#### Defendants' Preliminary Claim Constructions Exhibit A

Claim Terms	Proposed Construction and Supporting Evidence
1. "defined interaction" (all asserted claims); "interaction with a host	Construction: Indefinite under 35 U.S.C. § 112.
computing device in a defined way" ('802 Patent, claims 38-39)	Intrinsic Evidence:
	"In particular, the modular device can include a security module that is adapted performance of one or more security operations on data, and a target module that enable a defined interaction with a host computing device." '135 Patent, Abstrat Abstract ("In particular, the peripheral device can be adapted to enable, in a sing peripheral device, performance of one or more security operations on data, and interaction with a host computing device that has not previously been integrated operations in a single integral device.")
	"In particular, the modular device can include a security module that is adapted performance of one or more security operations on data, and a target module that enable a defined interaction with a host computing device." '135 Patent at 3:27 at 3:27-33 ("In particular, the peripheral device can be adapted to enable, in a si peripheral device, performance of one or more security operations on data, and interaction with a host computing device that has not previously been integrated operations in a single integral device.").
	"The peripheral device can also be implemented so that the security operations a in-line, i.e., the security operations are performed between the communication of from the host computing device and the performance of the defined interaction." at 3:40-45.
	"A peripheral device according to the invention can advantageously enable appl security operations to a wide variety of interactions with a host computing device a peripheral device according to the invention can accomplish this without nece peripheral devices: one that performs the security operations and one that perfor interaction. This can, for example, minimize the possibility that the device adap the defined interaction will be used with the host computing system without pro

IPR: IP

of security operations to that interaction." '802 Patent at 3:49-59.
"The target module is adapted to enable a defined interaction with a host com (examples of which are given below)." '135 Patent at 4:18-20.
"In another embodiment of the invention, a modular device includes a securit adapted to enable performance of one or more security operations on data, an that is adapted to enable a defined interaction with a host computing device (s interactions discussed above with respect to exemplary embodiments of the ta the previously discussed embodiment of the invention)." '135 Patent at 4:40-
"In yet another embodiment of the invention, a modular device that is adapted communication with a host computing device, and that includes a security model adapted to enable performance of one or more security operations on data and that is adapted to enable a defined interaction with a host computing device, is to enable provision of the type of a target module to a host computing device request from the host computing device for information regarding the type of device." '135 Patent at 4:56-65.
"In still another embodiment of the invention, a modular device that is adapted communication with a host computing device, and that includes a security modula adapted to enable performance of one or more security operations on data and that is adapted to enable a defined interaction with a host computing device, i to enable the security module and/or the target module to be operably connec computing device in response to an instruction from the host computing device 5:1-9.
"In another embodiment of the invention, a security module is adapted to ena communication with a host computing device, performance of one or more see on data, and communication with a target module that is adapted to enable a with a host computing device." '135 Patent at 5:13-18.
"The security module is also adapted to enable performance of one or more so on data, and communication with a target module that is adapted to enable a d with a host computing device." '135 Patent at 5:32-36.

**DOCKET A L A R M** Find authenticated court documents without watermarks at <u>docketalarm.com</u>.

"In a further particular embodiment of the system, the modular device further module which is adapted to enable communication with a security module, as a defined interaction with a host computing device (examples of which are dis with respect to exemplary embodiments of the target module of previously dis embodiments of the invention)." '135 Patent at 5:36-42. "A modular device according to the invention can advantageously enable appl security operations to a wide variety of interactions with a host computing dev a modular device according to the invention can accomplish this without nece multiple peripheral devices that each include security functionality in addition functionality of the peripheral device. This can, for example, facilitate use of having security capability that operate in a predictable, reliable and consistent manner, since a single security module can be used to provide security to mul interaction with a host computing device. This can also enable ease and flexib secure peripheral devices, since the same security module can be used with a modules. Moreover, the provision of in-line security in a modular device acco invention enables a more secure exchange of data between a host computing of modular device, overcoming the problems identified above in previous system security operations on data exchanged between such devices. Additionally, in modular device according to the invention so that the performance of security modular device is transparent can reduce or eliminate the need to modify aspe operation of the host computing device (e.g., device drivers of the host compu making implementation and use of a data security system including the modul and easier. Thus, the possibility that a user will use the system incorrectly (e.g security operations to an interaction with the host computing device, or apply operations incorrectly or incompletely) is reduced. Making the security operat can also enhance the security of those operations." '135 Patent at 3:48-4:13; ' 3:49-4:10 ("A peripheral device according to the invention can advantageousl application of security operations to a wide variety of interactions with a host device. In particular, a peripheral device according to the invention can accom necessity to use two peripheral devices: one that performs the security operati performs the defined interaction. This can, for example, minimize the possibil adapted to perform the defined interaction will be used with the host computin proper application of security operations to that interaction. Moreover, the prosecurity in a peripheral device according to the invention enables a more secu data between a host computing device and the peripheral device, overcoming identified above in previous systems for performing security operations on dat between such devices. Additionally, implementing a modular device according so that the performance of security operations by the modular device is transport or eliminate the need to modify aspects of the operation of the host computing device drivers of the host computing device), making implementation and use system including the modular device simpler and easier. Thus, the possibility use the system incorrectly (e.g., fail to apply security operations to an interact computing device, or apply the security operations incorrectly or incompletely Making the security operations transparent can also enhance the security of the

"The particular manner in which operation of the operating system software is that the modular device can establish its identity can depend on the characteris operating system software and/or the device interface. However, for many cor operating system software and device interface, the operating system software confirmation that the device connected to the device interface is ready for furt with the operating system software before the operating system software seeks type of the device connected to the interface (the standard for PCMCIA interface) specifies such operation). In such cases, the modular device can be configured informing the operating system software that the modular device is ready for f until the modular device has established its identity." '135 Patent at 10:11-25 7:44-59 ("The particular manner in which operation of the operating system set suspended so that the peripheral device can establish its identity can depend o characteristics of the operating system software and/or the device interface. H combinations of operating system software and device interface, the operating waits for confirmation that the device connected to the device interface is read interaction with the operating system software before the operating system software identify the type of the device connected to the interface (the standard for PCM for example, specifies such operation). In such cases, the peripheral device can delay informing the operating system software that the peripheral device is rea interaction until the peripheral device has established its identity.").

"Since use of the data security system is easier (e.g., a user need not provide in host driver to be appropriately tailored to enable desired interaction with a sec possibility that a user will use the system incorrectly (e.g., fail to apply securit interaction with the host computing device, or apply the security operations in incompletely) is reduced." '135 Patent at 11:4-11; '802 Patent at 8:28-35 ("Si

data security system is easier (e.g., a user need not provide input to cause the appropriately tailored to enable desired interaction with a security device), the user will use the system incorrectly (e.g., fail to apply security operations to a the host computing device, or apply the security operations incorrectly or inco reduced.").
"The modular device driver can have previously been installed on a data stora hard disk) of the host computing device (in FIG. 6, the modular device driver the memory section 606b of the memory device 606 of the host computing de be made accessible to the host computing device via an appropriate interface of disk drive, CD-ROM drive or network connection) at a time when the user wi interaction between the host computing device and the modular device." '132 37; '802 Patent at 9:5-14 ("The peripheral device driver can have previously be data storage device (e.g., hard disk) of the host computing device (in FIG. 6, the device driver is shown stored in the memory section 606b of the memory device computing device 601), or can be made accessible to the host computing devic appropriate interface (such as a floppy disk drive, CD-ROM drive or network time when the user wishes to initiate interaction between the host computing device.").
"In such an implementation, the modular device driver can be implemented to cause one or more predetermined security operations to be performed based u specified interaction with the target module, or the modular device can be consuch security operations to be performed any time a specified interaction with occurs." '135 Patent at 16:9-16; '802 Patent 12:64-13:4 ("In such an implemented peripheral device driver can be implemented to automatically cause one or mos security operations to be performed based upon a user-specified interaction with functionality, or the peripheral device can be configured to cause such securit performed any time a specified interaction with the target functionality occurs."
"A target module of a modular device according to the invention can also be a biometric module, which is defined herein as any module that is adapted to re regarding a physical characteristic of a person based upon a physical interacti- with the module." '135 Patent at 17:19-25; '802 Patent at 14:9-15 ("Target fu peripheral device according to the invention can also be embodied as a biome is defined herein as any device that is adapted to receive input data regarding

# DOCKET



## Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

## **Real-Time Litigation Alerts**



Keep your litigation team up-to-date with **real-time** alerts and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

## **Advanced Docket Research**



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

## **Analytics At Your Fingertips**



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

### API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

#### LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

#### **FINANCIAL INSTITUTIONS**

Litigation and bankruptcy checks for companies and debtors.

#### **E-DISCOVERY AND LEGAL VENDORS**

Sync your system to PACER to automate legal marketing.

