification for a person of ordinary skill to distinguish between “correct” and “incorrect” operation. For example, there is no description of which aspects of the application must be checked for correct operation or which aspects matter in terms of making the overall conclusion of whether the application is operating correctly.
'892, cls. 11, 12, 19	“hardware and software”	Deficient written description and/or enablement, and indefinite. The claim fails to recite anything that is performed by “hardware,” and it is unclear what hardware is needed to practice the claim, or what the hardware would be required to do.
'649, cls. 1, 9	“user function”	Deficient written description and/or enablement, and indefinite. A person of ordinary skill would not have understood

Claim(s)	Limitation / Term	Grounds of § 112 Invalidity Challenge
		with reasonable certainty the full scope of the term “user function” under <i>Nautilus</i> , as the specification does not describe what a user function is as opposed to a system or some other category of “function.”
'649, cls. 1, 9	“system area that cannot be modified by the user”	Deficient written description and/or enablement, and indefinite. The term “cannot be modified by the user” is subjective, lacks an exact meaning, and relies on the view of the person interpreting a term. Moreover, whether a memory area “cannot be modified” may depend on the expertise and ability of the user, which the specification fails to provide. The intrinsic record provides no guidance to hem in the flexible and shifting character of this term, and a person of ordinary skill would not have understood the objective meaning of the term with reasonable certainty under <i>Nautilus</i> and its progeny. Moreover, “system area that cannot be modified by the user” lacks sufficient disclosure because there is no description of how to protect an area of non-volatile memory against modification by a user.
'235, cl. 8	“A system comprising: ... a [BIOS] component ... wherein the BIOS component is capable of being integrated into a target BIOS binary image of the electronic device by operations including: opening a BIOS modification application, opening a target BIOS binary image of the electronic device within the BIOS modification application, and adding an electronic security and tracking system and method (ESTSM) Read-Only-Memory (ROM) image to the target BIOS binary image.”	Indefinite. The claims recite both apparatus and method steps such that a person of ordinary skill would not be able to readily ascertain from the scope of the claims with reasonable clarity under <i>IPXL</i> and its progeny, and whether infringement occurs through a system with the claimed functionality or when a user performs the claimed operations associated with the BIOS component (e.g., opening a BIOS modification application).
'235, cl. 15	“A non-transitory machine-readable medium... computer	Indefinite. The claims recite both apparatus and method steps such that a

Claim(s)	Limitation / Term	Grounds of § 112 Invalidity Challenge
	system to perform operations comprising: opening a BIOS modification application, opening a target BIOS binary image of the electronic device within the BIOS modification application, and adding an electronic security and tracking system and method (ESTSM) [Read-Only-Memory] (ROM) image to the target BIOS binary image”	person of ordinary skill would not be able to readily ascertain from the scope of the claims with reasonable clarity under <i>IPXL</i> and its progeny, and whether infringement occurs through a system with the claimed functionality or when a user performs the claimed operations associated with the BIOS component (<i>e.g.</i> , opening a BIOS modification application).
’649, cl. 1	“A mobile electronic device, comprising: ... a security application ... wherein the security application is operable to perform operations comprising: ...enabling an owner of the mobile electronic device to register the mobile electronic device with a security service ... after the owner has registered the mobile electronic device with the security service, ...”	Indefinite. The claims recite both apparatus and method steps such that a person of ordinary skill would not be able to readily ascertain the scope of the claims with reasonable clarity under <i>IPXL</i> and its progeny, and whether infringement occurs through a mobile electronic device with the claimed functionality or when an “owner” registers a mobile electronic device for the claimed security service.
’649, cl. 17	“An article of manufacture comprising: ... a security application ... wherein the security application, when executed by a mobile electronic device, enables the mobile electronic device to perform operations comprising: ...receiving, at the mobile electronic device, a request from an owner of the mobile electronic device to register the mobile electronic device with a security service ... after the owner has registered the mobile electronic device with the security service, ...”	Indefinite. The claims recite both apparatus and method steps such that a person of ordinary skill would not be able to readily ascertain the scope of the claims with reasonable clarity under <i>IPXL</i> and its progeny, and whether infringement occurs through an article of manufacture with the claimed functionality or when an “owner” registers a mobile electronic device for the claimed security service.
’892, cls. 11, 12	“[A system for providing an electronic device security service, / An electronic device]	Indefinite. The claims recite both apparatus and method steps such that a person of ordinary skill would not be able

Claim(s)	Limitation / Term	Grounds of § 112 Invalidity Challenge
	comprising: hardware and software components operable to ... present a user interface which allows a user of the electronic device to request activation of a security service for the electronic device, ... wherein, after the security service has been activated, ...”	to readily ascertain the scope of the claims with reasonable clarity under <i>IPXL</i> and its progeny, and whether infringement occurs through a system with the claimed functionality or when a user opts-in to the claimed security service.
’892, cl. 15	“An apparatus comprising: ... providing, to a user of the machine, a user interface which allows the user to request activation of a security service for the machine, ... in response to receiving the opt-in input from the user, activating the security service, wherein activation of the security service causes the machine to be provided with: a non-viewable component, an application component ... a Basic Input/Output System (BIOS) component ...”	Indefinite. The claims recite both apparatus and method steps such that a person of ordinary skill would not be able to readily ascertain the scope of the claims with reasonable clarity under <i>IPXL</i> and its progeny, and whether infringement occurs through an apparatus with the claimed functionality or when a user opts-in to the claimed security service.
’710, cl. 2	“A system for providing security for an electronic device, comprising: a server system capable of communicating through a secure medium with the application component, wherein the system is operable to perform operations comprising: accepting a selection of a data destruction service for an electronic device, ... after accepting the selection of the data destruction service ...”	Indefinite. The claims recite both apparatus and method steps such that a person of ordinary skill would not be able to readily ascertain the scope of the claims with reasonable clarity under <i>IPXL</i> and its progeny, and whether infringement occurs through a system with the claimed functionality or when one selects a data destruction service for an electronic device.
’710, cl. 19	“An article of manufacture, comprising: ... the computer system to perform operations comprising: accepting a selection of a data destruction service for an electronic device, ... after	Indefinite. The claims recite both apparatus and method steps such that a person of ordinary skill would not be able to readily ascertain the scope of the claims with reasonable clarity under <i>IPXL</i> and its progeny, and whether infringement occurs through an article of manufacture with the

Claim(s)	Limitation / Term	Grounds of § 112 Invalidity Challenge
	accepting the selection of the data destruction service ...”	claimed functionality or when one selects a data destruction service for an electronic device.

IV. Ineligible Subject Matter Under 35 U.S.C. § 101

The asserted claims of the ’410, ’892, ’603, and ’649 Patents, particularly as asserted by Plaintiff in this action, fail to recite patent-eligible subject matter under § 101 and applicable case law precedent.

Section 101 provides that “[w]hoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.” 35 U.S.C. § 101. The Supreme Court has “long held that this provision contains an important implicit exception: Laws of nature, natural phenomena, and abstract ideas are not patentable.” *Alice Corp. v. CLS Bank Int’l*, 573 U.S. 208, 216 (2014) (quoting *Ass’n for Molecular Pathology v. Myriad Genetics, Inc.*, 569 U.S. 576, 589 (2013)). “[S]uch discoveries are manifestations of...nature, free to all men and reserved exclusively to none.” *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 70 (2012) (quotations and citations omitted). The concern that underlies “this exclusionary principle” is “one of pre-emption.” *Alice*, 573 U.S. at 216. Thus, patents that seek to preempt others from using “the basic tools of scientific and technological work” are invalid. *Id.*

The Supreme Court in *Alice* set forth a two-step test “for distinguishing patents that claim laws of nature, natural phenomena, and abstract ideas from those that claim patent-eligible applications of those concepts.” *Alice*, 573 U.S. at 217.

1. First, the Court must “determine whether the claims at issue are directed to one of those patent-ineligible concepts,” such as an abstract idea. *Id.* If the Court determines that the claims are directed to a patent-ineligible concept such as an abstract idea, then:

2. The Court must “consider the elements of each claim both individually and as an ordered combination to determine whether the additional elements transform the nature of the claim into a patent-eligible application.” *Id.* (citation and quotation marks omitted). The Supreme Court describes this second step “as a search for an inventive concept—*i.e.*, an element or combination of elements that is sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the ineligible concept itself.” *Id.* at 217-18 (quotation marks and brackets omitted). For example, “[s]tating an abstract idea while adding the words ‘apply it’ is not enough for patent eligibility. Nor is limiting the use of an abstract idea ‘to a particular technological environment.’” *Id.* at 223 (internal citations and quotations omitted).

Each and every asserted claim of the ’410, ’892, ’603, and ’649 Patents is invalid under 35 U.S.C. § 101 and applicable case law authority. *See, e.g., Alice*, 573 U.S. at 216; *In re TLI Commc’ns LLC Patent Litig.*, 823 F.3d 607, 613 (Fed. Cir. 2016); *Intellectual Ventures I LLC v. Capital One Bank (USA)*, 792 F.3d 1363, 1369 (Fed. Cir. 2015); *Digitech Image Techs., LLC v. Elecs. for Imaging, Inc.*, 758 F.3d 1344, 1351 (Fed. Cir. 2014); *Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat’l Ass’n*, 776 F.3d 1343, 1348 (Fed. Cir. 2014); *Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 709, 719 (Fed. Cir. 2014); *BuySAFE, Inc. v. Google, Inc.*, 765 F.3d 1350, 1355 (Fed. Cir. 2014); *Internet Patents Corp. v. Active Network, Inc.*, 790 F.3d 1343, 1347-48 (Fed. Cir. 2015); *Intellectual Ventures I LLC v. Capital One Fin. Corp.*, 850 F.3d 1332, 1341 (Fed. Cir. 2017); *FairWarning IP, LLC v. Iatric Sys., Inc.*, 839 F.3d 1089, 1093 (Fed. Cir. 2016); *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1354 (Fed. Cir. 2016); *Two-Way Media Ltd. v. Comcast Cable Commc’ns, LLC*, 874 F.3d 1329, 1337 (Fed. Cir. 2017); *Affinity Labs of Tex., LLC v. Amazon.com Inc.*, 838 F.3d 1266, 1267-68 (Fed. Cir. 2016); *BSG Tech LLC v. Buyseasons, Inc.*, 899 F.3d 1281, 1287 (Fed. Cir. 2018); *SAP Am., Inc. v. InvestPic, LLC*, 898 F.3d 1161, 1166-68

(Fed. Cir. 2018); *Burnett v. Panasonic Corp.*, 741 F. App'x 777, 782-83 (Fed. Cir. 2018); *In re Villena*, 745 F. App'x 374, 376-77 (Fed. Cir. 2018); *Interval Licensing LLC v. AOL, Inc.*, 896 F.3d 1335, 1338, 1345-48 (Fed. Cir. 2018); *Intellectual Ventures I v. Symantec*, 725 F. App'x 976, 978 n.1 (Fed. Cir. 2018); *Zuili v. Google LLC*, 722 F. App'x 1027, 1030 (Fed. Cir. 2018); *WhitServe LLC v. Donuts Inc.*, 809 F. App'x 929, 932 (Fed. Cir. 2020); *Elec. Comm'n Techs., LLC v. ShoppersChoice.com, LLC*, 958 F.3d 1178, 1180-81 (Fed. Cir. 2020); *Dropbox, Inc. v. Synchronoss Techs., Inc.*, 815 F. App'x 529, 533 (Fed. Cir. 2020); *Am. Axle & Mfg., Inc. v. Neapco Holdings LLC*, 967 F.3d 1285, 1295 (Fed. Cir. 2020); *Chamberlain Grp., Inc. v. Techtronic Indus. Co.*, 935 F.3d 1341, 1348 (Fed. Cir. 2019); *Innovation Scis., LLC v. Amazon.com, Inc.*, 778 F. App'x 859, 863 (Fed. Cir. 2019); *Ameranth, Inc. v. Domino's Pizza, LLC*, 792 F. App'x 780, 788 (Fed. Cir. 2019); *ChargePoint, Inc. v. SemaConnect, Inc.*, 920 F.3d 759, 766 (Fed. Cir. 2019); *Voter Verified, Inc. v. Election Sys. & Software LLC*, 887 F.3d 1376, 1384 (Fed. Cir. 2018); *BSG Tech*, 899 F.3d at 1290; *Glasswall Sols. v. Clearswift, Ltd.*, 754 F. App'x 996, 999 (Fed. Cir. 2018); *Interval Licensing LLC v. AOL, Inc.*, 896 F.3d 1335, 1346 (Fed. Cir. 2018); *Smartflash LLC v. Apple Inc.*, 680 F. App'x 977, 983 (Fed. Cir. 2018); *Location Based Servs., LLC v. Niantic, Inc.*, 295 F. Supp. 3d 1031, 1040, 1045-49 (N.D. Cal. 2017), *aff'd*, 742 F. App'x 506 (Fed. Cir. 2018).

The independent claims of the '410 and '603 Patents are directed to the abstract idea of testing and qualifying an operator and using a gatekeeper to prevent startup if the operator does not qualify. Humans have performed these types of qualification procedures by hand for decades in various contexts, including for employment decisions. As an example, in claim 1 of the '603 Patent, an application component ascertains whether an electronic device has been reported stolen from third-party information, much like conducting a background check, physical fitness test, or medical/psychological evaluation for a potential employment candidate. This information may

then be passed to the hiring manager—analogue to the claimed BIOS component—who determine whether to move forward with the hiring process for the candidate depending on the test results. As another example, the claims could be analogized to someone performing a title check for a car, in which the person checks vehicle records to determine whether a car has been reported stolen and reports that information to the potential purchaser, who then makes the decision about whether to purchase the car based on the title check results. The alleged inventions merely apply this process to a computer environment which only uses conventional computer technologies and lacks any inventive concept. The asserted dependent claims simply add more routine steps, and the limitations of each claim considered together do not provide any inventive concept that transforms any claim into patent eligible subject matter. The claims are directed to known functionality, and thus the asserted claims of the '410 and '603 Patents are directed to patent ineligible subject matter and are invalid under § 101.

Similarly, the independent claims of the '649 Patent are directed to the abstract ideas of (1) signing up for a monitoring service; (2) communicating with that service; and (3) after receiving a specific message from the service, ceasing operations and copying information to be sent to the service. These human activities fail to recite a technological improvement or inventive concept that might confer patent eligibility, alone or in combination with each other. Registering or signing up with a party to provide security or monitoring services is an age-old human practice to ensure protection from external threats, *e.g.*, choosing to live in a building or community with security guards or a neighborhood watch group, forming military alliances, and/or hiring sentries to stand watch.

Nor are the claimed communications between the electronic device and the security service server anything more than a routine activity practiced by humans since time immemorial. This

communication is little more than “remote surveillance or monitoring for security or control purposes” between an electronic device and a server —“a ‘longstanding’ and ‘fundamental’ human activity that falls ‘squarely within the realm of abstract ideas.’” *Sensormatic Elecs., LLC v. Wyze Labs, Inc.*, 484 F. Supp. 3d 161, 166 (D. Del. 2020), *Joao Control & Monitoring Sys., LLC v. Digital Playground, Inc.*, No. 12-cv-6781, 2016 WL 5793745, at *5 (S.D.N.Y. Sept. 30, 2016); *see also Intellectual Ventures I LLC v. Erie Indemnity Co.*, 850 F.3d 1315, 1329 (Fed. Cir. 2017) (“sending and receiving information” over a network are “routine computer functions”), *buySAFE*, 765 F.3d at 1355 (“receiv[ing] and send[ing] the information over a network” is generic), *Callwave Commc’ns, LLC v. AT&T Mobility, LLC*, 207 F. Supp. 3d 405, 414-15 (D. Del. 2016) (finding claims directed to “remote tracking” invalid under § 101). *Joao Control & Monitoring Sys., LLC v. Telular Corp.*, 173 F. Supp. 3d 717, 727 (N.D. Ill. 2016); *see also Wireless Media Innovations, LLC v. Maher Terminals, LLC*, 100 F. Supp. 3d 405, 413 (D.N.J. 2015) (invalidating patents directed to the “abstract idea [of] monitoring locations, movements, and load status of shipping containers within a container-receiving yard, and storing, reporting, and communicating this information in various forms through generic computer functions”), *aff’d*, 636 F. App’x 1014 (Fed. Cir. 2016).

The claims describe, through the security server receiving theft reports and notifying the mobile device, the related abstract idea of “collecting and analyzing information to detect misuse and notifying a user when misuse is detected.” *FairWarning IP, LLC v. Iatric Sys., Inc.*, 839 F.3d 1089, 1094-95 (Fed. Cir. 2016).

The corrective actions taken in response to receiving a theft notification from a server—*e.g.*, remote commands to disable a device and to copy and delete information—are also age-old human activities not entitled to patent eligibility. *See, e.g., Whitserve LLC v. Dropbox, Inc.*, 854

F. App'x 367, 371-72 (Fed. Cir. 2021) (“requesting, transmitting, receiving, copying, deleting, and storing data” is an abstract idea); *ClearDoc, Inc. v. RiversideFM, Inc.*, No. 21-1422-RGA, 2022 WL 3355960, at *5 (D. Del. Aug. 15, 2022) (dismissing claims as patent ineligible under § 101 that were directed to the “abstract idea of remotely controlling the recording, storing, delivering, and automatic deletion of [data] on a mobile device.”); *Interactive Wearables, LLC v. Polar Electro Oy*, 501 F. Supp. 3d 162, 174 (E.D.N.Y. 2020), *aff'd*, 2021 WL 47838083 (Fed. Cir. Oct. 14, 2021) (noting providing “remote control” over the operation of an external device, where the function are “described in vague terms without any meaningful limitations” indicat[es] that “the focus of the patentee and of the claims was not on an improved’ version of any of these components.” (quoting *TLI Commc’ns LLC Patent Litig.*, 823 F.3d at 612-13)).

These claims merely invoke “well-understood, routine [and] conventionality” technology to carry out the abstract ideas. *See Alice*, 573 U.S. at 225. When filtering out the purported invention’s use of the abstract ideas described above, *see BSG Tech*, 889 F.3d at 1290, nothing is left to the claims except general computer technologies that cannot confer patent eligibility. Moreover, nothing about the ordered combination of claim elements transforms the nature of the claims into a patent eligible invention. *Alice*, 573 U.S. at 217.

Finally, the asserted independent claims of the ’892 Patent are essentially a mashup of the abstract ideas recited in the claims of the ’603, ’410, and ’649 Patents and are patent ineligible under § 101 for similar reasons. The asserted dependent claims of the ’892 Patent—*e.g.*, offering security services free of charge, on a trial basis, activating/administering security through manufactures and/or third-parties—involve “fundamental economic practice[s] long prevalent in our system of commerce,” and the “use of a third-party intermediary” that are patent-ineligible abstract ideas. *See Alice*, 573 U.S. at 219-20. Nothing in the claims are drawn to an inventive

concept that transform these disqualifying concepts into patent eligible subject matter.

V. Other Prior Art

In addition to the prior art references that Defendants have specifically discussed in these Invalidity Contentions, Defendants provide notice to Plaintiff of each reference produced in the accompanying document production of the same date. To the extent not specifically cited and relied upon as invalidating references with respect to the elements of the Asserted Claims, Defendants reserve the right to rely on these references at least as illustrating background knowledge in the field prior to the alleged inventions of the Asserted Claims and for other relevant purposes as may be disclosed pursuant to Defendants' continuing research and analysis of the Asserted Claims, accused instrumentalities, and the prior art.

VI. All Prior Art Referenced in the Invalidity Contentions

Pursuant to the Corrected Joint Rule 26(f) Report, all prior art documentation referenced in the Invalidity Contentions is being produced by secure FTP link at the following production number range: ABSOLUTE-SFTX00000001-ABSOLUTE-SFTX00004564.

VII. Technical Documents, Including Software Where Applicable, Sufficient to Show the Operation of the Accused Product(s)

Pursuant to the Corrected Joint Rule 26(f) Report, Defendants give notice that source code related to the Accused Absolute Functionality are available for inspection on a stand-alone source code computer at Cooley's offices in Palo Alto pursuant to the terms of the Protective Order in this matter.

Dated: June 29, 2023

COOLEY LLP

By: /s/ Dustin M. Knight
Heidi L. Keefe (CA Bar 178960)
hkeefe@cooley.com
Reuben H. Chen (CA Bar 228725)
rchen@cooley.com
Alexandra Leeper (admitted *pro hac vice*)
aleeper@cooley.com
3175 Hanover Street
Palo Alto, CA 94304
Telephone: (650) 843-5000
Fax: (650) 849-7400

Orion Armon (admitted *pro hac vice*)
oarmon@cooley.com
1144 15th Street, Suite 2300
Denver, CO 80202
Telephone: (720) 566-4000
Fax: (720) 566-4099

Dustin M. Knight (admitted *pro hac vice*)
dknight@cooley.com
11951 Freedom Drive, 16th Floor
Reston, VA 20190
Telephone: (703) 456-8000
Fax: (703) 456-8100

Samuel K. Whitt (admitted *pro hac vice*)
swhitt@cooley.com
1299 Pennsylvania Avenue, NW
Suite 700
Washington, DC 20004
Telephone: (202) 842-7800
Fax: (202) 842-7899

*Attorneys for Defendants Absolute
Software Corporation and Absolute
Software, Inc.*

APPENDIX A

Patent	Short Name	Prior Art Reference(s)	Priority Date(s)
U.S. Patent No. 5,748,084	Isikoff	Device security system	11/18/1996
U.S. Patent No. 6,711,660	Milne	System and method for performing disk drive diagnostics and restoration using a host-inaccessible hidden partition	6/22/2001
U.S. Patent No. 7,107,349	Britt	System and method for disabling and providing a notification for a data processing device	9/30/2002
U.S. Patent No. 7,461,249	Pearson	Computer platforms and their methods of operation	8/11/2000
U.S. Patent Application No. 2002/0045437	Kesler	Tracing a location of a mobile device	8/16/2001
	Schwartau	Winn Schwartau, <i>LoJack for laptops</i> , NetworkWorld, 14(48):81 (Dec. 1, 1997)	12/1/1997
		AlertPC, Welcome to Alert P.C., https://web.archive.org/web/20010721085709/http://www.alertpc.com/	7/21/2001
		AlertPC, Product Info, https://web.archive.org/web/20010603063149/http://www.alertpc.com/product_info.htm	6/3/2001
		AlertPC, Pricing, https://web.archive.org/web/20010603062106/http://www.alertpc.com/pricing.htm	6/3/2001
		AlertPC, Download, https://web.archive.org/web/20010603054924/http://www.alertpc.com/download.htm	6/3/2001
CN1304264A	Zhang	Mobile phone antitheft self-explosion and over-network registration alarming method	1/13/2000
U.S. Patent No. 5,210,875	Bealkowski	Initial bios load for a personal computer system	8/25/1989
U.S. Patent No. 5,530,431	Wingard	Anti-theft device for protecting electronic equipment	4/11/1995
U.S. Patent No. 5,729,192	Badger	Remote automobile disabler device and associated method	12/1/1995

Patent	Short Name	Prior Art Reference(s)	Priority Date(s)
U.S. Patent No. 5,896,497	Halstead	System for securing a computer	8/7/1996
U.S. Patent No. 6,166,688	Cromer '688	Data processing system and method for disabling a portable computer outside an authorized area	3/31/1999
U.S. Patent No. 6,177,860	Cromer '860	Method and economical direct connected apparatus for deploying and tracking computers	11/17/1997
U.S. Patent No. 6,271,541	Cromer '541	Data processing system and method for determining a physical location of a client computer system coupled to a server via a physical network	10/8/1998
U.S. Patent No. 6,282,642	Cromer '642	System for presetting a first or second remote boot protocol by a computer remotely receiving and storing a boot parameter prior to being powered on	11/18/1998
U.S. Patent No. 6,421,792	Cromer '792	Data processing system and method for automatic recovery from an unsuccessful boot	12/3/1998
U.S. Patent No. 6,480,972	Cromer '972	Data processing system and method for permitting a server to remotely perform diagnostics on a malfunctioning client computer system	2/24/1999
U.S. Patent No. 7,069,431	Dayan '431	Recovery of a BIOS image	7/31/2001
U.S. Patent No. 7,275,160	Pearson '160	Trusted System	8/17/2001
U.S. Patent No. 7,337,309	Nguyen	Secure online BIOS update schemes	3/24/2003
U.S. Patent No. 7,490,250	Cromer '250	Method and system for detecting a tamper event in a trusted computing environment	10/26/2001
WO 00/73880	Proudlar	Data event logging in computing platform	12/7/2000
	PhoenixBIOS 4.0	PhoenixBIOS 4.0, Revision 6 User's Manual, Phoenix Technologies Ltd.	1/6/2000
U.S. Patent No. 5,537,540	Miller	Transparent, secure computer virus detection method and apparatus	9/30/1994

Patent	Short Name	Prior Art Reference(s)	Priority Date(s)
U.S. Patent No. 6,009,520	Gharda	Method and apparatus standardizing use of non-volatile memory within a BIOS-ROM	12/10/1997
U.S. Patent No. 6,244,758	Solymar	Apparatus and method for monitoring electronic devices via a global network	11/15/1994
U.S. Patent No. 6,300,863	Cotichini	Method and apparatus to monitor and locate an electronic device using a secured intelligent agent via a global network	11/15/1994
U.S. Patent No. 6,518,874	Barrus	Portable computer supporting paging functions	6/17/1998
U.S. Patent No. 5,949,882	Angelo '882	Method and apparatus for allowing access to secured computer resources by utilizing a password and an external encryption algorithm	9/7/1999
U.S. Patent No. 5,859,911	Angelo '911	Method for the secure remote flashing of the BIOS of a computer	4/16/1997
U.S. Patent No. 6,085,299	Angelo '299	Secure updating of non-volatile memory	11/19/1997
U.S. Patent No. 6,119,228	Angelo '228	Method for securely communicating remote control commands in a computer network	8/22/1997
U.S. Patent No. 6,625,729	Angelo '729	Computer system having security features for authenticating different components	3/31/2000
U.S. Patent No. 6,625,730	Angelo '730	System for validating a bios program and memory coupled therewith by using a boot block program having a validation routine	3/31/2000
U.S. Patent No. 6,633,978	Angelo '978	Method and apparatus for restoring computer resources	3/31/2000
U.S. Patent No. 7,051,196	Angelo '196	Location-based security for a portable computer	12/5/2001
U.S. Patent No. 6,643,781	Merriam	Method and apparatus for rendering stolen computing devices inoperable	5/14/1999
U.S. Patent No. 6,032,257	Olarig '257	Hardware theft-protection architecture	8/29/1997

Patent	Short Name	Prior Art Reference(s)	Priority Date(s)
U.S. Patent No. 6,886,109	Olarig '109	Method and apparatus for expediting system initialization	5/18/2001
U.S. Patent No. 6,725,379	Dailey	Stolen computer detection and protection	8/11/1999
U.S. Patent No. 6,833,787	Levi	Method and system for device tracking	5/9/2000
U.S. Patent No. 7,191,464	Cromer '464	Method and system for tracking a secure boot in a trusted computing environment	10/16/2001
U.S. Patent No. 7,203,804	Kawano	Process, apparatus, and system for passing data between partitions in a storage device	6/4/2003
U.S. Patent No. 7,366,888	Dayan '888	Bootting to a recovery/maintenance environment	6/7/2001
U.S. Patent No. 7,945,709	Cain	Security apparatus and method	10/2/2002
U.S. Patent Application No. 2003/0126462	Howard	System and method for preventing use of a wireless device	1/2/2002
U.S. Patent Application No. 2003/0153328	Booth	Method and system for tracing missing network devices using hardware fingerprints	2/14/2002
U.S. Patent Application No. 2003/0143980	Choi	Security apparatus and method for information processing device using an e-mail	4/17/2001
U.S. Patent Application No. 2002/0133702	Stevens	Methods of granting access to a protected area	3/16/2001
U.S. Patent Application No. 2002/0188837	Dayan	Bootting to a recovery/manintenance [sic] environment	6/7/2001
U.S. Patent Application	Angelo Publication	Location-based security for a portable computer	12/5/2001

Patent	Short Name	Prior Art Reference(s)	Priority Date(s)
No. 2003/0105971			
U.S. Patent Application No. 2004/0203601	Morriss	Method and apparatus for activating a restrictive operating mode of a wireless communication device	12/19/2002
WO 01/13199	Pearson	Computer platforms and their methods of operation	8/11/2000
WO 01/27770	Hamilton	Security card	10/6/2000
GB 2365544	Flanagan	Storing back-up recovery files on a hidden partition of a disk	11/15/1999
U.S. Patent No. 6,560,702	Gharda '702	Method and apparatus for execution of an application during computer pre-boot operation	6/18/1999
U.S. Patent No. 6,654,820	Ishibashi	System capable of recording a content onto a recording medium which does not have a medium ID	3/31/2000
U.S. Patent No. 6,665,778	Assaf	System and method for storage of device performance data	9/23/1999
U.S. Patent No. 6,715,074	Chaiken	Virus resistant and hardware independent method of flashing system bios	7/27/1999
U.S. Patent No. 6,725,178	Cheston	Use of hidden partitions in a storage device for storing BIOS extension files	1/15/2002
U.S. Patent Application No. 2002/0016838	Geluc	Scheme for blocking the use of lost or stolen network-connectable computer systems	12/15/2000
U.S. Patent Application No. 2004/0123019	Garney	Interacting with optional read-only memory	12/19/2002
DE4315732	Osterlehner '732	Personal computer software integrity booting and testing - conducting power-on self-test in ROM-BIOS, loading partition, loading boot sector of operating system partition, starting operating system and kernel,	5/11/1993

Patent	Short Name	Prior Art Reference(s)	Priority Date(s)
		and using one-way hash function for cryptographic key and testing	
U.S. Patent No. 6,510,512	Alexander	Method and system for executing BIOS code in secure multitasking operating environment	1/20/1999
U.S. Patent No. 6,564,318	Gharda '318	Method and apparatus for execution of an application during computer pre-boot operation and post-boot under normal OS control	6/18/1999
U.S. Patent No. 6,618,810	Dirie	Bios based method to disable and re-enable computers	5/27/1999
U.S. Patent No. 6,813,498	Durga	Apparatus, method and system for detection and recovery of missing wireless devices in communication systems	10/27/2000
U.S. Patent No. 6,880,079	Kefford	Methods and systems for secure transmission of information using a mobile device	4/25/2002
U.S. Patent No. 6,938,164	England	Method and system for allowing code to be securely initialized in a computer	11/22/2000
U.S. Patent Application No. 2002/0198993	Cudd	Downloading and uploading data in information networks	8/30/2001
U.S. Patent Application No. 2003/0088633	Chiu	System and method for remotely controlling mobile communication devices	10/28/2002
U.S. Patent Application No. 2003/0145090	Ostergaard	Method for tracing a computer connected to a data network	1/30/2002
U.S. Patent Application No. 2003/0149526	Zhou	Systems and methods for monitoring and tracking related U.S. patent applications	10/29/2001

Patent	Short Name	Prior Art Reference(s)	Priority Date(s)
U.S. Patent Application No. 2003/0154392	Lewis	Secure system firmware using interrupt generation on attempts to modify shadow RAM attributes	2/11/2002
U.S. Patent Application No. 2004/0267926	Rothman	Accessing firmware of a remote computer system using a remote firmware interface	6/26/2003
WO 03/003242	Hearn	Security system and method for computers	6/28/2002
U.S. Patent No. 5,684,875	Ellenberger	Method and apparatus for detecting a computer virus on a computer	10/21/1994
	TCPA	Trusted Computing Platform Alliance (TCPA), Main Specification Version 1.1b	2/22/2002
U.S. Patent No. 4,959,860	Watters	Power-on password functions for computer system	2/7/1989
U.S. Patent No. 5,475,839	Watson	Method and structure for securing access to a computer system	11/16/1994
U.S. Patent No. 5,564,054	Bramnick	Fail-safe computer boot apparatus and method	8/25/1994
U.S. Patent No. 5,951,686	McLaughlin	Method and system for reboot recovery	3/31/1997
U.S. Patent No. 6,804,699	Henrie	Identifying and locating lost or stolen personal digital assistant devices via a landline- or wireless-connected web server	7/18/2000
U.S. Patent Application No. 2003/0023872	Chen	Trusted platform evaluation	7/11/2002
U.S. Patent Application No. 2004/0250126	Buer	Online trusted platform module	6/3/2003
	Schmeiser	Lisa Schmeiser, <i>Software Tracks Missing Macs, Dude, Where's My Mac?</i> , Macworld, p. 37 (Sept. 2002)	9/2002

Patent	Short Name	Prior Art Reference(s)	Priority Date(s)
		PC PhoneHome, Welcome, https://web.archive.org/web/20020603213231/http://pcphonehome.com/	6/3/2002
		PC PhoneHome, Product, https://web.archive.org/web/20020604001457/http://www.pcphonehome.com/product.html	6/4/2002
		PC PhoneHome, FAQ's, https://web.archive.org/web/20020604105344/http://www.pcphonehome.com/faq.html	6/4/2002
		PC PhoneHome, Purchase, https://web.archive.org/web/20020604010226/http://www.pcphonehome.com/purchase.html	6/4/2002
		PC PhoneHome, Download, https://web.archive.org/web/20020803102904/http://www.pcphonehome.com/download.html	8/3/2002
		PC PhoneHome, Tracking, https://web.archive.org/web/20020803105341/http://www.pcphonehome.com/tracking.cgi	8/3/2002
		PC PhoneHome, News & Events, https://web.archive.org/web/20020803102711/http://www.pcphonehome.com/events.html	8/3/2002
	McNamara	Paul McNamara, <i>'Net Buzz, The latest on the Internet Industry</i> , NetworkWorld, 17(35):82 (Aug. 28, 2000)	8/28/2000
U.S. Patent Application No. 2005/0027844	Hariprasad '844	Method and system for tracking and controlling a remote device	12/4/2003
WO 02/19121	Hariprasad	Method and system for tracking and controlling a remote device	9/1/2000
	Nelson	Matthew Nelson, <i>CSS protects stolen systems</i> , InfoWorld, 19(46):57 (Nov. 17, 1997)	11/17/1997
	Girard	Kim Girard, <i>Laptop thieves beware</i> , ComputerWorld, 32(1):14 (Dec. 29, 1997/Jan. 5, 1998)	12/29/1997
	Schlesinger	Lee Schlesinger, <i>Like LoJack for Your Laptop</i> , NetworkWorld, 17(11):62 (Mar. 13, 2000)	3/13/2000

Patent	Short Name	Prior Art Reference(s)	Priority Date(s)
		Sentry Inc., The Cyber Angel, https://web.archive.org/web/20010302050409/http://www.sentryinc.com/	3/2/2001
		Sentry Inc., The Cyber Angel, DataVault Information, https://web.archive.org/web/20021117112203/http://www.sentryinc.com/dvinfo.html	11/17/2002
	Phoenix FirstWare	(see associated claim chart for list of associated references)	Before 8/23/2003
	FirstAuthority Brochure	FirstAuthority SDK Data Sheet, available at https://web.archive.org/web/20021223235340/http://www.phoenix.com/resources/firstauthority_sdk.pdf	2002
	FirstAuthority Presentation	FirstAuthority Presentation, available at https://web.archive.org/web/20021223235340/http://www.phoenix.com/resources/firstauthority_sdk+sales+032002+rev.ppt	
	FirstAuthority SDK	FirstAuthority SDK, available at https://web.archive.org/web/20021223235340/http://www.phoenix.com/en/products/firstauthority/sdk/default1.htm	2002
	Phoenix cME	Phoenix Core Managed Environment™ (cME)—The Center of Digital Life, available at https://web.archive.org/web/20030228172005/http://www.phoenix.com:80/en/solutions/phoenix+cme/default1.htm	2003
	Phoenix cME Article	Phoenix Technologies Unveils cME – News Release, available at https://web.archive.org/web/20030405043023/http://www.phoenix.com:80/en/about+phoenix/investors/news+releases/2003/feb+17,+2003.htm	2/17/2003
	Phoenix FirstWare Article	Phoenix Technologies Introduces FirstWare Rescue – News Release, available at https://web.archive.org/web/20020705181633/http://www.phoenix.com/en/about+phoenix/investors/news+releases/2002/apr+29,+2002.htm	4/29/2002
	FirstWare Connect	FirstWare Connect, available at https://web.archive.org/web/20021202123734/	2002

Patent	Short Name	Prior Art Reference(s)	Priority Date(s)
		http://www.phoenix.com:80/en/products/firstware+rescue/fw_connect.htm	
	FirstWare Connect Brochure	FirstWare Connect Brochure, available at https://web.archive.org/web/20030323132058/http://www.phoenix.com/resources/firstware_connect_ext.pdf	2002
	FirstWare Check	FirstWare Check, available at https://web.archive.org/web/20020805202129/http://www.phoenix.com:80/en/products/firstware+rescue/fwcheck.htm	2002
	FirstWare Recover	FirstWare Recover, available at https://web.archive.org/web/20020805202232/http://www.phoenix.com/en/products/firstware+rescue/fwrecover.htm	2002
	FirstWare Rescue	FirstWare Rescue, available at https://web.archive.org/web/20020805201419/http://www.phoenix.com/en/products/firstware+rescue/default.htm	2002
	FirstWare Vault	FirstWare Vault, available at https://web.archive.org/web/20020805202413/http://www.phoenix.com/en/products/firstware+rescue/fwvault.htm	2002
	FirstWare Security	FirstWare Security Solutions, available at https://web.archive.org/web/20021215105946/http://www.phoenix.com/en/solutions/security/default.htm	2002
	FirstWare Recovery	FirstWare Recovery Solutions, available at https://web.archive.org/web/20021215105928/http://www.phoenix.com/en/solutions/recovery/default.htm	2002
	FirstBIOS FAQs	FirstBIOS Frequently Asked Questions, available at https://web.archive.org/web/20021212143045/http://www.phoenix.com/resources/firstbios+faq+-+external.pdf	2002
	FirstBIOS Overview	FirstBIOS – Phoenix FirstBIOS: The Right Choice for Client PCs, available at https://web.archive.org/web/20021212143045/	2002

Patent	Short Name	Prior Art Reference(s)	Priority Date(s)
		http://www.phoenix.com/resources/firstbios%20right%20choice%20wp1.0.pdf	
	FirstBIOS POST Codes	FirstBIOS POST Codes, available at https://www.scribd.com/document/419735019/BIOS-PostCodes-Phoenix	Before 8/23/2003
	zTrace	(see associated claim chart for list of associated references)	Before 8/23/2003
	zTrace.com – Overview	zTrace.com – Overview, available at https://web.archive.org/web/20020802143350/http://www.ztrace.com:80/	Before 8/23/2003
	zTrace.com – zSecurity Suite	zTrace.com – zSecurity Suite, available at https://web.archive.org/web/20020604051951/http://www.ztrace.com:80/zSecuritySuite.asp	Before 8/23/2003
	zSecurity Suite Brochure	zSecurity Suite Brochure, available at https://web.archive.org/web/20050307101451/http://www.ztrace.com/data_sheet/zSecuritySuite.pdf	Before 8/23/2003
	zTrace.com – zTrace Gold	zTrace.com – zTrace Gold, available at https://web.archive.org/web/20020810160306/http://www.ztrace.com:80/zTraceGold.asp	Before 8/23/2003
	zTrace Gold Brochure	zTrace Gold Brochure, available at https://web.archive.org/web/20020810160306/http://www.ztrace.com/data_sheet/zTraceGold.pdf	Before 8/23/2003
	zTrace.com – zPass	zTrace.com – zPass, available at https://web.archive.org/web/20020604052039/http://www.ztrace.com:80/zPass.asp	Before 8/23/2003
	zPass Brochure	zPass Brochure, available at https://web.archive.org/web/20020604052039/http://www.ztrace.com/data_sheet/zPass.pdf	Before 8/23/2003
	zTrace.com – zEncrypt	zTrace.com – zEncrypt, available at https://web.archive.org/web/20020604050748/http://www.ztrace.com:80/zEncrypt.asp	Before 8/23/2003
	zEncrypt Brochure	zEncrypt Brochure, available at https://web.archive.org/web/20020604050748/http://www.ztrace.com/data_sheet/zEncrypt.pdf	Before 8/23/2003
	zTrace.com – zControl	zTrace.com – zControl, available at https://web.archive.org/web/20020810155003/http://www.ztrace.com:80/zControl.asp	Before 8/23/2003

Patent	Short Name	Prior Art Reference(s)	Priority Date(s)
	zControl Brochure	zControl Brochure, available at https://web.archive.org/web/20020810155003/http://www.ztrace.com/data_sheet/zControl.pdf	Before 8/23/2003
	zTrace.com – zAsset Track	zTrace.com – zAsset Track, available at https://web.archive.org/web/20020604050138/http://www.ztrace.com:80/zAssetTrack.asp	Before 8/23/2003
	zAsset Track Brochure	zAsset Track Brochure, available at https://web.archive.org/web/20020604050138/http://www.ztrace.com/data_sheet/zAssetTrack.pdf	Before 8/23/2003
	zTrace.com – Why You Need It	zTrace.com – Why Do You Need It?, available at https://web.archive.org/web/20020613180259/http://www.ztrace.com:80/zTraceWhy.asp	Before 8/23/2003
	zTrace.com – FAQ	zTrace.com – FAQ, available at https://web.archive.org/web/20020405211735/http://www.ztrace.com:80/faq.asp	Before 8/23/2003
	zTrace.com – Individual Version	zTrace.com – Individual Version, available at https://web.archive.org/web/20051126232534/http://www.ztrace.com/screen1.asp	Before 8/23/2003
	zTrace.com – zGuarantee	zTrace.com – zGuarantee, available at https://web.archive.org/web/20021002045822/http://www.ztrace.com:80/guarantee.asp	Before 8/23/2003
	zTrace.com – Special Deals	zTrace.com – Special Deals, available at https://web.archive.org/web/20020606100347/http://www.ztrace.com/Corporate.asp	Before 8/23/2003
	HP zTrace	HP zTrace, available at https://web.archive.org/web/20120126160111/http://www.ztrace.com/sites/hp_ztrace_dsheets.pdf	Before 8/23/2003
	zTrace.com – How It Works	zTrace.com – How Does It Work?, available at https://web.archive.org/web/20020814065623/http://www.ztrace.com:80/zTraceHow.asp	Before 8/23/2003
	zTrace.com – Mission & Vision	zTrace.com – Mission & Vision, available at https://web.archive.org/web/20020604025540/http://www.ztrace.com:80/AboutzTrace.asp	Before 8/23/2003
	Computrace	(see associated claim chart for list of associated references)	Before 8/23/2003
	Absolute Software Homepage	Absolute Software Homepage, available at https://web.archive.org/web/20020804231524/http://www.absolute.com/public/Main/default.asp	Before 8/23/2003

Patent	Short Name	Prior Art Reference(s)	Priority Date(s)
	Absolute Software Corporate Backgrounder	Absolute Software – Corporate Backgrounder, available at https://web.archive.org/web/20020805165341/http://www.absolute.com/public/about/overview.asp	Before 8/23/2003
	Absolute Software History	Absolute Software History in PC Security, available at https://web.archive.org/web/20020804234619/http://www.absolute.com/public/products/default.asp	Before 8/23/2003
	Absolute Software Start	Absolute Software – Customer Start Here, available at https://web.archive.org/web/20020805143159/http://www.absolute.com/public/main/login.asp	Before 8/23/2003
	Absolute Software Theft Report	Absolute Software – Report a Theft, available at https://web.archive.org/web/20021015185104/http://absolute.com/public/Main/reporttheft.asp	Before 8/23/2003
	AbsoluteTrack Introduction	AbsoluteTrack: Introduction, available at https://web.archive.org/web/20020804233718/http://www.absolute.com/public/products/absolutetrack.asp	Before 8/23/2003
	Dell Services	Dell Services Introduces New Mobility Bundle and Virtual Tour, available at https://web.archive.org/web/20020804231317/http://www.absolute.com/PDF/dell_services.htm	Before 8/23/2003
	Dell Mobility Services	Protect your notebook investment with Dell Mobility Services, available at https://web.archive.org/web/20020826032925/http://dell.webjackmorton.com/mobile/index.asp?seg=SB	Before 8/23/2003
	AbsoluteTrack Benefits	AbsoluteTrack: Benefits, available at https://web.archive.org/web/20020805144524/http://www.absolute.com/public/products/absolutetrack_benefits.asp	Before 8/23/2003
	AbsoluteTrack Description	AbsoluteTrack: Description, available at https://web.archive.org/web/20020805145723/http://www.absolute.com/public/products/absolutetrack_description.asp	Before 8/23/2003
	AbsoluteTrack FAQs	AbsoluteTrack FAQs available at, https://web.archive.org/web/20020805145239/http://www.absolute.com/public/products/absolutetrack_faqs.asp	Before 8/23/2003

Patent	Short Name	Prior Art Reference(s)	Priority Date(s)
	AbsoluteTrack Brochure	AbsoluteTrack Brochure, available at https://web.archive.org/web/20020805145012/http://www.absolute.com/PDF/AbsoluteTrackBrochure.pdf	Before 8/23/2003
	AbsoluteTrack Whitepaper	AbsoluteTrack Whitepaper, available at https://web.archive.org/web/20020804235431/http://www.absolute.com/PDF/AbsoluteTrack_WP.pdf	Before 8/23/2003
	ComputracePlus Introduction	ComputracePlus: Introduction, available at https://web.archive.org/web/20020804235030/http://www.absolute.com/public/products/computraceplus.asp	Before 8/23/2003
	ComputracePlus Benefits	ComputracePlus: Benefits, available at https://web.archive.org/web/20020805145634/http://www.absolute.com:80/public/products/computraceplus_benefits.asp	Before 8/23/2003
	ComputracePlus Description	ComputracePlus: Description, available at https://web.archive.org/web/20020805145945/http://www.absolute.com:80/public/products/computraceplus_description.asp	Before 8/23/2003
	Pricing	Absolute Software Pricing Information, available at https://web.archive.org/web/20020804235050/http://www.absolute.com/public/purchase/default.asp	Before 8/23/2003
	ComputracePlus FAQs	ComputracePlus: FAQs, available at https://web.archive.org/web/20020805162731/http://www.absolute.com/public/products/computraceplus_faqs.asp	Before 8/23/2003
	ComputracePlus Brochure	ComputracePlus Brochure, available at https://web.archive.org/web/20031207070027/http://www.absolute.com/PDF/ComputracePlusBrochure.pdf	Before 8/23/2003
	TheftGuard	(see associated claim chart for list of associated references)	Before 8/23/2003
	Phoenix TheftGuard Press Release	Phoenix Technologies' TheftGuard Press Release, available at https://web.archive.org/web/20030716041218/http://investor.phoenix.com:80/en/about+phoenix/investors/news+releases/ReleaseDetail.cfm?ReleaseID=112560&Year=2003	5/27/2003

Patent	Short Name	Prior Art Reference(s)	Priority Date(s)
	Computer World TheftGuard Article	Computer World's TheftGuard Article, available at https://web.archive.org/web/20230622001352/https://www.computerworld.com/article/2570229/brief-companies-partner-to-stop-pc-theft.html	5/27/2003
	PCWorld.com TheftGuard Article	PCWorld.com's TheftGuard Article, available at https://web.archive.org/web/20030602174436/http://pcworld.com/news/article/0%2Caid%2C110883%2C00.asp	5/27/2003
	CNET TheftGuard Article	CNET's TheftGuard Article, available at https://www.cnet.com/tech/services-and-software/firms-offer-software-to-prevent-pc-theft/	5/30/2003
	CRN article	https://web.archive.org/web/20220420012756/https://www.crn.com/news/channel-programs/18822710/new-bios-technology-to-trace-and-disable-stolen-pcs.htm	5/27/2003
	AMIBIOS	(see associated claim chart for list of associated references)	Before 8/23/2003
	AMIBIOS Product Descriptions	AMIBIOS Product Descriptions, available at https://web.archive.org/web/20020805210756/http://www.ami.com/products/subpage.cfm?CatID=6&SubID=14	2000
	AMIBIOS8 Description	AMIBIOS8 Description, available at https://web.archive.org/web/20020806125245/http://www.ami.com/products/product.cfm?ProdID=127&CatID=6&SubID=14	2000
	AMIBIOS8 Brochure	AMIBIOS8 Brochure, available at https://web.archive.org/web/20030308125808/http://www.ami.com/support/doc/AMIBIO8Brochure.pdf	2001
	T13	T13 D1367, Information Technology - Protected Area Run Time Interface Extension Services, available at https://web.archive.org/web/20030315044257/http://www.t13.org/project/d1367r3.pdf	8/23/1999
	T13 D1386	T13 D1386, Information Technology - BIOS Enhanced Disk Drive Services (EDD), available at https://web.archive.org/web/20030315103746/http://www.t13.org/project/d1386r5a.pdf	6/21/1999

Patent	Short Name	Prior Art Reference(s)	Priority Date(s)
	ACPI 2.0	Advanced Configuration and Power Interface Specification, Revision 2.0, https://uefi.org/sites/default/files/resources/ACPI_2.pdf	2/1999
	AMIBIOS8 Flash Update	AMIBIOS8 Flash Update & BIOS Recovery Methods, available at https://web.archive.org/web/20230624185542/https://forums.futura-sciences.com/attachments/materiel-hardware/58894d1225034379-flash-bios-rate-amibios8_flash_recovery_whitepaper_v10.pdf	Before 8/23/2003
	AMIBIOS8 Whitepaper	Introduction to AMIBIOS8, available at https://www.scribd.com/document/51748486/Ami-Whitepaper	11/5/2001
	AMIBIOS Flash Utility	AMIBIOS Flash Utility, available at https://web.archive.org/web/20030403192214/http://www.ami.com/support/dlcenter/amiflash.zip	Before 8/23/2003
	AMIBIOS8 Codes	AMIBIOS8 Check Point and Beep Code List, available at https://www.scribd.com/document/88420278/Amibios-Codes	5/7/2002
	AMIBIOS ROM Utilities	AMIBIOS8 ROM Utilities: User Guide, Revision 1.29, available at https://www.scribd.com/document/79351607/AMIBIOS-ROM-Utilities-User-Guide	Before 8/23/2003
	Tait	Carl Tait et al., <i>Intelligent File Hoarding for Mobile Computers</i> , MOBICOM 95, pp. 119-125	1995
	Win2K SRK	Microsoft Windows 2000 Resource Kit	2000
	BB 5810 Getting Started Guide	Blackberry Wireless Handheld Getting Started Guide for BlackBerry 5810 and 5820	1/15/2003
	BES Admin Guide	BlackBerry Enterprise Server for Microsoft Exchange, Version 3.5 Service Pack 1, Administration Guide	10/30/2002
	BB 5800 Series User's Guide	BlackBerry Wireless Handheld User Guide for the BlackBerry 5810 and 5820 models	2/4/2003
	BES Datasheet	BlackBerry Enterprise Server for Microsoft Exchange Technical Datasheet	2003
	RIM User's Guide	BlackBerry Wireless Handheld User's Guide for the RIM 850, 857, 950, and 957 models	4/30/2003

Patent	Short Name	Prior Art Reference(s)	Priority Date(s)
		Research In Motion Delivers Wearable Wireless Device Based on Embedded Intel Architecture, Press Release http://web.archive.org/web/20011109195406/http://rim.com/news/press/1999/pr-19_01_1999-02.shtml	
		Technical Specifications, https://web.archive.org/web/20020203055155/http://www.rim.com/products/handhelds/specifications/index.shtml	
		BlackBerry 5810 Wireless Handheld, https://web.archive.org/web/20021216002908/http://www.blackberry.com:80/products/handhelds/blackberry5810.shtml	
		RIM Introduces Java-Based BlackBerry Handheld With Integrated Phone for GSM/GPRS Networks in North America, BlackBerry Press Release, https://web.archive.org/web/20040803093840/http://www.blackberry.com/news/press/2002/pr-04_03_2002-01.shtml	
WIPO Patent Publication No. 01/84455	Andrews	Portable computing device communication system and method	11/8/2001
U.S. Patent Application Publication No. 2003/0074577	Bean	Return-to-owner security lockout for a portable electronic device	10/17/2001
U.S. Patent Publication No. 2003/0051090	Bonnett	Apparatus and method for secure program upgrade	9/10/2001
US 7,134,006	Flanigan	Method and system for changing software access level within or outside a host protected area	6/3/2003
GB 2,369,205	Hayward	Personal data device and protection system with deletion of contents	5/22/2002
U.S. Patent No. 6,662,023	Helle	Method and apparatus for controlling and securing mobile phones that are lost, stolen or misused	7/6/2000

Patent	Short Name	Prior Art Reference(s)	Priority Date(s)
U.S. Patent Application Publication No. 2003/0126462	Howard	System and method for preventing use of a wireless device	1/2/2002
US 2003/0005244	Markkanen	Method and arrangement for securing a digital data file having financial value, terminal operating in the arrangement, and software application employing the method	6/27/2002

APPENDIX B

A. '837 Patent

Exhibit No.	Prior Art Reference
A-1	U.S. Patent No. 7,590,837 vs. AMIBIOS
A-2	U.S. Patent No. 7,590,837 vs. Angelo '729
A-3	U.S. Patent No. 7,590,837 vs. Angelo '978
A-4	U.S. Patent No. 7,590,837 vs. Angelo Publication
A-5	U.S. Patent No. 7,590,837 vs. Assaf
A-6	U.S. Patent No. 7,590,837 vs. Barrus
A-7	U.S. Patent No. 7,590,837 vs. Britt
A-8	U.S. Patent No. 7,590,837 vs. Cheston
A-9	U.S. Patent No. 7,590,837 vs. Choi
A-10	U.S. Patent No. 7,590,837 vs. Computrace
A-11	U.S. Patent No. 7,590,837 vs. Cotichini
A-12	U.S. Patent No. 7,590,837 vs. Dayan
A-13	U.S. Patent No. 7,590,837 vs. Hamilton
A-14	U.S. Patent No. 7,590,837 vs. Hariprasad
A-15	U.S. Patent No. 7,590,837 vs. Henrie
A-16	U.S. Patent No. 7,590,837 vs. Isikoff
A-17	U.S. Patent No. 7,590,837 vs. Miller
A-18	U.S. Patent No. 7,590,837 vs. Morriss
A-19	U.S. Patent No. 7,590,837 vs. Pearson
A-20	U.S. Patent No. 7,590,837 vs. Phoenix FirstWare
A-21	U.S. Patent No. 7,590,837 vs. PhoenixBIOS
A-22	U.S. Patent No. 7,590,837 vs. Solymar
A-23	U.S. Patent No. 7,590,837 vs. Stevens
A-24	U.S. Patent No. 7,590,837 vs. Tait
A-25	U.S. Patent No. 7,590,837 vs. TheftGuard
A-26	U.S. Patent No. 7,590,837 vs. zTrace

B. '710 Patent

Exhibit No.	Prior Art Reference
B-1	U.S. Patent No. 8,128,710 vs. AMIBIOS
B-2	U.S. Patent No. 8,128,710 vs. Angelo '729
B-3	U.S. Patent No. 8,128,710 vs. Angelo '978
B-4	U.S. Patent No. 8,128,710 vs. Angelo Publication
B-5	U.S. Patent No. 8,128,710 vs. Assaf

Exhibit No.	Prior Art Reference
B-6	U.S. Patent No. 8,128,710 vs. Barrus
B-7	U.S. Patent No. 8,128,710 vs. Britt
B-8	U.S. Patent No. 8,128,710 vs. Cheston
B-9	U.S. Patent No. 8,128,710 vs. Choi
B-10	U.S. Patent No. 8,128,710 vs. Computrace
B-11	U.S. Patent No. 8,128,710 vs. Cotichini
B-12	U.S. Patent No. 8,128,710 vs. Dayan
B-13	U.S. Patent No. 8,128,710 vs. Hamilton
B-14	U.S. Patent No. 8,128,710 vs. Hariprasad
B-15	U.S. Patent No. 8,128,710 vs. Henrie
B-16	U.S. Patent No. 8,128,710 vs. Isikoff
B-17	U.S. Patent No. 8,128,710 vs. Miller
B-18	U.S. Patent No. 8,128,710 vs. Morriss
B-19	U.S. Patent No. 8,128,710 vs. Pearson
B-20	U.S. Patent No. 8,128,710 vs. Phoenix FirstWare
B-21	U.S. Patent No. 8,128,710 vs. PhoenixBIOS
B-22	U.S. Patent No. 8,128,710 vs. Solymar
B-23	U.S. Patent No. 8,128,710 vs. Stevens
B-25	U.S. Patent No. 8,128,710 vs. TheftGuard
B-26	U.S. Patent No. 8,128,710 vs. zTrace
B-27	U.S. Patent No. 8,128,710 vs. Geluc

C. '410 Patent

Exhibit No.	Prior Art Reference
C-1	U.S. Patent No. 8,137,410 vs. AMIBIOS
C-2	U.S. Patent No. 8,137,410 vs. Angelo '729
C-3	U.S. Patent No. 8,137,410 vs. Angelo '978
C-4	U.S. Patent No. 8,137,410 vs. Angelo Publication
C-5	U.S. Patent No. 8,137,410 vs. Assaf
C-7	U.S. Patent No. 8,137,410 vs. Britt
C-8	U.S. Patent No. 8,137,410 vs. Cheston
C-9	U.S. Patent No. 8,137,410 vs. Choi
C-10	U.S. Patent No. 8,137,410 vs. Computrace
C-11	U.S. Patent No. 8,137,410 vs. Cotichini
C-12	U.S. Patent No. 8,137,410 vs. Dayan
C-13	U.S. Patent No. 8,137,410 vs. Hamilton
C-14	U.S. Patent No. 8,137,410 vs. Hariprasad

Exhibit No.	Prior Art Reference
C-15	U.S. Patent No. 8,137,410 vs. Henrie
C-17	U.S. Patent No. 8,137,410 vs. Miller
C-18	U.S. Patent No. 8,137,410 vs. Morris
C-19	U.S. Patent No. 8,137,410 vs. Pearson
C-20	U.S. Patent No. 8,137,410 vs. Phoenix FirstWare
C-21	U.S. Patent No. 8,137,410 vs. PhoenixBIOS
C-22	U.S. Patent No. 8,137,410 vs. Solymar
C-23	U.S. Patent No. 8,137,410 vs. Stevens
C-25	U.S. Patent No. 8,137,410 vs. TheftGuard
C-26	U.S. Patent No. 8,137,410 vs. zTrace
C-42	U.S. Patent No. 8,137,410 vs. Bramnick
C-43	U.S. Patent No. 8,137,410 vs. McLaughlin
C-44	U.S. Patent No. 8,137,410 vs. Watson

D. '892 Patent

Exhibit No.	Prior Art Reference
D-1	U.S. Patent No. 8,145,892 vs. AMIBIOS
D-2	U.S. Patent No. 8,145,892 vs. Angelo '729
D-3	U.S. Patent No. 8,145,892 vs. Angelo '978
D-4	U.S. Patent No. 8,145,892 vs. Angelo Publication
D-5	U.S. Patent No. 8,145,892 vs. Assaf
D-7	U.S. Patent No. 8,145,892 vs. Britt
D-8	U.S. Patent No. 8,145,892 vs. Cheston
D-9	U.S. Patent No. 8,145,892 vs. Choi
D-10	U.S. Patent No. 8,145,892 vs. Computrace
D-11	U.S. Patent No. 8,145,892 vs. Cotichini
D-12	U.S. Patent No. 8,145,892 vs. Dayan
D-13	U.S. Patent No. 8,145,892 vs. Hamilton
D-14	U.S. Patent No. 8,145,892 vs. Hariprasad
D-15	U.S. Patent No. 8,145,892 vs. Henrie
D-17	U.S. Patent No. 8,145,892 vs. Miller
D-18	U.S. Patent No. 8,145,892 vs. Morriss
D-19	U.S. Patent No. 8,145,892 vs. Pearson
D-20	U.S. Patent No. 8,145,892 vs. Phoenix FirstWare
D-21	U.S. Patent No. 8,145,892 vs. PhoenixBIOS
D-22	U.S. Patent No. 8,145,892 vs. Solymar
D-23	U.S. Patent No. 8,145,892 vs. Stevens

Exhibit No.	Prior Art Reference
D-25	U.S. Patent No. 8,145,892 vs. TheftGuard
D-26	U.S. Patent No. 8,145,892 vs. zTrace

E. '603 Patent

Exhibit No.	Prior Art Reference
E-1	U.S. Patent No. 8,287,603 vs. AMIBIOS
E-2	U.S. Patent No. 8,287,603 vs. Angelo '729
E-4	U.S. Patent No. 8,287,603 vs. Angelo Publication
E-6	U.S. Patent No. 8,287,603 vs. Barrus
E-7	U.S. Patent No. 8,287,603 vs. Britt
E-9	U.S. Patent No. 8,287,603 vs. Choi
E-10	U.S. Patent No. 8,287,603 vs. Computrace
E-11	U.S. Patent No. 8,287,603 vs. Cotichini
E-12	U.S. Patent No. 8,287,603 vs. Dayan
E-13	U.S. Patent No. 8,287,603 vs. Hamilton
E-14	U.S. Patent No. 8,287,603 vs. Hariprasad
E-15	U.S. Patent No. 8,287,603 vs. Henrie
E-16	U.S. Patent No. 8,287,603 vs. Isikoff
E-17	U.S. Patent No. 8,287,603 vs. Miller
E-18	U.S. Patent No. 8,287,603 vs. Morriss
E-19	U.S. Patent No. 8,287,603 vs. Pearson
E-20	U.S. Patent No. 8,287,603 vs. Phoenix FirstWare
E-21	U.S. Patent No. 8,287,603 vs. PhoenixBIOS
E-22	U.S. Patent No. 8,287,603 vs. Solymar
E-23	U.S. Patent No. 8,287,603 vs. Stevens
E-25	U.S. Patent No. 8,287,603 vs. TheftGuard
E-26	U.S. Patent No. 8,287,603 vs. zTrace
E-28	U.S. Patent No. 8,287,603 vs. Cromer '464
E-29	U.S. Patent No. 8,287,603 vs. Dailey
E-30	U.S. Patent No. 8,287,603 vs. Kesler
E-31	U.S. Patent No. 8,287,603 vs. Levi

F. '649 Patent

Exhibit No.	Prior Art Reference
F-1	U.S. Patent No. 8,506,649 vs. AMIBIOS
F-2	U.S. Patent No. 8,506,649 vs. Angelo '729
F-4	U.S. Patent No. 8,506,649 vs. Angelo Publication

Exhibit No.	Prior Art Reference
F-6	U.S. Patent No. 8,506,649 vs. Barrus
F-7	U.S. Patent No. 8,506,649 vs. Britt
F-8	U.S. Patent No. 8,506,649 vs. Cheston
F-9	U.S. Patent No. 8,506,649 vs. Choi
F-10	U.S. Patent No. 8,506,649 vs. Computrace
F-11	U.S. Patent No. 8,506,649 vs. Cotichini
F-12	U.S. Patent No. 8,506,649 vs. Dayan
F-13	U.S. Patent No. 8,506,649 vs. Hamilton
F-14	U.S. Patent No. 8,506,649 vs. Hariprasad
F-15	U.S. Patent No. 8,506,649 vs. Henrie
F-16	U.S. Patent No. 8,506,649 vs. Isikoff
F-17	U.S. Patent No. 8,506,649 vs. Miller
F-18	U.S. Patent No. 8,506,649 vs. Morriss
F-19	U.S. Patent No. 8,506,649 vs. Pearson
F-20	U.S. Patent No. 8,506,649 vs. Phoenix FirstWare
F-21	U.S. Patent No. 8,506,649 vs. PhoenixBIOS
F-22	U.S. Patent No. 8,506,649 vs. Solymar
F-23	U.S. Patent No. 8,506,649 vs. Stevens
F-25	U.S. Patent No. 8,506,649 vs. TheftGuard
F-26	U.S. Patent No. 8,506,649 vs. zTrace
F-29	U.S. Patent No. 8,506,649 vs. Dailey
F-30	U.S. Patent No. 8,506,649 vs. Kesler
F-31	U.S. Patent No. 8,506,649 vs. Levi
F-32	U.S. Patent No. 8,506,649 vs. Andrews
F-33	U.S. Patent No. 8,506,649 vs. Bean
F-34	U.S. Patent No. 8,506,649 vs. BlackBerry
F-35	U.S. Patent No. 8,506,649 vs. Bonnett
F-36	U.S. Patent No. 8,506,649 vs. Flanigan
F-37	U.S. Patent No. 8,506,649 vs. Hayward
F-38	U.S. Patent No. 8,506,649 vs. Helle
F-39	U.S. Patent No. 8,506,649 vs. Howard
F-40	U.S. Patent No. 8,506,649 vs. Markkanen
F-45	U.S. Patent No. 8,506,649 vs. Windows

G. '235 Patent

Exhibit No.	Prior Art Reference
G-1	U.S. Patent No. 8,516,235 vs. AMIBIOS

Exhibit No.	Prior Art Reference
G-2	U.S. Patent No. 8,516,235 vs. Angelo '729
G-3	U.S. Patent No. 8,516,235 vs. Angelo '978
G-4	U.S. Patent No. 8,516,235 vs. Angelo Publication
G-5	U.S. Patent No. 8,516,235 vs. Assaf
G-6	U.S. Patent No. 8,516,235 vs. Barrus
G-7	U.S. Patent No. 8,516,235 vs. Britt
G-8	U.S. Patent No. 8,516,235 vs. Cheston
G-9	U.S. Patent No. 8,516,235 vs. Choi
G-10	U.S. Patent No. 8,516,235 vs. Computrace
G-11	U.S. Patent No. 8,516,235 vs. Cotichini
G-12	U.S. Patent No. 8,516,235 vs. Dayan
G-13	U.S. Patent No. 8,516,235 vs. Hamilton
G-14	U.S. Patent No. 8,516,235 vs. Hariprasad
G-15	U.S. Patent No. 8,516,235 vs. Henrie
G-17	U.S. Patent No. 8,516,235 vs. Miller
G-18	U.S. Patent No. 8,516,235 vs. Morriss
G-19	U.S. Patent No. 8,516,235 vs. Pearson
G-20	U.S. Patent No. 8,516,235 vs. Phoenix FirstWare
G-21	U.S. Patent No. 8,516,235 vs. PhoenixBIOS
G-22	U.S. Patent No. 8,516,235 vs. Solymar
G-23	U.S. Patent No. 8,516,235 vs. Stevens
G-25	U.S. Patent No. 8,516,235 vs. TheftGuard
G-26	U.S. Patent No. 8,516,235 vs. zTrace
G-41	U.S. Patent No. 8,516,235 vs. Gharda

CERTIFICATE OF SERVICE

I hereby certify that, on June 29, 2023, all counsel of record who have appeared in this case are being served with a copy of the foregoing via electronic mail.

/s/ Dustin M. Knight
Dustin Knight
COOLEY LLP
11951 Freedom Drive, 16th Floor
Reston, VA 20190
(703) 456-8000