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

SOFTEX LLC **Plaintiff,** **vs.** **LENOVO (SHANGHAI) ELECTRONICS TECHNOLOGY CO. LTD., LENOVO GROUP, LTD., LENOVO BEIJING, LTD., LENOVO PC HK LIMITED, AND LENOVO (UNITED STATES), INC.,** **Defendants.**	**Civil Action No. 1:22-cv-01310** **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Softex LLC ("Plaintiff") files this Complaint against Lenovo (Shanghai) Electronics Technology Co. Ltd., Lenovo Group, Ltd., Lenovo Beijing, Ltd., Lenovo PC HK Limited, and Lenovo (United States), Inc. (collectively, "Lenovo" or "Defendants") and alleges as follows:

PARTIES

1. Plaintiff Softex LLC is a Delaware limited liability company having its principal place of business at 9300 Jollyville Road, Suite 201, Austin, Texas 78759.

2. Softex LLC is the owner by assignment of U.S. Patent Nos. 7,590,837 ("the '837 Patent"), 8,516,235 ("the '235 Patent"), 8,145,892 ("the '892 Patent"), 8,287,603 ("the '603 Patent"), 8,506,649 ("the '649 Patent"), 8,137,410 ("the '410 Patent"), and 8,128,710 ("the '710 Patent") (collectively "the Asserted Patents").

3. Softex, Inc. is the original named assignee to the Asserted Patents. Softex, Inc. was founded in 1992 by Mahendra Bhansali and current CEO Apurva Bhansali with a mission to

provide innovative security-focused software products and solutions for computing devices. Softex, Inc. has established itself as one of the top security solution providers with disruptive products focused on persistent theft detection security, enterprise single sign on, identity and access management, and data protection of self-encrypting drives. Softex, Inc. pioneered a class of theft prevention and recovery software that is embedded on Basic Input/Output System (BIOS) chips and/or non-viewable portions of hard disk drives at the point of manufacture, and Softex, Inc. holds many patents directly related to this technology. Softex, Inc.'s persistent theft detection security software, including "TheftGuard," competed for some time with products sold by Absolute Software Corp. and Absolute Software, Inc. (collectively "Absolute") that offered functionality that mirrored Softex, Inc.'s patented technology.

4. Defendant Lenovo Group, Ltd. ("Lenovo Group") is a company organized under the laws of the People's Republic of China, with its principal place of business at Lincoln House, 23rd Floor, Taikoo Place, 979 King's Road, Quarry Bay, Hong Kong, China.

5. Defendant Lenovo (Shanghai) Electronics Technology Co. Ltd. is a company organized under the laws of the People's Republic of China, with its principal place of business at Wai Gao Qiao Free Trade Zone, 199 Fenju Road, No. 68 Building, Shanghai, China 200131. Lenovo (Shanghai) Electronics Technology Co. Ltd. operates as a subsidiary of Lenovo Group.

6. Defendant Beijing, Ltd. is a company organized under the laws of the People's Republic of China, with its principal place of business at Lenovo Building, 6 Chuangye Rd, Shangdi Haidian District, Beijing, China 100085. Lenovo Beijing, Ltd. operates as a subsidiary of Lenovo Group.

7. Defendant Lenovo PC HK Limited is a company organized under the laws of the People's Republic of China, with its principal place of business at Lincoln House, 23rd Floor,

Taikoo Place, 979 King's Road, Quarry Bay, Hong Kong, China. Lenovo PC HK Limited operates as a subsidiary of Lenovo Group.

8. Defendant Lenovo (United States), Inc. is a company organized under the laws of the Delaware, with its principal place of business at 1009 Think Place, Morrisville, NC 27560. Lenovo (United States), Inc. operates as a subsidiary of Lenovo Group. Lenovo advertises positions on its LinkedIn Profile available in Austin, and distributes, markets, and sells electronic devices in the United States. Upon information and belief, Lenovo (United States), Inc. is authorized to do business in Texas where it can be served with process through its registered agent CT Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201-3136.

9. On information and belief, Lenovo owns and controls the internet domain "lenovo.com." Lenovo directly and/or indirectly develops, designs, manufactures, uses, distributes, markets, tests, offers to sell, and/or sells software that implements the Asserted Patents in the United States, including in this district, and otherwise purposefully directs infringing activities to this district in connection with its software.

10. Lenovo has placed or contributed to placing infringing products like its infringing software and computers with Microsoft Windows' Find My Device (and similar technology) (collectively "Windows Functionality"), Absolute Home & Office, Absolute Computrace Persistence, Absolute LoJack, LoJack for Laptops, and Computrace software (collectively "Absolute Functionality") into the stream of commerce via an established distribution channel knowing or understanding that such products would be sold and used in the United States, including in the Western District of Texas. On information and belief, Lenovo also has derived substantial revenues from infringing acts in the Western District of Texas, including from the sale

and use of infringing products like its infringing software and computers using infringing software, including Windows Functionality and Absolute Functionality.

11. "Absolute delivers security and protection for your digital data and devices in case of loss or theft. Its products, such as Absolute Home & Office, can help you locate, control, and access your device if it's stolen or misplaced. With so much important personal and business information stored digitally on our devices, it's important to keep it all safe and protected. Lenovo proudly offers Absolute products among our broad selection of PC accessories and small tech items. Among these is Absolute Home & Office, an easy-to-use, feature-packed software solution. Not only can it help you access your devices, it can help you recover them with location tracking. Whether you're seeking to protect your personal laptop, your office computer, or a group of business devices, you owe it to yourself to consider products from Absolute." https://www.lenovo.com/us/en/d/accessories/absolute/?orgRef=https%253A%252F%252Fwww.google.com%252F.

12. "Absolute is a part of Lenovo ThinkShield® — a comprehensive end-to-end security platform. It begins on the factory floor, when Lenovo embeds Absolute in the firmware of its devices. This creates an unbreakable link that gives IT and security professionals unprecedented control. Automatically heal broken controls. Gather hundreds of data points per device. Protect sensitive and valuable data. Exclusively on Lenovo devices, use Lenovo RSVP to create, change, or remove the supervisor password remotely and at scale. Lenovo and Absolute make it possible to streamline security and IT asset management. So you can protect your devices, data, apps, and budget." https://www.absolute.com/partners/device-manufacturers/lenovo/.

13. "The Lenovo X1 family and Lenovo ThinkPad T14s are part of an exclusive group of premium devices with hardware protected visibility and resilience, making them the most secure

laptops in the world right out of the box. Additionally, Lenovo Security Assurance leverages Absolute technology in the firmware of these premium Lenovo devices to fortify critical security applications through self-healing technology." https://www.absolute.com/partners/lenovo/lsa/. "Lenovo Security Assurance, powered by Absolute, allows you to defend data privacy, update and self-heal cybersecurity applications, ensure protection is in place to prevent a data breach, and provide remote supervisor password (RSVP) that allows admins to set the firmware's supervisor password remotely as needed. Security Assurance is a Lenovo X1 family and Lenovo ThinkPad T14s exclusive that's ready to use with a single activation right out of the box." *Id*.

14. Exemplary infringing products include, but are not limited to, the following products, which are collectively referred to as "Accused Products":

- Computers and devices that utilize the accused Windows Functionality, including computers and devices that utilize the Windows 10, Windows 10 IoT, Windows 10 Home, Windows 10 Pro, Windows 11, Windows 11 Pro, and Windows 11 Home operating systems.

- Computers and devices (including those in development after the time of filing this Complaint) that utilize the accused Absolute Functionality including:

Notebooks & Tablets	Models
Essentials	B40-30, B40-45, B40-80, B430, B4450s, B480, B490, B50-45, B560, B580, B590, E49, G40-80, K49, K490s, M4400, M490, M490s, M495, V110, V310, V330, V340, V480, V490, V490u, V510, V510z, V580, V580c
IdeaPad	100, 110, 300, 310, 310 TOUCH, 305, 320, 320 TOUCH, 320C, 330, 500, 510, 510S, 520, 720S, 3000, 3105, D330, Duet 3, FLEX 4, Flex 14, FLEX 15, MIIX 320, MIIX 520, MIIX 700, N580, N581, P580, P585, S10, S10e, S205S, S206, S300, S310, S400, S410, S400 Touch, S540, S9e, U160, U260, U300(s), U310, U310 Touch, U330P, U330 Touch, U430P, U430 Touch, U400, U410, U410 Touch, U430 Touch, U510, U530 Touch, V130, V330, Y400, Y410P, V460, Y480, Y510p, Y580, Y700, Yoga 11, Yoga 11S, Yoga 13, YOGA 2 PRO, Yoga 900, Yoga 910, Z410, Z460, Z465, Z510, Z560, Z565
ThinkPad	10 1st GEN, 10 2ND GEN, 11E 1st GEN, 11E 2ND GEN, 11E 3RD GEN, 11E 4TH GEN, 11E 5TH GEN, 11E YOGA GEN 6, 13 1ST GEN, 13 2ND GEN, 13 3RD GEN, YOGA 370, ThinkPad 25

ThinkPad A Series	A275, A285, A475, A485
Thinkpad Edge Series / E Series	E13, E14, E14 GEN 2, E14 GEN 3, E14 GEN 4, E15, E15 GEN 2, E15 GEN 3, E10, E120, E125, E130, E135, E145, E220s, E30, E31, E320, E325, E330, E335, E40, E420, E420s, E425, E430, E430c, E431, E435, E440, E445, E450, E450c, E455, E460, E465, E470, E470c, E475, E480, E485, E49, E490, E490s,E495, E50, E520, E525, E530, E530(c), E531, E535, E540, E545, E550, E550c, E555, E560, E565, E570, E570c, E575, E580, E585, E590, E595, HELIX GEN 2, S230u, S430, Twist
ThinkPad G Series	G460, G40, G470, G480, G50, G550, G560, G570, G580, G780
ThinkPad L Series	L13 GEN 1, L13 GEN 2, L13 GEN 2A, L13 YOGA GEN1, L13 YOGA GEN 2, L14 GEN 1, L14 GEN 2, L14 GEN 2A, L14 GEN 3, L15 GEN 1, L15 GEN 2, L15 GEN 2A, L14 GEN 3, L330, L380, L380 Yoga, L390, L390 Yoga, L410, L411, L412, L420, L421, L430, L440, L450, L460, L470, L480, L490, L510, L512, L520, L530, L540, L560, L570, L580, L590
ThinkPad P Series	P1, P1 GEN 2, P1 GEN 3, P1 GEN 4i, P14S GEN 1, P14S GEN 2, P15 GEN 1, P15S GEN 1, P15 GEN 2, P15S GEN 2, P15V GEN 1, P15V GEN 2, P17 GEN 1, P17 GEN 2, P40 YOGA
ThinkPad Mobile Workstation	P1, P40, P43s, P50, P50s, P51, P51s, P52, P52s, P53, P53s, P70, P71, P72, P73, W500, W510, W520, W530, W540, W541, W550s, W700, W700ds, W701, W701ds
ThinkPad R Series	R400, R480, R500, R51e, R52, R60, R60e, R61, R61e, R61i
ThinkPad SL Series	SL300, SL400, SL400c, SL410, SL500, SL500c, SL510, SL512
ThinkPad S Series	S1 YOGA, S1 YOGA 12, S1 YOGA GEN 2, S2, S3 YOGA 14, S430, S5, S5 YOGA 15
ThinkPad T Series	T14 GEN 1, T14 GEN 2, T14S GEN 1, T15 GEN 1, T15 GEN 2, T15G GEN 1, T15G GEN 2, T15P GEN 1, T400, T400s, T410, T410i, T410s, T410si, T420, T420i, T420s, T420si, T43, T430, T430s, T430u, T431s, T43p, T440, T440p, T440s, T450, T450s, T460, T460p, T460s, T462, T470, T470p, T470s, T480, T480s, T490, T490s, T495, T495S, T500, T510, T510i, T520, T520i, T530, T540p, T550, T560, T560s, T570, T580, T590, T60, T60p, T61, T61p
ThinkPad Tablet & Hybrid	Helix, Miix 310, Miix 320, Miix 510, Miix 700, Miix 720, Tablet 2, Tablet (Android), ThinkPad 10, ThinkPad 8, ThinkPad Yoga, ThinkPad Yoga 260, Thinkpad Yoga 370
ThinkPad X Series	X1, X1 Carbon, X1 Carbon GEN 2, X1 Carbon GEN 3, X1 Carbon GEN 4, X1 Carbon GEN 5, X1 Carbon GEN 6, X1 Carbon GEN 7, X1 Carbon GEN 8, X1 Carbon GEN 9, X1 Carbon GEN 10, X1 Carbon Touch, X1 Extreme GEN 1, X1 Extreme GEN 2, X1 Extreme GEN 3, X1 Extreme GEN 4, X1 FOLD GEN 1, X1 NANO GEN 1, X1 Tanium GEN 1, X1 Tablet GEN 1, X1 Tablet GEN 2, X1 Tablet GEN 3, X1 Yoga GEN 1, X1 Yoga GEN 2, X1 Yoga GEN 3, X1 Yoga GEN 4, X1 Yoga GEN 5, X1

	Yoga GEN 6, X12 Detachable GEN 1, X13 GEN 1, X13 GEN 2, X13 YOGA GEN 1, X13 YOGA GEN 2, X13 YOGA GEN 3, X13S YOGA GEN 1, X100e, X120e, X121e, X130e, X131e, X140e, X141e, X200, X200 Tablet, X200s, X200t, X201, X201 Tablet, X201i, X201s, X201si, X201T, X220, X220 Tablet, X220i, X220i Tablet, X230, X230S, X230T, X230 Tablet, X240, X240S, X250, X260, X270, X280, X300, X301, X380, X380 Yoga, X380 Yoga S1, X390, X390 YOGA, X395, X41, X41 Tablet, X60, X60 Tablet, X60s, X61, X61 Tablet, X61s, XYoga 260, YOGA 11E 2ND GEN, YOGA 11E 3RD GEN, YOGA 11E 4TH GEN, YOGA 11E 5TH GEN, YOGA 12, YOGA 14, YOGA 260, YOGA 370, YOGA 460
ThinkPad Z Series	Z61P, Z61T
ThinkBook Series	13s, 14, 14s, 15

Desktops & All In One	Models
ThinkCentre A Series	A57, A58, A61, A61e, A62, A70, A70z
ThinkCentre Edge Series	E62z, E63z, E72, E72z, E73, E73z, E75, E79, E91z, E92, E92z, E93, E93z
ThinkCentre M Series	705 G1, 705 G2, 800 G1, 800 G2, 800 G3 AiO, 800 G4 AIO, 800 G5 AIO, 800 G6, 800 G8, 800 G9, 1000 G1 AIO, 1000 G2

Desktop Workstations	Models
ThinkStation	E20, E30, E31, E32, P300, P310, P320, P320 Tiny, P330, P330 Tiny, P340, P340 Tiny, P350, P350 Tiny, P410, P500, P510, P520, P520C, P620, P700, P710, P720, P900, P910, P920

https://www.absolute.com/partners/device-compatibility/#hp.

15. Lenovo has actual knowledge of the Asserted Patents at least as early as the filing of this Complaint.

JURISDICTION AND VENUE

16. This is an action for patent infringement under the Patent Laws of the United States, 35 U.S.C. §271.

17. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

18. This Court has specific personal jurisdiction over Defendants pursuant to due process and/or the Texas Long Arm Statute, at least in part, because (i) Defendants have conducted and continue to conduct business in this judicial district and (ii) Softex LLC's causes of action arise, at least in part, from Lenovo's contacts with and activities in the state of Texas and this judicial district. Upon information and belief, each Defendant has committed acts of infringement within the state of Texas and this judicial district by, *inter alia*, directly and/or indirectly using, testing, selling, offering to sell, or importing products that infringe one or more claims of the Asserted Patents in this judicial district and/or importing accused products into this judicial district, including via the Internet, and inducing others to commit acts of patent infringement in this judicial district, and/or committing at least a portion of any other infringements alleged herein.

19. Defendants have committed acts within this district giving rise to this action, and have established sufficient minimum contacts with the state of Texas such that the exercise of jurisdiction would not offend traditional notions of fair play and substantial justice.

20. Lenovo has placed or contributed to placing infringing products, including the Accused Products into the stream of commerce via an established distribution channel knowing or understanding that such products would be sold and used in the United States, including in the Western District of Texas. On information and belief, Lenovo also has derived substantial revenues from these infringing acts in the Western District of Texas.

21. On information and belief, Lenovo employs individuals in Austin to design, test, market, and sell the Accused Products, which infringe the Asserted Patents. On information and belief, Lenovo's Austin employees induce customers with numerous physical operating locations in this judicial district to buy, use, test, and sell the Accused Products, which infringe the Asserted Patents.

22. Lenovo offers computers and devices with variety of infringing security functionalities, including Absolute Functionality, Windows Functionality, and other software with similar security functionality. Therefore, on information and belief, Lenovo has derived substantial revenues from its infringing acts in the state of Texas and this district.

23. In addition, on information and belief, Lenovo has, and continues to, knowingly induce infringement by others within the United States and this district by advertising, marketing, and directing products containing infringing functionality to consumers, customers, manufacturers, distributors, resellers, partners, and/or end users in the United States and by providing instructions, user manuals, advertising, and/or marketing materials that facilitate, direct, or encourage the use of infringing functionality with knowledge thereof. *See, e.g.*, https://www.lenovo.com/us/en/d/accessories/absolute/?orgRef=https%253A%252F%252Fwww.google.com%252F (encouraging customers to activate the Absolute Functionality); https://www.verizon.com/support/knowledge-base-238409/ (encouraging customers to use Find My Device to find a lost Windows device).

24. Venue is proper in this judicial district pursuant to 28 U.S.C. §§ 1391(b), (c), and 1400(b). Venue is proper for Lenovo because it (1) has a regular and established place of business in this judicial district, and (2) has committed and continues to commit acts of patent infringement in this judicial district by, *inter alia*, directly and/or indirectly using, testing, selling, offering to sell, or importing products that infringe one or more claims of the Asserted Patents.

BACKGROUND

25. Founded in 1992, Softex, Inc. provides innovative security-focused software solutions to businesses and individuals around the globe. Shortly after its founding, Softex, Inc. was invited to become one of the only software developers permitted to work with Phoenix Technologies ("Phoenix") to develop BIOSs for computer manufacturers as an Independent

Authorized Developer. Softex, Inc.'s relationship with Phoenix was especially significant because available space for the BIOS is extremely limited and, at the time, Phoenix had a virtual monopoly on the development of BIOSs for Original Equipment Manufacturers (OEM) of laptop and desktop computers. Through its independent work with BIOSs, Softex, Inc. gained unique insight that allowed it to conceptualize the inventive concepts in the Asserted Patents and to develop a persistent theft detection security technology that dramatically improved and indeed changed the face of the computer security industry.

26. Traditional software-based theft prevention and recovery systems were ineffective because the software components, which were stored on viewable components of hard drives, were easily tampered with by thieves. Because the memory storing the BIOS is ordinarily incorporated into motherboards at the factory by OEMs, embedding persistent theft detection security software in the BIOS can drastically improve the possibility of recovering stolen or lost devices and preventing data theft. Softex, Inc. pioneered the embedding of persistent theft detection security software into the BIOS and on hidden hard drive partitions, thus enabling computer security systems to do things that could not be accomplished prior to Softex, Inc.'s innovative solutions. Softex, Inc. filed patent applications concerning these solutions and obtained some of the earliest patents in this field, including the Asserted Patents.

27. In the early 2000s, Softex, Inc. began promoting and marketing its proprietary persistent theft detection security technology to other software companies and OEMs. Phoenix was especially interested and asked for Softex, Inc.'s permission to demonstrate TheftGuard to OEM partners, including Lenovo. In May 2003, Phoenix and Absolute issued a joint press release announcing Phoenix's intent to install TheftGuard on OEM BIOSs. The press release stated, "TheftGuard is a new Core Managed Environment (cME) application that will run independent of

the operating system, in the highly secure host protect area (Lenovo) of the hard drive" and that "TheftGuard is the first theft deterrent application that cannot be removed or replaced merely by installing another hard drive." More than a dozen news outlets covered the press release, including CNET and Business Week, calling TheftGuard a "great piece of software." Journalists also recognized the innovative nature of TheftGuard, reporting that "[s]ince TheftGuard [is] also in the BIOS, even if you remove the hard drive," Softex, Inc. would still be able to "track or disable the machine, or wipe the drive." News outlets also discussed TheftGuard's software component stored on non-visible portions of hard drives, reporting that even thieves who format hard drives are "foiled by TheftGuard's place in the [host protected] section of the hard drive, which is immune to simple reformatting tools."

28. Softex, Inc. transferred all rights, title, and interest in and to the Asserted Patents to Softex LLC on August 5, 2022. The assignment was recorded on August 9, 2022 at reel/frame: 060760/0082.

THE ASSERTED PATENTS

U.S. PATENT NO. 7,590,837

29. On September 15, 2009, United States Patent No. 7,590,837 (the "'837 Patent") entitled "Electronic Device Security and Tracking System and Method," was duly and legally issued by the United States Patent and Trademark office to inventors Apurva Mahendrakumar Bhansali, Manoj Kumar Jain, Shradha Dube, Gayathri Rangarajan, Mehul Ramjibhai Patel, Rayesh Kashinath Raikar, Kamal Mansukhlal Dhanani, Ranjit Kapila, Elza Abraham, and Thomas David Tucker. Softex LLC is the sole owner by assignment of the entire rights, title, and interest in and to the '837 Patent, including the rights to sue on and recover for any past infringement thereof. A true and correct copy of the '837 Patent is attached hereto as Exhibit A.

30. The ’837 Patent pertains to systems for securing and tracking an electronic device. *See* Ex. A, 1:34-38. The ’837 Patent discloses an electronic device security and tracking system and method (ESTSM). Such a system and method may comprise “a plurality of hardware, software and firmware components that cooperate to allow tracking, disabling, and other interaction with the stolen electronic device.” *Id.*, 1:34-42. The systems and methods of the ’837 Patent are designed, *inter alia*, to solve certain technical problems affecting users of electronic devices who wish to deter device and/or data theft. *Id.*, 1:12-30. In the absence of an ESTSM, like that disclosed in the ’837 Patent, users of electronic devices were limited to preventing theft of devices and data by means of physical attachment to the user or immovable object, password protection schemes to discourage theft, or motion sensors or alarms placed on devices. *Id.*, 1:22-28. However, these means of preventing device or data theft “do not always prevent theft, are costly and once the electronic device is stolen, do not allow tracking or recovery.” *Id.*, 1:28-30. Traditional software-based theft prevention and recovery systems were ineffective because the software components, which were stored on viewable components of hard drives, were easily tampered with by thieves. *Id.*, 18:34-37. Among other things, the systems of the ’837 Patent dramatically increase the effectiveness of theft prevention by using a combination of a basic input/output system (BIOS) security component, a non-viewable security component, and an application component, working in conjunction with one another to provide a persistent theft detection security solution.

31. The ’837 Patent claims are directed to patent-eligible, non-abstract ideas in that they provide technical solutions to at least the technical problems described above. The claims relate to a system that uses an ESTSM to deter electronic device theft and, if stolen or lost, empowering users to disable or take other administrative actions in relation to the stolen/lost

device. "The ESTSM system may include an electronic device with three components and a server computer system. The three components may be an application component, a non-viewable component, and a Basic Input/Output System (BIOS) component. *Id*., 2:12-17. This system allows the application component to cause a stolen electronic device to send, to the server system, a message that contains location information for the electronic device. In one embodiment, the BIOS component ensures that the application cannot be tampered with, bypassed, or removed from the electronic device. *Id*., 17:62-64. The BIOS component "consists of a small piece of code that resides in the system BIOS ROM image located in a secure non-volatile area," and "[e]very time the electronic device boots up, the BIOS component will check the integrity of the ESTSM non-viewable component and application component programs and files, and restore the original programs and files, if they have been tampered with." *Id*., 17:64-18:8. The BIOS component ensures that the application component has "run properly on the previous device boot and will take action if it is determined that an attempt to bypass the application component has occurred." *Id*., 18:8-12. Thus, by utilizing the ESTSM disclosed in the '837 Patent, users can deter the theft of their devices and thwart thieves who attempt to remove or alter the theft prevention and recovery software. The claimed inventions are directed to patent-eligible, non-abstract ideas because they improve the overall security of electronic devices that employ the inventions disclosed in the '837 Patent. Further, the systems claimed in the '837 Patent cannot be performed as mental steps by a human, nor do they represent the application of a generic computer to any well-known method of organizing human behavior.

32. The language of each of the claims, including Claim 1, is consistent with the inventive concepts described above, as found in the specification. For example, the electronic device security and tracking system of Claim 1 requires, among other things, "an application

component to execute within an OS environment wherein said application component is configured to cause the electronic device to send, to the server system, a message that contains location information for the electronic device, and wherein said application component is configured to determine whether the electronic device has been reported stolen, based on information received from the server system," "a non-viewable security component in the electronic device … compris[ing] a validator module capable of determining whether the application component is present and … has been tampered with," "a non-volatile storage device comprising a secure area" and "a basic input/output security (BIOS) component stored in the secure area, the BIOS security component configured to check the integrity of the application component during a boot process for the electronic device." *Id.*, Claim 1. In addition, Claim 1 specifies further configurations for the BIOS component—namely that the BIOS component is configured to, e.g., determine whether the non-viewable security component has been tampered with, automatically cause the electronic device to restore the integrity of the application component in response to a negative integrity check for the application component, and prevent the electronic device from booting the OS in response to receiving a notification that the electronic device has been reported stolen. *Id.* In addition, Claim 1 specifies further configurations for the application component: "the application component is configured to notify the BIOS security component that the electronic device has been reported stolen" and that the "application component is substantially distinct from the BIOS security component and the validator component." *Id.*

33. Claim 1 is directed to a specific technical improvement to the prior art problems addressed above. Claim 1 as whole is inventive and novel, as are at least each of the identified claim limitations that require an electronic device and security tracking system capable of providing a *persistent* theft detection security solution. *Id.*, 18:13-19:7. As of the priority date of

the ’837 Patent, the identified claim limitations that require a specific implementation for a *persistent* theft detection security solution (such as, e.g., the claimed application component, BIOS component and/or security component configurations) were not well-understood, routine or conventional. As of the priority date of the ’837 Patent, traditional prior art security solutions included security such as password protection schemes, physical attachments, motion sensors or alarms. *Id.*, 1:13-27. “However, such techniques do not always prevent theft, are costly and once the electronic device is stolen, do not allow tracking or recovery.” *Id.*, 1:27-30. The persistent theft detection security solution of Claim 1 provides a vast improvement over traditional prior art solutions because the security features remain in an area inaccessible to the user in the claimed invention at least because, e.g., the BIOS security component is configured to determine whether the non-viewable security component has been tampered with, causes the electronic device to restore the integrity of the application component in response to a negative integrity check, and prevents the electronic device from booting the OS in response to receiving a notification that the electronic device has been stolen.

34. As evidenced by the preceding paragraphs, the ’837 Patent claims are directed to a non-abstract improvement in computer functionality rather than the abstract idea of computer security at large. By reciting technical solutions that enable a computer security system to do things it could not do before, the ’837 Patent claims recite more than a mere result and provide an inventive arrangement for accomplishing a novel result.

U.S. PATENT NO. 8,506,649

35. On August 13, 2013, United States Patent No. 8,506,649 (the “’649 Patent”) entitled “Electronic Device Security and Tracking System and Method,” was duly and legally issued by the United States Patent and Trademark office to inventors Apurva Mahendrakumar

Bhansali, Manoj Kumar Jain, Shradha Dube, Gayathri Rangarajan, Mehul Ramjibhai Patel, Rayesh Kashinath Raikar, Kamal Mansukhlal Dhanani, Ranjit Kapila, Elza Abraham, and Thomas David Tucker. Softex LLC is the sole owner by assignment of the entire rights, title, and interest in and to the '649 Patent, including the rights to sue on and recover for any past infringement thereof. A true and correct copy of the '649 Patent is attached hereto as Exhibit B.

36. The'649 Patent pertains to devices, articles of manufacture, and methods for securing and tracking an electronic device, and discloses an electronic device security system and tracking system and method ("ESTSM"). *See* Ex. B, 1:34-40. Such systems and methods may comprise "a plurality of hardware, software and firmware components that cooperate to allow tracking, disabling, and other interaction with the stolen electronic device." *Id.*, 1:38-40. The devices, articles of manufacture, and methods claimed in the '649 Patent are designed, *inter alia*, to solve certain technical problems affecting users of mobile electronic devices who wish to deter device and/or data theft. In the absence of an ESTSM like that disclosed in the '649 Patent, users of mobile electronic devices were limited to preventing theft of devices and data by means of physical attachment to the user or immovable object, password protection schemes to discourage theft, or motion sensors or alarms placed on devices. *Id.*, 1:24-29. However, these means of preventing device or data theft "do not always prevent theft, are costly and once the electronic device is stolen, do not allow tracking or recovery." *Id.*, 1:30-32. Traditional software-based theft prevention and recovery systems were ineffective because the software components, which were stored on viewable components of hard drives, were easily tampered with by thieves. *Id.*, 18:34-37. Among other things, the devices, articles of manufacture, and methods of the '649 Patent dramatically increase the effectiveness of stolen device data recovery by using a combination of a

security application that utilizes code residing within a memory area that cannot be modified by the user.

37. The ’649 Patent claims are directed to patent-eligible, non-abstract ideas in that they provide technical solutions to at least the technical problems described above. The claims relate to a mobile electronic device, an article of manufacture, and a method for providing security for a mobile electronic device. *Id.*, 1:57-62, 2:1-8. The mobile electronic device, article of manufacture, and method include/use an electronic device security and tracking system and method (ESTSM) application stored on a memory having a changeable area and a system area that is not changeable by a user. The ESTSM may reside, at least partially, on the system area of the memory. *Id.*, 3:44-60. For example, non-viewable components of the ESTSM may reside on a protected area of the memory and periodically communicate with security service. *Id.*, 19:8-44, 26:13-16. In response to the ESTSM receiving a device-loss notification, the ESTSM disables at least one user function of the mobile electronic device while still allowing the mobile electronic device to communicate with a security service and causes some data to be copied to a server. *Id.*, 2:16-37, 34:15-37. Thus, by utilizing the ESTSM disclosed in the ’649 Patent, users can recover data from stolen devices. The claimed inventions are directed to patent-eligible, non-abstract ideas because they improve the overall security of electronic devices that employ the inventions disclosed in the ’649 Patent. Further, the device, methods and article of manufacture implementations claimed in the ’649 Patent cannot be performed as mental steps by a human, nor do they represent the application of a generic computer to any well-known method of organizing human behavior.

38. The language of each of the claims, including Claim 1, is consistent with the inventive concepts described above and found in the specification. For example, the mobile

electronic device of Claim 1 requires, among other things, a security application operable to perform operations "causing the mobile electronic device to periodically communicate with the security service," "accepting a notification at the mobile electronic device from the security service, wherein the notification comprises a message indicating that the owner of the mobile electronic device has reported a loss or requested disabling of the mobile electronic device," and "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," and "automatically causing at least some user data to be copied from the mobile electronic device to at least one of the servers" where "the security application utilizes code residing at least partially in the system area" that "cannot be modified by the user" and where "the security application receives the notification from at least one of the servers via the system area." *Id.*, Claim 1.

39. Claim 1 is directed to a specific technical solution to the prior art problems addressed above. Claim 1 as whole is inventive and novel, as are at least each of the identified claim limitations that require that the mobile electronic device be capable of providing a *persistent* theft detection security solution. As of the priority date of the '649 Patent, the identified claim limitations that require a specific implementation for a *persistent* theft detection security solution (such as, e.g., the claimed security application having code housed at least partially in the system area, which cannot be modified by a user and where the security application receives the notification from at least one of the servers via the system area that cannot be modified by a user) were not well-understood, routine or conventional. As of the priority date of the '649 Patent, traditional prior art security solutions included security such as password protection schemes, physical attachments, motion sensors or alarms. *Id.*, 1:15-32. "However, such techniques do not

always prevent theft, are costly and once the electronic device is stolen, do not allow tracking or recovery." *Id.*, 1:30-32. The persistent theft detection security solution of Claim 1 provides a vast improvement over traditional prior art solutions because the security features remain in an area inaccessible to the user in the claimed invention at least because, e.g., the code for the security application is housed at least partially in the system area (which cannot be modified by a user) and, when the device is reported stolen or a request to disable is received when (e.g., the device cannot be located), the security application receives the notification from at least one of the servers via the system area that cannot be modified by a user. Claim 1 additionally further improves traditional prior art security solutions because the claimed invention is operable to disable at least one user function while still communicating with the security service and automatically copy some user data from the mobile electronic device to at least one of the servers.

40. As evidenced by the preceding paragraphs, the '649 Patent claims are directed to a non-abstract improvement in computer functionality rather than the abstract idea of computer security at large. By reciting technical solutions that enable a computer security system to do things it could not do before, the '649 Patent claims recite more than a mere result and provide an inventive arrangement for accomplishing a novel result.

U.S. PATENT NO. 8,516,235

41. On August 20, 2013, United States Patent No. 8,516,235 (the "'235 Patent") entitled "Basic Input/Output System Read Only Memory Image Integration System and Method," was duly and legally issued by the United States Patent and Trademark office to inventors Apurva Mahendrakumar Bhansali, Manoj Kumar Jain, Shradha Dube, Gayathri Rangarajan, Mehul Ramjibhai Patel, Rayesh Kashinath Raikar, Kamal Mansukhlal Dhanani, Ranjit Kapila, Elza Abraham, and Thomas David Tucker. Softex LLC is the sole owner by assignment of the entire

rights, title, and interest in and to the ’235 Patent, including the rights to sue on and recover for any past infringement thereof. A true and correct copy of the ’235 Patent is attached hereto as Exhibit C.

42. The’235 Patent pertains to systems, methods, and computer readable mediums for securing and tracking an electronic device. *See* Ex. C, 1:1-3. The ’235 Patent discloses an ESTSM. The ’235 Patent is designed, *inter alia*, to solve certain technical problems affecting users of electronic devices who wish to deter device and/or data theft. In the absence of an ESTSM like the systems, methods, and computer readable mediums disclosed in the ’235 Patent, users of electronic devices were limited to preventing theft of devices and data by means of physical attachment to the user or immovable object, password protection schemes to discourage theft, or motion sensors or alarms placed on devices. *Id*., 1:25-31. However these means of preventing device or data theft “do not always prevent theft, are costly and once the electronic device is stolen, do not allow tracking or recovery.” *Id*., 1:31-33. Traditional software-based theft prevention and recovery systems were ineffective because the software components, which were stored on viewable components of hard drives, were easily tampered with by thieves. *Id*., 16:36-38. Among other things, the systems and methods of the ’235 Patent dramatically increase the effectiveness of theft prevention and recovery by installing components on non-viewable portions of an electronic device’s memory and BIOS.

43. The ’235 Patent claims are directed to patent-eligible, non-abstract ideas in that they provide technical solutions to at least the technical problems described above. The claims relate to the systems, methods, and computer readable mediums that include/use an ESTSM to deter electronic device theft and, if stolen or lost, empower users to disable or take other administrative actions in relation to the stolen/lost device. The ESTSM system may include an

electronic device with three components. The three components may be an application component, a non-viewable component, and a BIOS component. *Id*., Fig. 47. The non-viewable component determines whether the application component is present and whether it has been tampered with. The BIOS component determines whether the non-viewable component is present and whether it has been tampered with, checks the integrity of the application component, and restores the application component's integrity if it has been compromised. This arrangement allows for a persistent application component. In one embodiment, the BIOS component ensures that the application cannot be tampered with, bypassed, or removed from the electronic device. *Id*., 16:62-66. The BIOS component "consists of a small piece of code that resides in the system BIOS ROM image located in a secure non-volatile area," and "[e]very time the electronic device boots up, the BIOS component will check the integrity of the ESTSM non-viewable component and application component programs and files, and restore the original programs and files, if they have been tampered with." *Id*., 15:64-16:8. The BIOS component ensures that the application component has "run properly on the previous device boot and will take action if it is determined that an attempt to bypass the application component has occurred." *Id*., 16:8-12. Thus, by utilizing the ESTSM disclosed in the '235 Patent, users can deter the theft of their devices and thwart thieves who attempt to remove or alter the theft prevention and recovery software. The claimed inventions are directed to patent-eligible, non-abstract ideas because they improve the overall security of electronic devices that employ the inventions disclosed in the '235 Patent. Further, the systems, methods and computer readable mediums implementations claimed in the '235 Patent cannot be performed as mental steps by a human, nor do they represent the application of a generic computer to any well-known method of organizing human behavior.

44. The language of each of the claims, including Claim 8, is consistent with the inventive concepts described above, as found in the specification. For example, the system of Claim 8 includes, among other things, limitations requiring "a non-viewable component," "an application component connected to the non-viewable component" that is configured a particular way and "a Basic Input/Output System (BIOS) component connected to the non-viewable component" where the BIOS component is configured a specific way and where the "application component is substantially distinct from the BIOS component and the non-viewable component." *Id.*, Claim 8. In addition, "the BIOS component is configured to determine whether the non-viewable component is present," "determine whether the non-viewable component has been tampered with," "check integrity of the application component during a boot process for an electronic device," and "automatically cause the electronic device to restore the integrity of the application component in response to a negative integrity check of the application component." *Id.*, Claim 8. In addition, the "non-viewable component is configured to determine whether the application component is present and whether the application component has been tampered with." *Id.*, Claim 8.

45. Claim 8 is directed to a specific technical improvement to the prior art problems addressed above. Claim 8 as whole is inventive and novel, as are at least each of the identified claim limitations that require a system capable of providing a *persistent* theft detection security solution. As of the priority date of the '235 Patent, the identified claim limitations that require a specific implementation for a persistent theft detection security solution (such as, e.g., the claimed BIOS component and non-viewable component configurations) were not well-understood, routine or conventional. As of the priority date of the '235 Patent, traditional prior art security solutions included security such as password protection schemes, physical attachments, motion sensors or

alarms. *Id.*, 1:16-33. "However, such techniques do not always prevent theft, are costly and once the electronic device is stolen, do not allow tracking or recovery." *Id.*, 1:31-33. The persistent theft detection security solution of Claim 8 provides a vast improvement over traditional prior art solutions because the security features remain in an area in accessible to the user in the claimed invention at least because, e.g., the application component is substantially distinct from the BIOS component and the non-viewable component and, the BIOS security component is configured to determine whether the non-viewable security component is present and has been tampered with, check the integrity of the application component during a boot process for an electronic device, and cause the electronic device to automatically restore the integrity of the application component in response to a negative integrity check.

46. As evidenced by the preceding paragraph, the '235 Patent claims are directed to a non-abstract improvement in computer functionality rather than the abstract idea of computer security at large. By reciting technical solutions that enable a computer security system to do things it could not do before, the '235 Patent claims recite more than a mere result and provide an inventive arrangement for accomplishing a novel result.

U.S. PATENT NO. 8,145,892

47. On March, 27, 2012, United States Patent No. 8,145,892 (the "'892 Patent") entitled "Providing an Electronic Device Security and Tracking System and Method," was duly and legally issued by the United States Patent and Trademark office to inventors Apurva Mahendrakumar Bhansali, Manoj Kumar Jain, Shradha Dube, Gayathri Rangarajan, Mehul Ramjibhai Patel, Rayesh Kashinath Raikar, Kamal Mansukhlal Dhanani, Ranjit Kapila, Elza Abraham, and Thomas David Tucker. Softex LLC is the sole owner by assignment of the entire rights, title, and interest in and to the '892 Patent, including the rights to sue on and recover for

any past infringement thereof. A true and correct copy of the '892 Patent is attached hereto as Exhibit D.

48. The '892 Patent pertains to systems, methods, devices and apparatuses for securing and tracking an electronic device. *See* Ex. D, 1:37-41. Such systems, methods, devices and apparatuses may comprise "a plurality of hardware, software and firmware components that cooperate to allow tracking, disabling, and other interaction with the stolen electronic device." *Id.*, 1:39-41. The '892 Patent is designed, *inter alia*, to solve certain technical problems affecting users of electronic devices who wish to deter device and/or data theft. In the absence of an ESTSM like the method disclosed in the '892 Patent, users of electronic devices were limited to preventing theft of devices and data by means of physical attachment to the user or immovable object, password protection schemes to discourage theft, or motion sensors or alarms placed on devices. *Id.*, 1:25-30. However these means of preventing device or data theft "do not always prevent theft, are costly and once the electronic device is stolen, do not allow tracking or recovery." *Id.*, 1:31-33. Traditional software-based theft prevention and recovery systems were ineffective because the software components, which were stored on viewable components of hard drives, were easily tampered with by thieves. *Id.*, 18:60-63. Among other things, systems and methods of the '892 Patent dramatically increases the effectiveness of theft prevention and recovery by installing components on non-viewable portions of an electronic device's memory and/or the BIOS.

49. The '892 Patent claims are directed to patent-eligible, non-abstract ideas in that they provide technical solutions to at least the technical problems described above. The claims relate to the use of an ESTSM to deter electronic device theft and, if stolen or lost, empowering users to disable or take other administrative actions in relation to the stolen/lost device. "The ESTSM system may include an electronic device with three components and a server computer

system. The three components may be an application component, a non-viewable component, and a Basic Input/Output System (BIOS) component." *Id*., 2:17-21. This system allows the application component to cause a stolen electronic device to send, to the server system, a message that contains location information for the electronic device. In one embodiment, the BIOS component ensures that the application cannot be tampered with, bypassed, or removed from the electronic device. *Id*., 18:21-23. The BIOS component "consists of a small piece of code that resides in the system BIOS ROM image located in a secure non-volatile area," and "[e]very time the electronic device boots up, the BIOS component will check the integrity of the ESTSM non-viewable component and application component programs and files, and restore the original programs and files, if they have been tampered with." *Id*., 18:23-34. The BIOS component ensures that the application component has "run properly on the previous device boot and will take action if it is determined that an attempt to bypass the application component has occurred." *Id*., 18:34-38. Thus, by utilizing the ESTSM disclosed in the '892 Patent, users can deter the theft of their devices and thwart thieves who attempt to remove or alter the theft prevention and recovery software. The claimed inventions are directed to patent-eligible, non-abstract ideas because they improve the overall security of electronic devices that employ systems and methods disclosed in the '892 Patent. Further, the systems, methods, devices and apparatuses claimed in the '892 Patent cannot be performed as mental steps by a human, nor do they represent the application of a generic computer to any well-known method of organizing human behavior. The language of each of the claims, including Claim 12, is consistent with the inventive concepts described above, as found in the specification. For example, the electronic device of Claim 12 requires, among other things, "a non-viewable component," an application component connected to the non-viewable component capable of communicating with the non-viewable component and operable to execute within the

operating system environment, and "a Basic Input/Output System (BIOS) security component connected to the non-viewable component" where "the application component is substantially distinct from the BIOS component and the non-viewable component." *Id.*, Claim 12. In addition, Claim 12 requires that, "after the security service has been activated," the "non-viewable component is operable to determine whether the application component is present and whether the application component has been tampered with" and the BIOS security component is operable to "determine whether the non-viewable component is present and whether the non-viewable component has been tampered with," "check integrity of the application component during a boot process for an electronic device," and "automatically cause the electronic device to restore the integrity of the application component in response to a negative integrity check of the application component." *Id.*, Claim 12. In addition, Claim 12 requires that "the application component is substantially distinct from the BIOS component and the non-viewable component."

50. Claim 12 is directed to a specific technical improvement to the prior art problems addressed above. Claim 12 as whole is inventive and novel, as are the identified claim limitations that require an electronic device capable of providing a *persistent* theft detection security solution. *Id.*, 18:21-19:33. As of the priority date of the '892 Patent, the identified claim limitations that require a specific implementation for a persistent theft detection security solution (such as, the claimed BIOS security component and non-viewable component configurations) were not well-understood, routine or conventional. As of the priority date of the '892 Patent, traditional prior art security solutions included security such as password protection schemes, physical attachments, motion sensors or alarms. *Id.*, 1:16-33. "However, such techniques do not always prevent theft, are costly and once the electronic device is stolen, do not allow tracking or recovery." *Id.*, 1:31-33. The persistent theft detection security solution of Claim 12 provides a vast improvement over

traditional prior art solutions because the security features remain in an area inaccessible to the user in the claimed invention at least because, e.g., the claimed configuration provides security and tracking for an electronic device with a non-viewable component configured to determine whether the application component is present and has been tampered with, and a BIOS security component configured to determine whether the non-viewable security component is present and has been tampered with, check the integrity of the application component during a boot process for the electronic device, and cause the electronic device to automatically restore the integrity of the application component in response to a negative integrity check all whether the application component is substantially distinct from the BIOS component and non-viewable component.

51. As evidenced by the preceding paragraph, the ’892 Patent claims are directed to a non-abstract improvement in computer functionality rather than the abstract idea of computer security at large. By reciting technical solutions that enable a computer security system to do things it could not do before, the ’892 Patent claims recite more than a mere result and provide an inventive arrangement for accomplishing a novel result.

U.S. PATENT NO. 8,137,410

52. On March 20, 2012, United States Patent No. 8,137,410 (the “’410 Patent”) entitled “Electronic Device Disabling System and Method,” was duly and legally issued by the United States Patent and Trademark office to inventors Apurva Mahendrakumar Bhansali, Manoj Kumar Jain, Shradha Dube, Gayathri Rangarajan, Mehul Ramjibhai Patel, Rayesh Kashinath Raikar, Kamal Mansukhlal Dhanani, Ranjit Kapila, Elza Abraham, and Thomas David Tucker. Softex LLC is the sole owner by assignment of the entire rights, title, and interest in and to the ’410 Patent, including the rights to sue on and recover for any past infringement thereof. A true and correct copy of the ’410 Patent is attached hereto as Exhibit E.

53. The ’410 Patent pertains to apparatuses and methods for securing and tracking an electronic device. *See* Ex. E, 1:36-40. Such systems and methods may comprise “a plurality of hardware, software and firmware components that cooperate to allow tracking, disabling, and other interaction with the stolen electronic device.” *Id*., 1:38-40. The’410 Patent is designed, inter alia, to solve certain technical problems affecting users of electronic devices who wish to prevent device and/or data theft. In the absence of an ESTSM like the method disclosed in the ’410 Patent, users of electronic devices were limited to preventing theft of devices and data by means of physical attachment to the user or immovable object, password protection schemes to discourage theft, or motion sensors or alarms placed on devices. *Id*., 1:24-30. However these means of preventing device or data theft “do not always prevent theft, are costly and once the electronic device is stolen, do not allow tracking or recovery.” *Id*., 1:30-32. Traditional software-based theft prevention and recovery systems were ineffective because the software components, which were stored on viewable components of hard drives, were easily tampered with by thieves. *Id*., 2:66-3:1. Among other things, apparatuses and methods of the ’410 Patent dramatically increase the effectiveness of theft prevention and recovery by installing components associated with an application for tracking and locating the electronic device on hidden partitions of the electronic device’s memory.

54. The ’410 Patent claims are directed to patent-eligible, non-abstract ideas in that they provide technical solutions to at least the technical problems described above. The claims relate to apparatuses and methods for providing device security. *Id.*, 1:57-62, 2:1-8. The apparatuses and methods include/use memory with a hidden partition and an application component associated with tracking and locating the electronic device/apparatus. *Id.*, 2:48-3:12, 18:29-19:44. In response to determining that the application component did not operate correctly in a power-up, restoring the application component from a backup fileset. *Id*. Thus, by utilizing

the ESTSM disclosed in the ’410 Patent, users track and locate lost or stolen devices and thieves cannot remove the persistent tracking and locating software. *Id.* The claimed inventions are directed to patent-eligible, non-abstract ideas because they improve the overall security of electronic devices that employ the inventions disclosed in the ’410 Patent. Further, the device, methods and article of manufacture implementations claimed in the ’410 Patent cannot be performed as mental steps by a human, nor do they represent the application of a generic computer to any well-known method of organizing human behavior.

55. The language of each of the claims, including Claim 8, is consistent with the inventive concepts described above, as found in the specification. For example, the apparatus of Claim 8 requires, among other things, a device capable of “automatically determining whether a hidden partition in the electronic device is valid,” whether the “hidden partition and an application component [are] associated with tracking and locating the electronic device,” and “wherein the hidden partition comprises a non-viewable component associated with tracking and locating the electronic device.” *Id.*, Claim 8. In addition, Claim 8 further specifies that, in response to a determination that hidden partition is valid, the apparatus is capable of “automatically loading the non-viewable component and transferring control to the non-viewable component.” *Id.*, Claim 8. In addition, Claim 8 further specifies that non-viewable component is operable to “automatically determin[e] whether the application component correctly loaded during the last power-up of the electronic device” and “automatically restor[e] the application component from a backup fileset” in response to a negative determination. *Id.*, Claim 8.

56. Claim 8 is directed to a specific technical improvement to the prior art problems addressed above. Claim 8 as whole is inventive and novel, as are at least the identified claim limitations that require an apparatus capable of providing a *persistent* theft detection security

solution. *Id.*, 2:48-3:12, 18:29-19:44. As of the priority date of the '410 Patent, the identified claim limitations that require a specific implementation for a persistent theft detection security solution (such as, e.g., the claimed configuration and capabilities of the hidden partition and non-viewable component) were not well-understood, routine or conventional. As of the priority date of the '410 Patent, traditional prior art security solutions included security such as password protection schemes, physical attachments, motion sensors or alarms. *Id.*, 1:15-32. "However, such techniques do not always prevent theft, are costly and once the electronic device is stolen, do not allow tracking or recovery." *Id.*, 1:30-32. The persistent theft detection security solution of Claim 8 provides a vast improvement over traditional prior art solutions because the security features remain in an area inaccessible to the user in the claimed invention at least because, e.g., the apparatus is having a hidden partition with a non-viewable component associated with tracking and locating the electronic device, where the apparatus is capable of determining whether a hidden partition is valid in the electronic device and, if valid, loading the non-viewable component and transferring control to the non-viewable component where the non-viewable component is configured to automatically determine whether the application component operated correctly during the last power-up of the electronic device and, in response to a negative determination, automatically restoring the application component from a backup files set.

57. As evidenced by the preceding paragraph, the '410 Patent claims are directed to a non-abstract improvement in computer functionality rather than the abstract idea of computer security at large. By reciting technical solutions that enable a computer security system to do things it could not do before, the '410 Patent claims recite more than a mere result and provide an inventive arrangement for accomplishing a novel result.

U.S. PATENT NO. 8,287,603

58. On October 16, 2012, United States Patent No. 8,287,603 (the "'603 Patent") entitled "Electronic Device With Protection From Unauthorized Utilization," was duly and legally issued by the United States Patent and Trademark office to inventors Apurva Mahendrakumar Bhansali, Manoj Kumar Jain, Shradha Dube, Gayathri Rangarajan, Mehul Ramjibhai Patel, Rayesh Kashinath Raikar, Kamal Mansukhlal Dhanani, Ranjit Kapila, Elza Abraham, and Thomas David Tucker. Softex LLC is the sole owner by assignment of the entire rights, title, and interest in and to the '603 Patent, including the rights to sue on and recover for any past infringement thereof. A true and correct copy of the '603 Patent is attached hereto as Exhibit F.

59. The '603 Patent pertains to electronic devices, articles of manufacture, and methods that prevent lost/stolen devices from booting. *See* Ex. F, 1:36-40. The electronic devices, articles of manufacture, and methods disclosed in the '603 Patent may comprise "a plurality of hardware, software and firmware components that cooperate to allow tracking, disabling, and other interaction with the stolen electronic device." *Id.*, 1:38-40. The '603 Patent is designed, *inter alia*, to solve certain technical problems affecting users of electronic devices who wish to deter device and/or data theft. In the absence of an ESTSM like the method disclosed in the '603 Patent, users of electronic devices were limited to preventing theft of devices and data by means of physical attachment to the user or immovable object, password protection schemes to discourage theft, or motion sensors or alarms placed on devices. *Id.*, 1:24-30. However these means of preventing device or data theft "do not always prevent theft, are costly and once the electronic device is stolen, do not allow tracking or recovery." *Id.*, 1:30-32. Traditional software-based theft prevention and recovery systems were ineffective because the software components, which were stored on viewable components of hard drives, were easily tampered with by thieves. *Id.*, 2:66-3:1. Among other things, the invention disclosed in the '603 Patent dramatically increases the effectiveness of

theft prevention and recovery by installing components on non-viewable portions of an electronic device's HDD and/or the BIOS.

60. The '603 Patent claims are directed to patent-eligible, non-abstract ideas in that they provide technical solutions to at least the technical problems described above. The claims relate to the use of an ESTSM to deter electronic device theft and, if stolen or lost, empowering users to disable or take other administrative actions in relation to the stolen/lost device. "The ESTSM system may include an electronic device with three components and a server computer system. The three components may be an application component, a non-viewable component and a Basic Input/Output System (BIOS) component." *Id*., 2:16-20. This system allows the application component to cause a stolen electronic device to send, to the server system, a message that contains location information for the electronic device. *Id*., 11:4-13. In one embodiment, the BIOS component ensures that the application cannot be tampered with, bypassed, or removed from the electronic device. *Id*., 18:13-15. The BIOS component "consists of a small piece of code that resides in the system BIOS ROM image located in a secure non-volatile area," and "[e]very time the electronic device boots up, the BIOS component will check the integrity of the ESTSM non-viewable component and application component programs and files, and restore the original programs and files, if they have been tampered with." *Id*., 18:15-26. The BIOS component ensures that the application component has "run properly on the previous device boot and will take action if it is determined that an attempt to bypass the application component has occurred." *Id*., 18:26-30. Thus, by utilizing the ESTSM disclosed in the '603 Patent, users can deter theft of their devices and thwart thieves who attempt to remove or alter the theft prevention and recovery software. The claimed inventions are directed to patent-eligible, non-abstract ideas because they improve the overall security of electronic devices that employ the systems and methods disclosed in the '603

Patent. Further, the electronic device, articles of manufacture, and methods claimed in the '603 Patent cannot be performed as mental steps by a human, nor do they represent the application of a generic computer to any well-known method of organizing human behavior.

61. The language of each of the claims, including Claim 18, is consistent with the inventive concepts described above, as found in the specification. For example, Claim 18 requires, among other things, an electronic device capable of "executing an application component … configured to automatically ascertained whether the electronic device has been reported stolen based on information received from a server system," "automatically determining whether the application component is operating correctly," "in response to a determination that the application component is operating correctly, automatically providing a basic input/output system (BIOS) component of the electronic device with information indicating that the application component is operating correctly" and "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." *Id.*, Claim 18.

62. Claim 18 is directed to a specific technical solution to the prior art problems addressed above. Claim 18 as whole is inventive and novel, as are at least the identified claim limitations that requiring that electronic device be capable of providing a persistent theft detection security solution. *Id.*, 18:13-19:27. As of the priority date of the '603 Patent, the identified limitations of Claim 18 that require a specific implementation for a persistent theft detection security solution (such as, executing the application component as claimed and automatically determining whether it is operating correctly, automatically providing a BIOS component with information it is operating correctly, and, during a subsequent boot process, preventing the

electronic device from completing the boot process if the BIOS component does not find the required information from the application component) were not well-understood, routine or conventional. As of the priority date of the '603 Patent, traditional prior art security solutions included security such as password protection schemes, physical attachments, motion sensors or alarms. *Id.*, 1:15-32. "However, such techniques do not always prevent theft, are costly and once the electronic device is stolen, do not allow tracking or recovery." *Id.*, 1:30-32. The persistent theft detection security solution of Claim 18 provides a vast improvement over traditional prior art solutions because the security features remain in an area inaccessible to the user in the claimed invention at least because, e.g., the electronic device is provided with software for protecting the electronic device for unauthorized utilization where, in response to a determination that the application component is operating correctly, automatically providing the BIOS component with information indicating the application component is operating correctly and, during a subsequent boot process, 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.

63. As evidenced by the preceding paragraph, the '603 Patent claims are directed to a non-abstract improvement in computer functionality rather than the abstract idea of computer security at large. By reciting technical solutions that enable a computer security system to do things it could not do before, the '603 Patent claims recite more than a mere result and provide an inventive arrangement for accomplishing a novel result.

U.S. PATENT NO. 8,128,710

64. On March 6, 2012, United States Patent No. 8,128,710 (the "'710 Patent") entitled "Electronic Device Security System and Method," was duly and legally issued by the United States

Patent and Trademark office to inventors Apurva Mahendrakumar Bhansali, Manoj Kumar Jain, Shradha Dube, Gayathri Rangarajan, Mehul Ramjibhai Patel, Rayesh Kashinath Raikar, Kamal Mansukhlal Dhanani, Ranjit Kapila, Elza Abraham, and Thomas David Tucker. Softex LLC is the sole owner by assignment of the entire rights, title, and interest in and to the '710 Patent, including the rights to sue on and recover for any past infringement thereof. A true and correct copy of the '710 Patent is attached hereto as Exhibit G.

65. The'710 Patent pertains to systems, methods, and articles of manufacture for securing and tracking an electronic device. *See* Ex. G, 1:15-4:29. The '710 Patent discloses an ESTSM. The '710 Patent is designed, *inter alia*, to solve certain technical problems affecting users of electronic devices who wish to deter device and/or data theft. In the absence of an ESTSM like the systems, methods, and articles of manufacture disclosed in the '710 Patent, users of electronic devices were limited to preventing theft of devices and data by means of physical attachment to the user or immovable object, password protection schemes to discourage theft, or motion sensors or alarms placed on devices. *Id*., 1:24-32. However these means of preventing device or data theft "do not always prevent theft, are costly and once the electronic device is stolen, do not allow tracking or recovery." *Id*., 1:30-32. Traditional software-based theft prevention and recovery systems were ineffective because the software components, which were stored on viewable components of hard drives, were easily tampered with by thieves. *Id*., 19:2-4. Among other things, the systems and methods of the '710 Patent dramatically increase the effectiveness of theft prevention and recovery by installing components on non-viewable portions of an electronic device's memory and BIOS.

66. The '710 Patent claims are directed to patent-eligible, non-abstract ideas in that they provide technical solutions to at least the technical problems described above. The claims

relate to the systems, methods, and articles of manufacture that include/use an ESTSM to deter electronic device theft and, if stolen or lost, empower users to disable or take other administrative actions in relation to the stolen/lost device. The ESTSM system may include an electronic device with three components. The three components may be an application component, a non-viewable component, and a BIOS component. *Id*., Fig. 47. The non-viewable component determines whether the application component is present and whether it has been tampered with. The BIOS component determines whether the non-viewable component is present and whether it has been tampered with, checks the integrity of the application component, and restores the application component's integrity if it has been compromised. This arrangement allows for a persistent application component. In one embodiment, the BIOS component ensures that the application cannot be tampered with, bypassed, or removed from the electronic device. *Id*., 19:28-30. The BIOS component "consists of a small piece of code that resides in the system BIOS ROM image located in a secure non-volatile area," and "[e]very time the electronic device boots up, the BIOS component will check the integrity of the ESTSM non-viewable component and application component programs and files, and restore the original programs and files, if they have been tampered with." *Id*., 18:29-46. The BIOS component ensures that the application component has "run properly on the previous device boot and will take action if it is determined that an attempt to bypass the application component has occurred." *Id*. Thus, by utilizing the ESTSM disclosed in the '710 Patent, users can deter the theft of their devices and thwart thieves who attempt to remove or alter the theft prevention and recovery software. And, in response to a theft, the user can wipe the non-volatile storage device to secure their data. *Id.*, 16:26-41; *see also id.*, 4:61-5:24, 9:9-15, 18:22-28, 24:15-22, 27:35-41. The claimed inventions are directed to patent-eligible, non-abstract ideas because they improve the overall security of electronic devices that employ the

inventions disclosed in the ’710 Patent. Further, the systems, methods and articles of manufacture implementations claimed in the ’710 Patent cannot be performed as mental steps by a human, nor do they represent the application of a generic computer to any well-known method of organizing human behavior.

67. The language of each of the claims, including Claim 2, is consistent with the inventive concepts described above, as found in the specification. For example, the system of Claim 2 includes, among other things, limitations requiring “a non-viewable component,” “an application component connected to the non-viewable component” that is configured a particular way and “a Basic Input/Output System (BIOS) component connected to the non-viewable component” where the BIOS component is configured a specific way and where the “application component is substantially distinct from the BIOS component and the non-viewable component.” *Id.*, Claim 2. In addition, “the BIOS component is configured to determine whether the non-viewable component is present,” “determine … whether the non-viewable component has been tampered with,” “check integrity of the application component during a boot process for the electronic device,” and “automatically cause the electronic device to restore the integrity of the application component in response to a negative integrity check of the application component.” *Id.*, Claim 2. In addition, the “non-viewable component is configured to determine whether the application component is present and whether the application component has been tampered with.” *Id.*, Claim 2. The system is also operable to perform operations, such as “causing to be presented, by a device other than the electronic device, an option to confirm that the non-volatile storage device of the electronic device is to be erased; accepting, from the device other than the electronic device, input to confirm that the non-volatile storage device is to be erased; and after receiving the

report that the electronic device has been stolen, causing the electronic device to erase the non-volatile storage device." *Id.*, Claim 2.

68. Claim 2 is directed to a specific technical improvement to the prior art problems addressed above. Claim 2 as whole is inventive and novel, as are at least each of the identified claim limitations that require a system capable of providing a *persistent* theft detection security solution with the ability to wipe data on a compromised device. As of the priority date of the '710 Patent, the identified claim limitations that require a specific implementation for a persistent theft detection security solution (such as, e.g., the claimed BIOS component and non-viewable component configurations alone or together with the ability to erase data from a stolen device) were not well-understood, routine or conventional. As of the priority date of the '710 Patent, traditional prior art security solutions included security such as password protection schemes, physical attachments, motion sensors or alarms. *Id.*, 1:16-32. "However, such techniques do not always prevent theft, are costly and once the electronic device is stolen, do not allow tracking or recovery." *Id.*, 1:30-32. The persistent theft detection security solution of Claim 2 provides a vast improvement over traditional prior art solutions because the security features remain in an area in accessible to the user in the claimed invention at least because, e.g., the application component is substantially distinct from the BIOS component and the non-viewable component and, the BIOS security component is configured to determine whether the non-viewable security component is present and has been tampered with, check the integrity of the application component during a boot process for an electronic device, cause the electronic device to automatically restore the integrity of the application component in response to a negative integrity check, and cause the electronic device to erase the non-volatile storage device.

69. As evidenced by the preceding paragraph, the ’710 Patent claims are directed to a non-abstract improvement in computer functionality rather than the abstract idea of computer security at large. By reciting technical solutions that enable a computer security system to do things it could not do before, the ’710 Patent claims recite more than a mere result and provide an inventive arrangement for accomplishing a novel result.

LENOVO’S INFRINGING PRODUCTS AND SERVICES

70. Upon information and belief, Lenovo has infringed and continues to infringe one or more claims of the Asserted Patents, as shown below, by making, testing, using, offering to sell, and selling one or more infringing products including Windows Functionality and/or Absolute Functionality.

71. Windows Functionality: Lenovo computers with Microsoft Windows 10 and/or Windows 11 include Microsoft’s “Find My Device” a feature that helps a user locate their device if it is lost or stolen.

Find and lock a lost Windows device

Microsoft account, Windows 10, Microsoft account dashboard

Find My Device is a feature that can help you locate your Windows 10 device if it's lost or stolen. To use this feature, sign in to your device with a Microsoft account and make sure you're an administrator on it. This feature works when location is turned on for your device, even if other users on the device have turned off location settings for their apps. Any time you attempt to locate the device, users using the device will see a notification in the notification area.

- This setting works for any Windows device, such as a PC, laptop, Surface, or Surface Pen. It needs to be turned on before you can use it.
- You can't use it with a work or school account, and it doesn't work for iOS devices, Android devices, or Xbox One consoles. Here's what to do if your Xbox gets stolen.

Turn on Find my device

When you set up a new device, you can decide whether to turn on or turn off the Find my device setting. If you turned it off during setup and now want to turn it on, make sure your Windows device is connected to the internet, has enough battery power so it can send its location, and that you're signed in to the device using your Microsoft account.

1. On the device that you want to change, select **Start** > **Settings** > **Update & Security** > **Find my device**.
2. Select **Change** for the device you want to change.

https://support.microsoft.com/en-us/account-billing/find-and-lock-a-lost-windows-device-890bf25e-b8ba-d3fe-8253-e98a12f26316.

72. Lenovo computers and devices with this feature asks the administrator ("owner") to enable location tracking ["register the mobile electronic device with a security service"] so that when the device is stolen, the administrator can log into their account from a different computer to lock the stolen computer/send messages to the stolen computer/track the stolen computer. This security service resides at least in part on one or more servers. For example, Microsoft shows that a user should "sign in to account.microsoft.com from another device" to view the location of the laptop that has Find My Device enabled, to lock the device, or to display a message on the laptop's screen.

Microsoft's "Find My Device" feature is so much more than a simple device locator that it's like calling a "car" nothing more than just four tires and a steering wheel. The online service is a powerful PC manager in its own right, and arguably more effective in that regard than Windows itself.

https://www.pcworld.com/article/394201/microsofts-find-my-device-is-the-pc-management-tool-you-didnt-know-you-needed.html. When the administrator accesses their Microsoft account, the stolen computer reports its location. The location is shown by choosing the name of the device on

the web portal. Thus, the Find My Device feature causes the mobile electronic device to automatically send the device's identifying information to the security server. The Find My Device service, when enabled, causes the mobile electronic device to periodically communicate with the security service when in a state other than being powered off. For example, it causes the mobile electronic device to periodically send its location to the security service. A Lenovo device with Find My Device enabled can accept a notification from the service comprising a message indicating that the owner of the device has requested disabling ("locking") the device. The mobile device is locked ("disabled") in response to receiving the message. But the device can still communicate with the Find My software, e.g., by continuing to share its location. The Find My Device service automatically causes at least some user data to be copied from the mobile electronic device to at least one of the servers. For example, an owner can view device details and location from the owner's Microsoft user account, and therefore the information, when sent to the server, is automatically paired with some user identifying data. Depending on administrative settings and user permissions, an operating system and file system, stored in non-volatile memory, either provide access to certain files (e.g., files stored in a changeable area) or restrict access to certain files (e.g., files stored in a system area that cannot be modified by a user). Microsoft Find My Device is not changeable by a user and therefore resides at least partially in the system area. By segregating access and not allowing the user access to the administrator area, MSFT provides a system area that cannot be accessed by the user. Microsoft does not allow its device locking to be thwarted by allowing a thief to wipe the old system. When the device is locked, for example, a user cannot reset the device to remove the lock. *See, e.g.*, U.S. Patent No. 9,558,372, assigned to Microsoft.

73. Absolute Functionality: Absolute markets the Absolute Home & Office as a "persistent security solution that can track and recover stolen devices."

> **Absolute Home & Office is the only persistent security solution that can track and recover stolen devices, while also providing additional features to protect your personal information.**

https://homeoffice.absolute.com/.

74. Absolute Home & Office includes a component called Computrace (also called Absolute Persistence Technology) that is "embedded in the firmware and once activated will self-heal our software onto the device if we are removed."

> What is the difference between Absolute Home & Office and Computrace?
>
> **A: Computrace** (also called Absolute Persistence Technology) is one component of Absolute Home & Office and is available on compatible devices. This component is embedded in the firmware and once activated will self-heal our software onto the device if we are removed.
>
> For more information on Computrace compatibility, you may refer to our **BIOS & Firmware Compatibility Checker** page (https://www.absolute.com/partners/device-compatibility/). As this list is not exhaustive, we also recommend speaking directly to your device manufacturer if your device model is not listed.

https://homeoffice.absolute.com/support/faq/#toggle-id-2.

75. Absolute Home & Office includes services residing, at least in part, on a server, allowing a user to view a device's location on a map, remotely lock a device, and remotely delete some or all files from a device.

76. The Absolute Persistence component of Absolute Home & Office (also known as Computrace) is installed on the Accused Products during the manufacturing process.

What is Absolute Persistence?

Absolute's Persistence® is a patented security solution that provides a continuous, tamper-proof connection between devices, data, and the cloud-based Absolute console.

Through our partnerships with device manufacturers such as Dell, HP, Lenovo and others, Persistence is embedded in the firmware of computers, tablets, and smartphones at the factory, remaining dormant until the Absolute agent is installed. Installation initiates a call to the Absolute Monitoring Center, and Persistence is activated.

Once activated, the status of the Absolute agent or any third-party applications is continuously monitored and, if it is missing or damaged, a reinstallation will automatically occur. Persistence will survive attempts to disable it, even if the device is re-imaged, the hard drive is replaced, or the firmware is flashed.

https://www.absolute.com/platform/editions/.

COUNT 1
INFRINGEMENT OF U.S. PATENT NO. 7,590,837

77. Softex LLC realleges and incorporates by reference each and every allegation of Paragraphs 1-76 above as if fully set herein.

78. Lenovo has directly infringed, and continues to directly infringe, literally or under the doctrine of equivalents, at least independent claim 1 of the '837 Patent by making, testing, using, selling, and/or offering for sale Accused Products with Absolute Functionality in the United States, in violation of 35 U.S.C. § 271(a). *See* Ex. H.

79. The Accused Products, which incorporate Absolute Functionality, meet each and every element of at least Claim 1 of the'837 Patent, either literally or equivalently.

80. At least as of the day the Complaint was filed, Lenovo has indirectly infringed one or more claims thereof under 35 U.S.C. § 271(b) through the active inducement of direct infringement by intending to encourage, and in fact encouraging customers to activate Absolute Functionality into the Accused Products sold and used within the United States in an infringing manner that practiced the inventions of one or more claims of the '837 Patent, including at least Claim 1. Lenovo has actively induced such direct infringement through its contacts with customers

thereby providing, *inter alia*, functionality, instructions, user manuals and other documentation and other assistance that have served to facilitate, promote, and cause customers to directly infringe at least Claim 1 of the ’837 Patent, as described in Ex. H. Upon information and belief, Lenovo has performed the acts that constitute inducement of infringement with the knowledge or willful blindness that the resulting acts induced thereby would constitute direct infringement by customers.

81. As a direct and proximate consequence of Lenovo’s infringement of the ’837 Patent, Softex LLC has suffered damages in an amount not yet determined for which Softex LLC is entitled to relief.

COUNT 2
INFRINGEMENT OF U.S. PATENT NO. 8,506,649

82. Softex LLC realleges and incorporates by reference each and every allegation of Paragraphs 1-81 above as if fully set herein.

83. Lenovo has directly infringed, and continues to directly infringe, literally or under the doctrine of equivalents, at least independent claim 1 of the ’649 Patent by making, testing, using, selling, and/or offering for sale its devices with Windows Functionality in the United States, in violation of 35 U.S.C. §271(a). *See* Ex. I. Lenovo has also directly infringed, and continues to directly infringe, literally or under the doctrine of equivalents, at least independent claim 1 of the ’649 Patent by making, testing, using, selling, and/or offering for sale its devices with Absolute Functionality in the United States, in violation of 35 U.S.C. § 271(a). *See* Ex. J.

84. The Accused Products, which incorporate Windows Functionality, and separately which incorporate Absolute Functionality meet each and every element of at least Claim 1 of the’649 Patent, either literally or equivalently.

85. At least as of the day the Complaint was filed, Lenovo has indirectly infringed one or more claims thereof under 35 U.S.C. § 271(b) through the active inducement of direct infringement by intending to encourage, and in fact encouraging customers to activate enable Windows Functionality, and similar features, and/or encouraging customers to activate Absolute Functionality into the Accused Products sold and used within the United States in an infringing manner that practiced the inventions of one or more claims of the ’649 Patent, including at least Claim 1. Lenovo has actively induced such direct infringement through its contacts with customers thereby providing, *inter alia*, functionality, instructions, user manuals and other documentation and other assistance that have served to facilitate, promote, and cause customers to directly infringe at least Claim 1 of the ’649 Patent, as described in Exs. I, J. Upon information and belief, Lenovo has performed the acts that constitute inducement of infringement with the knowledge or willful blindness that the resulting acts induced thereby would constitute direct infringement by customers.

86. As a direct and proximate consequence of Lenovo’s infringement of the ’649 Patent, Softex LLC has suffered damages in an amount not yet determined for which Softex LLC is entitled to relief.

COUNT 3
INFRINGEMENT OF U.S. PATENT NO. 8,516,235

87. Softex LLC realleges and incorporates by reference each and every allegation of Paragraphs 1-86 above as if fully set herein.

88. Lenovo has directly infringed, and continues to directly infringe, literally or under the doctrine of equivalents, at least independent claim 8 of the ’235 Patent by making, testing, using, selling, and/or offering for sale Accused Products with Absolute Functionality in the United States, in violation of 35 U.S.C. § 271(a). *See* Ex. K.

89. The Accused Products, which incorporate Absolute Functionality, meet each and every element of at least Claim 8 of the'235 Patent, either literally or equivalently.

90. At least as of the day the Complaint was filed, Lenovo has indirectly infringed one or more claims thereof under 35 U.S.C. § 271(b) through the active inducement of direct infringement by intending to encourage, and in fact encouraging customers to activate Absolute Functionality into the Accused Products sold and used within the United States in an infringing manner that practiced the inventions of one or more claims of the '235 Patent, including at least Claim 8. Lenovo has actively induced such direct infringement through its contacts with customers thereby providing, *inter alia*, functionality, instructions, user manuals and other documentation and other assistance that have served to facilitate, promote, and cause customers to directly infringe at least Claim 8 of the '235 Patent, as described in Ex. K. Upon information and belief, Lenovo has performed the acts that constitute inducement of infringement with the knowledge or willful blindness that the resulting acts induced thereby would constitute direct infringement by customers.

91. As a direct and proximate consequence of Lenovo's infringement of the '235 Patent, Softex LLC has suffered damages in an amount not yet determined for which Softex LLC is entitled to relief.

COUNT 4
INFRINGEMENT OF U.S. PATENT NO. 8,145,892

92. Softex LLC realleges and incorporates by reference each and every allegation of Paragraphs 1-91 above as if fully set herein.

93. Lenovo has directly infringed, and continues to directly infringe, literally or under the doctrine of equivalents, at least independent claim 12 of the '892 Patent by making, testing,

using, selling, and/or offering for Accused Products with Absolute Functionality in the United States, in violation of 35 U.S.C. § 271(a). *See* Ex. L.

94. The Accused Products, which incorporate Absolute Functionality, meet each and every element of at least Claim 12 of the'892 Patent, either literally or equivalently.

95. At least as the day the Complaint was filed, Lenovo has indirectly infringed one or more claims thereof under 35 U.S.C. § 271(b) through the active inducement of direct infringement by intending to encourage, and in fact encouraging customers to activate Absolute Functionality into the Accused Products sold and used within the United States in an infringing manner that practiced the inventions of one or more claims of the '892 Patent, including at least Claim 12. Lenovo has actively induced such direct infringement through its contacts with customers thereby providing, *inter alia*, functionality, instructions, user manuals and other documentation and other assistance that have served to facilitate, promote, and cause customers to directly infringe at least Claim 12 of the '892 Patent, as described in Ex. L. Upon information and belief, Lenovo has performed the acts that constitute inducement of infringement with the knowledge or willful blindness that the resulting acts induced thereby would constitute direct infringement by customers.

96. As a direct and proximate consequence of Lenovo's infringement of the '892 Patent, Softex LLC has suffered damages in an amount not yet determined for which Softex LLC is entitled to relief.

COUNT 5
INFRINGEMENT OF U.S. PATENT NO. 8,137,410

97. Softex LLC realleges and incorporates by reference each and every allegation of Paragraphs 1-96 above as if fully set herein.

98. Lenovo has directly infringed, and continues to directly infringe, literally or under the doctrine of equivalents, at least independent claim 8 of the ’410 Patent by making, testing, using, selling, and/or offering for sale Accused Products with Absolute Functionality in the United States, in violation of 35 U.S.C. § 271(a). *See* Ex. M.

99. The Accused Products, which incorporate Absolute Functionality, meet each and every element of at least Claim 8 of the’410 Patent, either literally or equivalently.

100. At least as of the day the Complaint was filed, Lenovo has indirectly infringed one or more claims thereof under 35 U.S.C. § 271(b) through the active inducement of direct infringement by intending to encourage, and in fact encouraging customers to activate Absolute Functionality into the Accused Products sold and used within the United States in an infringing manner that practiced the inventions of one or more claims of the ’410 Patent, including at least Claim 8. Lenovo has actively induced such direct infringement through its contacts with customers thereby providing, *inter alia*, functionality, instructions, user manuals and other documentation and other assistance that have served to facilitate, promote, and cause customers to directly infringe at least Claim 8 of the ’410 Patent, as described in Ex. M. Upon information and belief, Lenovo has performed the acts that constitute inducement of infringement with the knowledge or willful blindness that the resulting acts induced thereby would constitute direct infringement by customers.

101. As a direct and proximate consequence of Lenovo’s infringement of the ’410 Patent, Softex LLC has suffered damages in an amount not yet determined for which Softex LLC is entitled to relief.

COUNT 6
INFRINGEMENT OF U.S. PATENT NO. 8,287,603

102. Softex LLC realleges and incorporates by reference each and every allegation of Paragraphs 1-101 above as if fully set herein.

103. Lenovo has directly infringed, and continues to directly infringe, literally or under the doctrine of equivalents, at least independent claim 18 of the ’603 Patent by making, testing, using, selling, and/or offering for sale Accused Products with Absolute Functionality in the United States, in violation of 35 U.S.C. § 271(a). *See* Ex. N.

104. The Accused Products, which incorporate Absolute Functionality, meet each and every element of at least Claim 18 of the’603 Patent, either literally or equivalently.

105. At least as of the day the Complaint was filed, Lenovo has indirectly infringed one or more claims thereof under 35 U.S.C. § 271(b) through the active inducement of direct infringement by intending to encourage, and in fact encouraging customers to activate Absolute Functionality into the Accused Products sold and used within the United States in an infringing manner that practiced the inventions of one or more claims of the ’603 Patent, including at least Claim 18. Lenovo has actively induced such direct infringement through its contacts with customers thereby providing, *inter alia*, functionality, instructions, user manuals and other documentation and other assistance that have served to facilitate, promote, and cause customers to directly infringe at least Claim 18 of the ’603 Patent, as described in Ex. N. Upon information and belief, Lenovo has performed the acts that constitute inducement of infringement with the knowledge or willful blindness that the resulting acts induced thereby would constitute direct infringement by customers.

106. As a direct and proximate consequence of Lenovo’s infringement of the ’603 Patent, Softex LLC has suffered damages in an amount not yet determined for which Softex LLC is entitled to relief.

COUNT 7
INFRINGEMENT OF U.S. PATENT NO. 8,128,710

107. Softex LLC realleges and incorporates by reference each and every allegation of Paragraphs 1-106 above as if fully set herein.

108. Lenovo has directly infringed, and continues to directly infringe, literally or under the doctrine of equivalents, at least independent claim 2 of the ’710 Patent by making, testing, using, selling, and/or offering for sale Accused Products with Absolute Functionality in the United States, in violation of 35 U.S.C. § 271(a). *See* Ex. O.

109. The Accused Products, which incorporate Absolute Functionality, meet each and every element of at least Claim 2 of the’710 Patent, either literally or equivalently.

110. At least as of the day the Complaint was filed, Lenovo has indirectly infringed one or more claims thereof under 35 U.S.C. § 271(b) through the active inducement of direct infringement by intending to encourage, and in fact encouraging customers to activate Absolute Functionality into the Accused Products sold and used within the United States in an infringing manner that practiced the inventions of one or more claims of the ’710 Patent, including at least Claim 2. Lenovo has actively induced such direct infringement through its contacts with customers thereby providing, *inter alia*, functionality, instructions, user manuals and other documentation and other assistance that have served to facilitate, promote, and cause customers to directly infringe at least Claim 2 of the ’710 Patent, as described in Ex. O. Upon information and belief, Lenovo has performed the acts that constitute inducement of infringement with the knowledge or willful blindness that the resulting acts induced thereby would constitute direct infringement by customers.

111. As a direct and proximate consequence of Lenovo's infringement of the '710 Patent, Softex LLC has suffered damages in an amount not yet determined for which Softex LLC is entitled to relief.

DEMAND FOR JURY TRIAL

112. Plaintiff hereby demands a jury trial for all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. Declare that Defendants have infringed, and continue to infringe, one or more claims of the Asserted Patents, contributed to the infringement of the Asserted Patents, and/or induced the infringement of the Asserted Patents;

B. Enter judgment that Defendants' acts of patent infringement are willful;

C. Award damages no less than a reasonable royalty to Plaintiff arising out of this infringement of the Asserted Patents, including enhanced damages for willful infringement pursuant to 35 U.S.C. § 284 and prejudgment and post-judgment interest, in an amount according to proof;

D. Award attorneys' fees to Plaintiff pursuant to 35 U.S.C. §§ 284 and 285 or as otherwise permitted by law;

E. Award Plaintiff the interest and costs incurred in this action; and

F. Grant Plaintiff such other and further relief, including equitable relief, as the Court deems just and proper.

Dated: December 14, 2022

Respectfully submitted,

MCKOOL SMITH, P.C.

/s/ Blair M. Jacobs

Blair M. Jacobs (WDTX. Bar No. 32010)
bjacobs@McKoolSmith.com
Christina A. Ondrick (WDTX. Bar No. 494625)
condrick@McKoolSmith.com
John S. Holley (SBN 24078678)
jholley@McKoolSmith.com
Steven W. Peters (DC Bar No. 176041
pro hac vice to be submitted)
speters@McKoolSmith.com
1999 K Street, NW Suite 600
Washington, D.C. 20006
Telephone: (202) 370-8300
Facsimile: (202) 370-8344

John B. Campbell (SBN 24036314)
jcampbell@McKoolSmith.com
MCKOOL SMITH, P.C.
303 Colorado Street, Suite 2100
Austin, TX 78701
Telephone: (512) 692-8700
Facsimile: (512) 692-8744

Casey L. Shomaker (SBN 24110359)
cshomaker@McKoolSmith.com
Matthew Folks (SBN 24116368)
mfolks@McKoolSmith.com
MCKOOL SMITH, P.C.
300 Crescent Court, Suite 1500
Dallas, TX 75201
Telephone: (214) 978-4218
Facsimile: (214) 978-4044

ATTORNEYS FOR PLAINTIFF SOFTEX LLC