IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

CXT SYSTEMS, INC., Plaintiff,	§	Case No.
	§	**JURY TRIAL DEMANDED**
v.	§	
IKEA NORTH AMERICA SERVICES, LLC, Defendant.	§	

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff CXT Systems, Inc. ("CXT" or "Plaintiff"), for its Complaint against Defendant IKEA North America Services, LLC ("IKEA" or "Defendant"), alleges as follows:

THE PARTIES

1. CXT is a corporation organized and existing under the laws of the State of Texas, with its principal place of business located at 100 West Houston Street, Marshall, Texas 75670.

2. Upon information and belief, IKEA is a corporation organized and existing under the laws of Pennsylvania, with its principal place of business located at 420 Alan Wood Road, Conshohocken, Pennsylvania 19428. Defendant may be served with process through its registered agent, CT Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201.

3. On information and belief, Defendant maintains regular and established places of business within this Judicial District including at least the location at 7171 Ikea Drive, Frisco, TX 75034. Upon information and belief, Defendant employs individuals in this Judicial District involved in the sales and marketing of its products.

JURISDICTION

4. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. §§ 1, *et seq*. This Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1331 and 1338(a).

5. This Court has personal jurisdiction over Defendant. Defendant regularly conducts business and has committed acts of patent infringement and/or has induced acts of patent infringement by others in this Judicial District and/or has contributed to patent infringement by others in this Judicial District, the State of Texas, and elsewhere in the United States.

6. Venue is proper in this Judicial District pursuant to 28 U.S.C. §§ 1391 and 1400(b) because, among other things, Defendant is subject to personal jurisdiction in this Judicial District, has a regular and established place of business in this Judicial District, has purposely transacted business involving the accused products in this Judicial District, including sales to one or more customers in Texas, and certain of the acts complained of herein, including acts of patent infringement, occurred in this Judicial District.

7. Defendant is subject to this Court's jurisdiction pursuant to due process and/or the Texas Long Arm Statute due at least to its substantial business in this State and Judicial District, including (a) at least part of its past infringing activities, (b) regularly doing or soliciting business in Texas, and/or (c) engaging in persistent conduct and/or deriving substantial revenue from goods and services provided to customers in Texas.

PATENTS-IN-SUIT

8. On March 21, 2006, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 7,016,875 (the "'875 Patent") entitled "Single Sign-On for Access to a Central Data Repository." A true and correct copy of the '875 Patent is attached as Exhibit A.

9. On August 14, 2007, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 7,257,581 (the "'581 Patent") entitled "Storage, Management and Distribution of Consumer Information." A true and correct copy of the '581 Patent is attached as Exhibit B.

10. On September 4, 2012, the United States Patent and Trademark Office duly and legally issued U.S. Patent No. 8,260,806 (the "'806 Patent") entitled "Storage, Management and Distribution of Consumer Information." A true and correct copy of the '806 Patent is attached as Exhibit C.

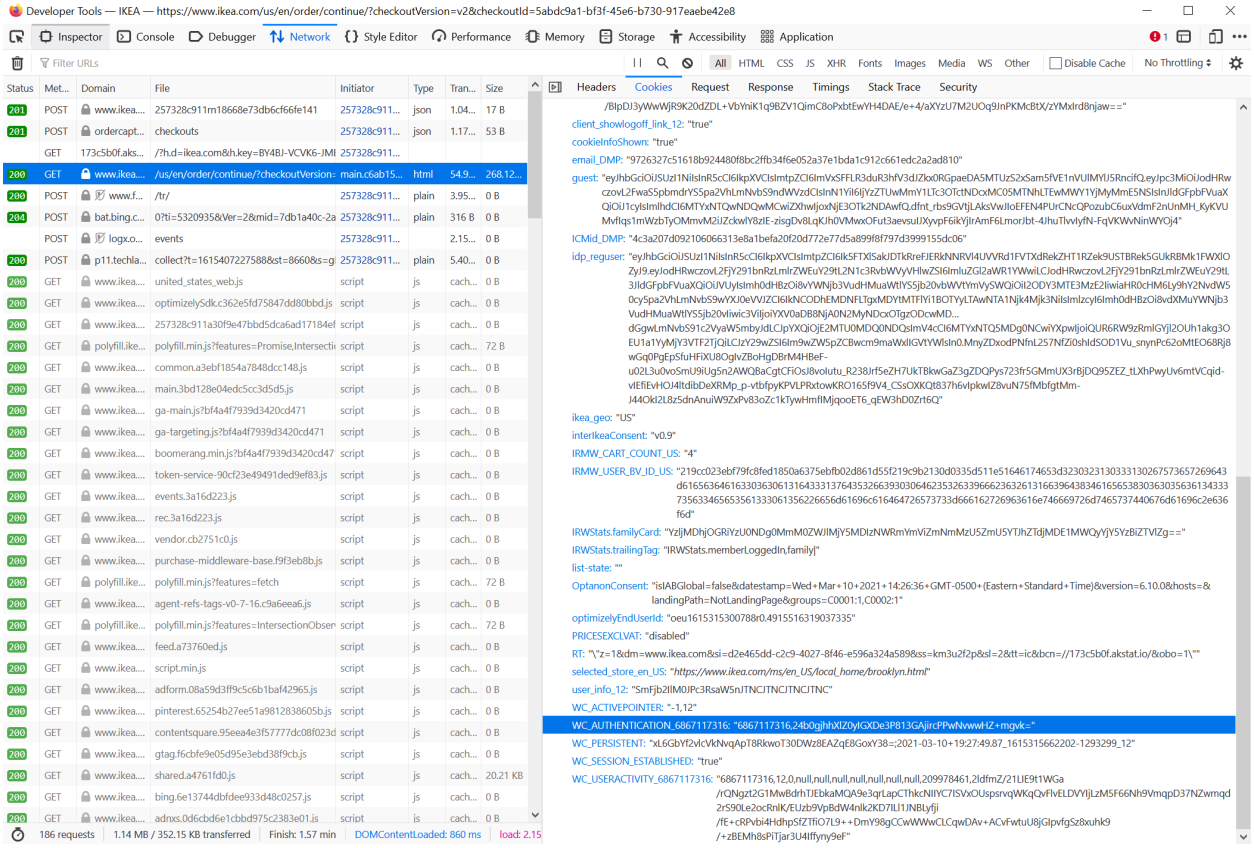
11. CXT is the sole and exclusive owner of all right, title, and interest to and in the '875 Patent, '581 Patent, and '806 Patent (together, the "Patents-in-Suit"), and holds the exclusive right to take all actions necessary to enforce its rights to the Patents-in-Suit, including the filing of this patent infringement lawsuit. CXT also has the right to recover all damages for past, present, and future infringement of the Patents-in-Suit and to seek injunctive relief as appropriate under the law.

12. The inventions covered by the '875 Patent, '581 Patent, and '806 Patent were invented by Nick Steele, Stan Hawkins, Joe Maranville, and Andrew Bradnan (collectively, the "Steele Patents"). The Steele Patents generally cover systems and methods relating to optimizing the online shopping experience. In one exemplary embodiment, an authenticated user may be provided with access and control of relevant account information, such as shipping address or payment information. For example, address or payment information may be automatically populated into input fields of a checkout page for an authenticated user without requiring a permanent software download or repeated log-ins. In another embodiment, a user need only authenticate himself once in order to repeatedly access consumer information from different web

pages and websites. In other embodiments, a client-side or server-side application may effect retrieval of selected information elements. Systems implementing the inventions covered by the Steele Patents achieve significant benefits and improvements in their operation and performance. By allowing a user to store and repeatedly access relevant account information, more efficient usage of the buyer's system is achieved. For example, e-commerce webstore experiences, improved conversion rates, and decreased shopping cart abandonment rates by improving users' shopping experiences. Additionally, by allowing the buyer's system to manage the request/response process through an application, the request/response process can be more properly geared to the buyer's system including its processing load and network latency. Further, in the case where the buyer's computer is a handheld device, which typically has limited resources, the improvements in performance provided by the inventions of the Steele Patents are determinative as to whether many consumers will complete a given transaction.

13. IKEA is in the business of selling products through its webstore available at https://www.ikea.com/ (the "IKEA Webstore") and has been since at least as early as 2014. On information and belief, the IKEA Webstore has included and utilized the HCL Commerce platform (previously known as IBM WebSphere Commerce Platform) ("WebSphere Commerce") for account management and checkout functionality since at least 2014. On information and belief, in accordance with standard implementations of WebSphere Commerce, the IKEA Webstore is supported by a backend computer system including, but not limited to, a host server, a vendor server, a central data repository, and a database management system. Together, the current and previous versions of the IKEA Webstore and their backend computers systems are instances of the Accused Infrastructures. On information and belief, the Accused Infrastructures are hosted within the United States.

14. IKEA's use of WebSphere Commerce in the Accused Infrastructures is demonstrated by the various "WC" session and authentication cookies associated with www.IKEA.com. On information and belief, IKIEA's implementation of WebSphere Commerce is consistent with the documentation of the HCL Help Center, available athttps://help.hcltechsw.com/commerce/index.html.

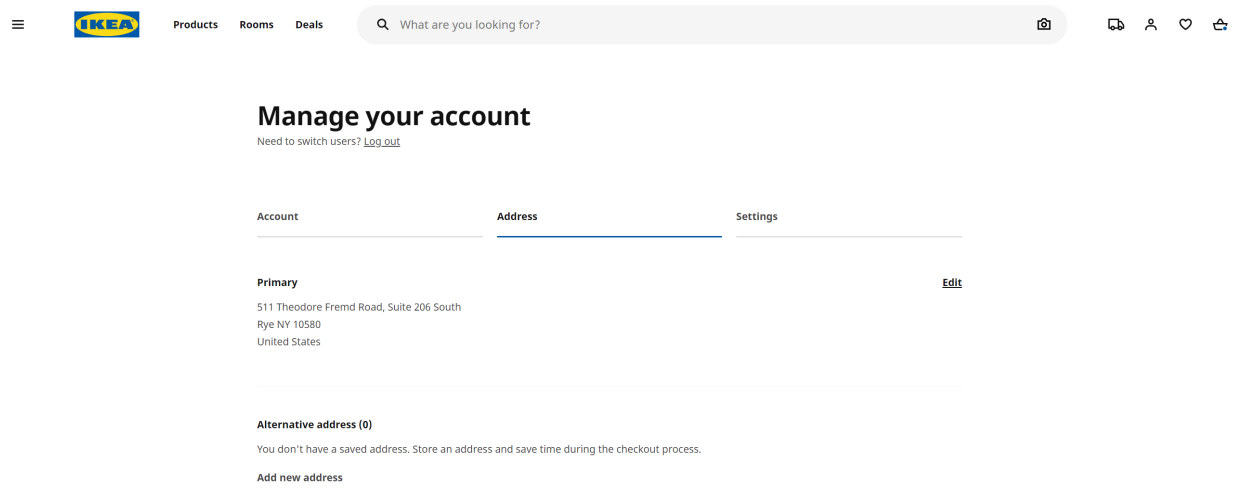


Firefox Developer Tools Console View of WC Cookies in requests associated with https://www.ikea.com/us/en/order/delivery/

15. The Accused Infrastructures employ methods covered by the Steele Patents in order to improve the shopping experience of its buyers. For example, the Accused Infrastructures practice a method comprising retrieving selected consumer information elements from the information stored within a data repository by filtering data from the online account with a

database management system, and transmitting the selected consumer information elements, over a distributed electronic network, to a network device.

16. The Accused Infrastructures comprise and utilize a central data repository comprising a plurality of customer information elements (*e.g.*, name and address), such as an HCL commerce database,[1] and/or tables within an HCL commerce database (*e.g.*, an address table).[2] The Accused Infrastructures store customer information that is subject to the customer's control and management, such as through the account details page of the IKEA Webstore.



IKEA Webstore Manage Your Account page

[1] https://help.hcltechsw.com/commerce/9.0.0/database/concepts/cdb_schema_overview.html
[2] https://help.hcltechsw.com/commerce/9.0.0/database/database/address.html

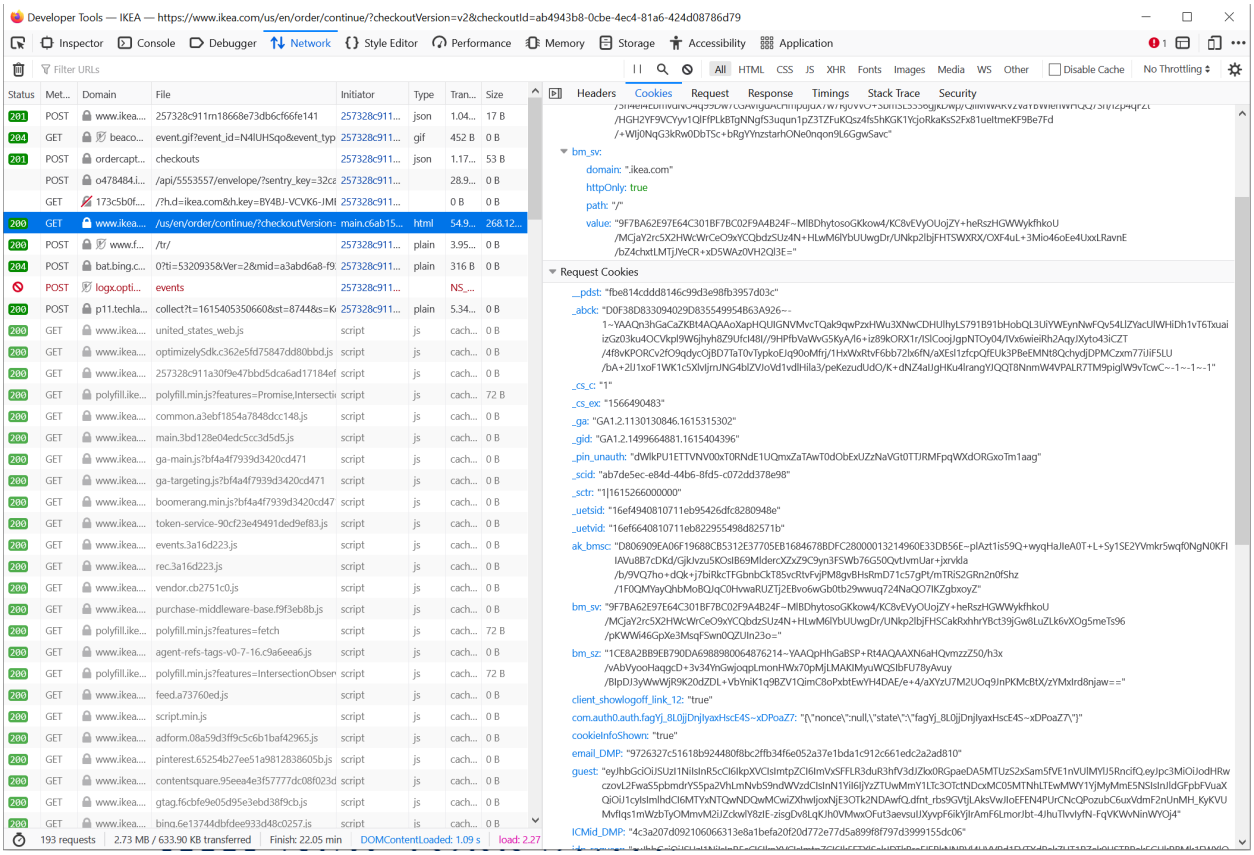
LASTNAME	VARCHAR (128)	Last name of the person to which this address applies, replacing `SALNAME` used in previous versions of WebSphere Commerce or HCL Commerce Suite.
PERSONTITLE	VARCHAR (50)	Title of the person to which this address applies, replacing `SATITLE` used in previous versions of WebSphere Commerce or HCL Commerce Suite. LDAP uses a length of 50. Valid values are Dr, Prof, Rev, Mr, Mrs, Ms, and N (not provided). The default is N.
FIRSTNAME	VARCHAR (128)	First name of the person to which this address applies, replacing `SAFNAME` used in previous versions of WebSphere Commerce or HCL Commerce Suite.
MIDDLENAME	VARCHAR (128)	Middle name or initials of the person to which this address applies, replacing `SAMNAME` used in previous versions of WebSphere Commerce or HCL Commerce Suite.
BUSINESSTITLE	VARCHAR (128)	The business title. For example, Manager or Chief Executive Officer. LDAP uses a length of 128 characters for title attribute in `ePerson`. Compare with the BUCONT.BCTITLE column.
PHONE1	VARCHAR (32)	The primary phone number, replacing `SAPHONE1` used in previous versions of WebSphere Commerce or HCL Commerce Suite.
FAX1	VARCHAR (32)	The primary fax number 1, replacing `SAFAX` used in previous versions of HCL Commerce or HCL Commerce Suite.
PHONE2	VARCHAR (32)	The secondary phone number, replacing `SAPHONE2` used in previous versions of WebSphere Commerce or HCL Commerce Suite.
ADDRESS1	VARCHAR (256)	Address line 1, replacing `SAADDR1` used in previous versions of WebSphere Commerce or HCL Commerce Suite.

HCL WebSphere Commerce Standard User Profile Repository Definition depicting fields for contactInfo including at least name and address information, available at https://help.hcltechsw.com/commerce/9.0.0/database/database/address.html

17. The Accused Infrastructures comprise and utilize a database management system, such as DB2 and/or a WebSphere Commerce federated system, "[a] distributed database management system (DBMS) that consists of a DB2 instance that operates as a server, a database that serves as the federated database, one or more data sources, and clients (users and applications) who access the database and data sources."[3] The central data repository of the Accused Infrastructures (*e.g.*, an HCL commerce database and/or tables thereof) are managed by a DBMS (*e.g.*, DB2) that handles and authenticates requests for customer information, such as requests for customer information elements to autopopulate one or more address or payment fields of an IKEA

[3] https://help.hcltechsw.com/commerce/9.0.0/base/misc/glossary.html

checkout page.[4] For example, as depicted below, a user's browser sends a GET request for address information when the user actuates the checkout button of the IKEA Webstore, including a "WC_AUTHENTICATION" token. In response to the request, the DBMS of the Accused Infrastructures (*e.g.*, the federated system including DB2) authenticates the authentication information (*e.g.*, the WC_AUTHENTICATION token), filters selected consumer information elements from an information account, such as by retrieving address elements according to the WebSphere Commerce Database schema and transmits the selected information back to the user's browser.

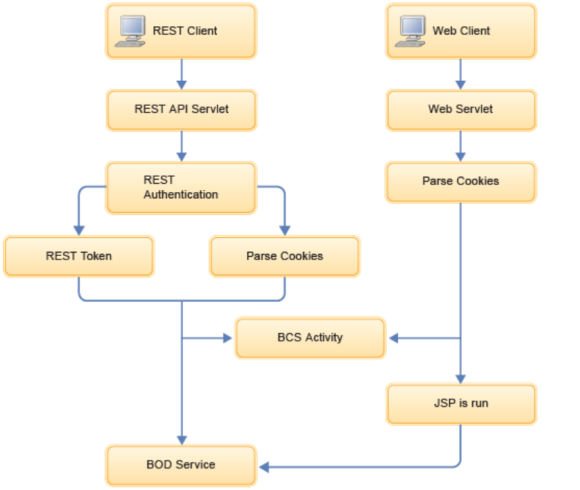


Firefox developer tools view of a GET request for address information from an information account, including a WC_AUTHENTICATION token

[4] https://help.hcltechsw.com/commerce/9.0.0/data/refs/rmlpersonex.html

REST services are authenticated in HCL Commerce on secure and unsecured channels.

The following diagram shows the REST authentication flow for the REST and Web clients:



Where:

If the call is on a secure channel:

1. If the `WCTrustedToken` header is present, use the `WCTrustedToken` header.
2. If the `WC_AUTHENTICATION_*` cookie is present and cookie usage is allowed for REST, use the `WC_AUTHENTICATION_*` cookie matching the specified store ID.
3. If the `WC_PERSISTENT` cookie is present and cookie usage is allowed for REST, use the `WC_PERSISTENT` cookie if persistent sessions are enabled for the service. Otherwise, an exception is thrown indicating that partial authentication is not allowed.

WebSphere Commerce Authentication Flow for WC_AUTHENTICATION token[5]

18. The Accused Infrastructures further authenticate a first request for access to a consumer information account when a registered user logs in with their username and password. The Accused Infrastructures authenticate subsequent requests for access to the information account by authenticating authentication information, such as a WC_AUTHENTICATION token issued to the user's browser based on a previous authentication. The Accused Infrastructures also automatically manage subsequent request authentications with the DBMS when the user interacts with subsequent websites.

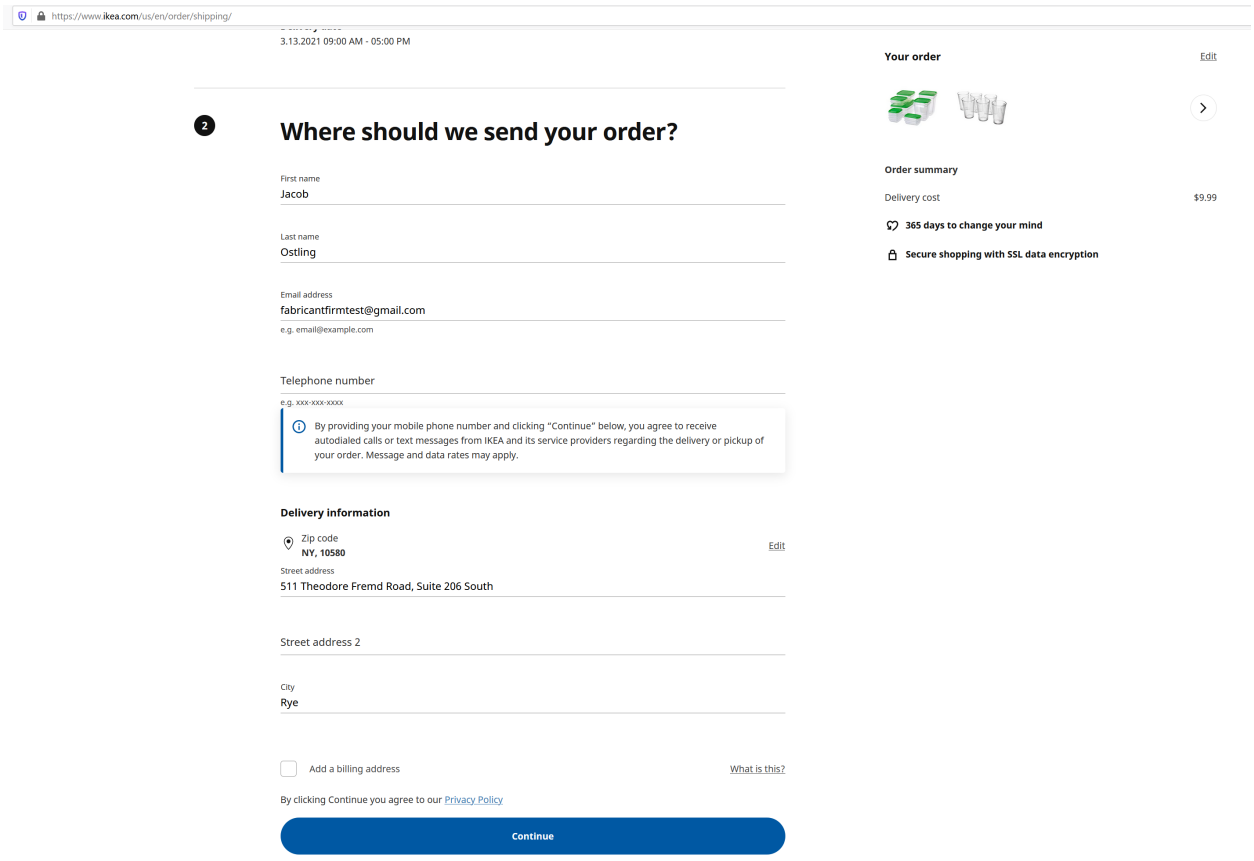
19. Checkout Website of the Accused Infrastructures. For example, the Accused Infrastructures automatically authenticate a request for name, address, and/or payment information at the Checkout website of the Accused Infrastructure based on a previous authentication.

---

5 https://help.hcltechsw.com/commerce/9.0.0/webservices/concepts/cwvrestauthflow.html?hl=wc_authentication

20. The Accused Infrastructures further cause a browser to display a web page file retrieved from a vendor server (*e.g.*, a checkout web page file retrieved from a IKEA WebSphere Commerce Server) which instructs the browser to request a temporary client-side application, such as a javas applet, javascript, and/or Ajax (asynchronous javascript and XML) script. For example, the IKEA web page checkout causes the user's browser to request the https://www.ikea.com/us/en/order/continue/?checkoutVersion=v2&checkoutId=ab4943b8-0cbe-4ec4-81a6-424d08786d79, which includes instructions to download scripts that manage a request/response process for consumer information elements (*e.g.*, name and address information) when executed.

21. The Accused Infrastructures further autopopulate consumer information elements (*e.g.*, name and address information) into at least one input field of a web page file, such as the checkout page depicted below:



IKEA Webstore checkout page with autopopulated consumer information elements

22. CXT has at all times complied with the marking provisions of 35 U.S.C. § 287 with respect to the Patents-in-Suit. On information and belief, prior assignees and licensees have also complied with the marking provisions of 35 U.S.C. § 287.

COUNT I
(Infringement of the '581 Patent)

23. Paragraphs 1 through 21 are incorporated herein by reference as if fully set forth in their entireties.

24. CXT has not licensed or otherwise authorized Defendant to make, use, offer for sale, sell, or import any products that embody the inventions of the '581 Patent.

25. Defendant has directly infringed and continues to directly infringe the '581 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C.

§ 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the ’581 Patent. Upon information and belief, these products include the Accused Infrastructures that practice the methods and systems covered by the ’581 Patent including, for example, account management and checkout functionality implemented at least in part with WebSphere Commerce. For example, these infrastructures infringe at least claim 1 of the ’581 Patent.

26. Defendant has and continues to directly infringe at least claim 1 of the ’581 Patent by making, using, offering to sell, selling, and/or importing into the United States infrastructures that implement a method for storing, managing, and distributing consumer information via a distributed electronic network, the method comprising the steps of: storing an information account in a central data repository accessible via the distributed electronic network, the information account comprising a plurality of consumer information elements associated with a consumer and being subject to the consumer’s control and management; receiving with a database management system, a request over the distributed electronic network from a network device for one or more selected consumer information elements, the request including consumer authentication information and being made by the network device responsive to an input command supplied by the consumer; in response to the request, authenticating the consumer based on the authentication information, retrieving the selected consumer information elements from the information account by filtering data from the information account with the database management system, and transmitting the selected consumer information elements, over the distributed electronic network, to the network device; and autopopulating the selected consumer information elements into at least one input field of a web page file.

27. The Accused Infrastructures store an information account in a central data repository accessible via the distributed electronic network, where the information account comprising a plurality of consumer information elements associated with a consumer and being subject to the consumer's control and management. For example, on information and belief, the Accused Infrastructures store an information account, such as a user profile, in a central data repository such as the user profile repository of the IKEA Webstore. For example, the information account comprises a plurality of consumer information elements, such as name, address, and payment information which the IKEA Webstore allows a consumer to save through their account pages.

28. For example, the Accused Infrastructures receive with a database management system, a request over the distributed electronic network from a network device for one or more selected consumer information elements, the request including consumer authentication information and being made by the network device responsive to an input command supplied by the consumer. For example, upon checkout by a logged in user, the Accused Infrastructures receive a request for one or more selected consumer information elements, such as a GET request for shipping address information. For example, the request is made by a network device, such as a PC, smartphone, or tablet, responsive to actuation of a "checkout" button, and includes authentication information, such as an authentication token.

29. For example, the Accused Infrastructures authenticate the consumer based on the authentication information, retrieve the selected consumer information elements from the information account by filtering data from the information account with the database management system, and transmit the selected consumer information elements, over the distributed electronic network, to the network device. For example, the Accused Infrastructures authenticate a request

for address information at the checkout page based on an authentication token. On information and belief, the database management system of the Accused Infrastructures, such as a federated system including DB2, retrieves the selected consumer information (*e.g.*, name, address, and/or payment information) by filtering the information from a user profile stored on a central repository of the Accused Infrastructures.

30. For example, the Accused Infrastructures autopopulate the selected consumer information elements into at least one input field of a web page file. For example, the Accused Infrastructures autopopulate the selected consumer information elements, such as name, address, and/or payment information into input fields of a web page file of the IKEA Webstore checkout.

31. Defendant has indirectly infringed and continues to indirectly infringe one or more claims of the ’581 Patent by knowingly and intentionally inducing others, including end users and service providers of the Accused Infrastructures, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling and/or importing into the United States products that include infringing technology, such as the Accused Infrastructure that practice the systems and methods covered by the ’581 Patent.

32. Defendant, with knowledge that these products, or the use thereof, infringe the ’581 Patent knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’581 Patent by providing these Accused Infrastructures to end users and/or service providers for use in an infringing manner.

33. Defendant induced infringement by others, including end users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end users, infringe the ’581 Patent, while remaining willfully blind to the infringement.

34. CXT has suffered damages as a result of Defendant's direct and indirect infringement of the '581 Patent in an amount to be proved at trial.

35. CXT has suffered, and will continue to suffer, irreparable harm as a result of Defendant's infringement of the '581 Patent for which there is no adequate remedy at law, unless Defendant's infringement is enjoined by this Court.

COUNT II
(Infringement of the '806 Patent)

36. Paragraphs 1 through 21 are incorporated herein by reference as if fully set forth in their entireties.

37. CXT has not licensed or otherwise authorized Defendant to make, use, offer for sale, sell, or import any products that embody the inventions of the '806 Patent.

38. Defendant has directly infringed and continues to directly infringe the '806 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States products that satisfy each and every limitation of one or more claims of the '806 Patent. Upon information and belief, these products include the Accused Infrastructures that practice the methods and systems covered by the '806 Patent including, for example, account management and checkout functionality implemented at least in part with WebSphere Commerce. For example, these infrastructures infringe at least claim 1 of the '806 Patent.

39. Defendant has and continues to directly infringe at least claim 1 of the '806 Patent by making, using, offering to sell, selling and/or importing into the United States infrastructures that comprise a computer-readable storage medium having stored thereon computer-executable instructions for storing, managing, and distributing consumer information via a distributed electronic network, by causing a computing device to perform operations comprising: determining

one or more consumer information elements for fields of a web page, the one or more consumer information elements associated with an information account and in a data storage accessible via the distributed electronic network, the information account comprising a plurality of consumer information elements associated with a consumer and being subject to the consumer's control and management; causing a browser to display a web page file that has been retrieved from a vendor server, the web page file including an instruction that causes the browser to request transmission of a client-side application having at least a temporary portion; executing at a network device an application configured to manage a request/response process for the network device; transmitting over the distributed electronic network from the network device a request for the determined one or more consumer information elements, the request including consumer authentication information and being made by the network device responsive to an input command supplied by the consumer; receiving at the network device the one or more consumer information elements filtered from the information account; and autopopulating the filtered one or more consumer information elements into corresponding fields.

40. For example, the executable instructions stored on the Accused Infrastructures determine one or more consumer information elements for fields of a web page, the one or more consumer information elements associated with an information account and in a data storage accessible via the distributed electronic network, the information account comprising a plurality of consumer information elements associated with a consumer and being subject to the consumer's control and management. For example, on information and belief, the Accused Infrastructures determine consumer information elements for fields of a web page based on field codes or identifiers which correspond with fields of a user profile repository of the IKEA Webstore. For example, on information and belief, the Accused Infrastructures comprise a user profile repository

further comprising a plurality of information elements, such as name, address, and payment information, which is associated with an account subject to the consumer's control and management via the account profile pages of the IKEA Webstore. For example, on information and belief, the user profile repository includes at least fields corresponding with the default ADDRESS table including, but not limited to, name and address.

41. For example, the executable instructions stored on the Accused Infrastructures cause a browser to display a web page file that has been retrieved from a vendor server, the web page file including an instruction that causes the browser to request transmission of a client-side application having at least a temporary portion. For example, the Accused Infrastructures cause a web browser to render a web page file retrieved from a vendor server, such as an IKEA server, or third-party vendor server included and utilized in the IKEA Webstore, which includes an instruction to request transmission of a client-side application having a temporary portion, such as a Java applet, ajax script, and/or javascript having a temporary portion in the web browser. For example, on information and belief, the web page files of the IKEA Webstore of the Accused Infrastructures cause a browser to issue a request for an application having a temporary portion, such as a javascript, ajax script, and/or Java applet.

42. On information and belief, the executable instructions stored on the Accused Infrastructures execute at a network device an application configured to manage a request/response process for the network device. For example, on information and belief, the Accused Infrastructures cause a network device, such as a consumer's computer, smartphone, and/or tablet, to execute an application configured to manage a request/response process, such as the applications discussed above. For example, on information and belief, the Accused Infrastructures further execute an application configured to manage a request/response process associated with name,

address, and payment information at web page files associated with the IKEA Webstore checkout of the Accused Infrastructures.

43. For example, the executable instructions stored on the Accused Infrastructures transmit over the distributed electronic network from the network device a request for the determined one or more consumer information elements, the request including consumer authentication information and being made by the network device responsive to an input command supplied by the consumer. For example, on information and belief, in response to a consumer actuating a checkout button (*e.g.*, for the IKEA Webstore checkout), the Accused Infrastructures transmit a request for the determined name, address, and payment information.

44. For example, the executable instructions stored on the Accused Infrastructures cause the network device to receive the one or more consumer information elements filtered from the information account. For example, the client-device, such as a computer, smartphone, or tablet receive determined name, address, and payment information filtered from the information account. For example, on information and belief, those information elements are filtered from the information account.

45. On information and belief, the executable instructions stored on the Accused Infrastructures autopopulate the filtered one or more consumer information elements into corresponding fields. For example, the Accused Infrastructures autopopulate the selected consumer information elements, such as name, address, and/or payment information into input fields of a checkout web page file of the IKEA Webstore. For example, after a user has authenticated himself, he further has access to his account where certain customer information elements are autopopulated.

46. Defendant has indirectly infringed and continues to indirectly infringe one or more claims of the ’806 Patent by knowingly and intentionally inducing others, including end users and service providers of the Accused Infrastructures, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling and/or importing into the United States products that include infringing technology, such as the Accused Infrastructure that practice the systems and methods covered by the ’806 Patent.

47. Defendant, with knowledge that these products, or the use thereof, infringe the ’806 Patent knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’806 Patent by providing these Accused Infrastructure to end users and/or service providers for use in an infringing manner.

48. Defendant induced infringement by others, including end users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end users, infringe the ’806 Patent, while remaining willfully blind to the infringement.

49. CXT has suffered damages as a result of Defendant’s direct and indirect infringement of the ’806 Patent in an amount to be proved at trial.

50. CXT has suffered, and will continue to suffer, irreparable harm as a result of Defendant’s infringement of the ’806 Patent for which there is no adequate remedy at law, unless Defendant’s infringement is enjoined by this Court.

COUNT III
(Infringement of the ’875 Patent)

51. Paragraphs 1 through 21 are incorporated herein by reference as if fully set forth in their entireties.

52. CXT has not licensed or otherwise authorized Defendant to make, use, offer for sale, sell, or import any products that embody the inventions of the '875 Patent.

53. Defendant has directly infringed and continues to directly infringe the '875 Patent, either literally or under the doctrine of equivalents, without authority and in violation of 35 U.S.C. § 271, by making, using, offering to sell, selling, and/or importing into the United States infrastructures that satisfy each and every limitation of one or more claims of the '875 Patent. Upon information and belief, these products include the Accused Infrastructures that practice the methods and systems covered by the '875 Patent including, for example, account management and checkout functionality implemented at least in part with WebSphere Commerce.

54. For example, Defendant has and continues to directly infringe at least claim 1 of the '875 Patent by making, using, offering to sell, selling, and/or importing into the United States infrastructures that provides access to an information account via a distributed electronic network that is coupled to a database management system, such as by providing access to a user's information account over the internet at checkout pages of https://www.IKEA.com/. For example, on information and belief, the IKEA Webstore is coupled to a database management system, such as DB2.

55. For example, Defendant has and continues to directly infringe at least claim 1 of the '875 Patent by making, using, offering to sell, selling, and/or importing into the United States infrastructures that perform a method comprising the steps of: receiving, over the distributed electronic network, a first request from a network device for access to the information account and consumer authentication information in response to the consumer inputting the consumer authentication information while interacting with a first web-site; in response to the request, authenticating the consumer with the database management system based on the consumer

authentication information, thereby providing the consumer with access to the information account stored in the central data repository, a first consumer information element of the information account comprising one or more name fields to identify the consumer, a second consumer information element of the information account comprising one or more geographic address fields associated with the consumer; in response to authenticating the consumer, automatically managing subsequent authentications of the consumer with the database management system so that the consumer will not be required to again input the consumer authentication information upon initiating a second request for access to the information account while interacting with a subsequent web-site that is configured to provide access to the information account upon authentication of the consumer; in response to the first, second, and subsequent requests for access to the information account stored in the central data repository, retrieving one or more consumer information element from the information account by filtering data from the information account with the database management system based on an identification of a web-site being accessed by the consumer; sending the retrieved consumer information elements over the distributed electronic network; parsing the retrieved consumer information elements; and autopopulating input fields of a displayed web page file of the website being accessed by the consumer with the consumer information elements.

56. For example, the Accused Infrastructures receive, over the distributed electronic network, a first request from a network device for access to the information account and consumer authentication information in response to the consumer inputting the consumer authentication information while interacting with a first website. For example, the Accused Infrastructures of the IKEA Webstore receive a first request from a network device, such as a client device (*e.g.*, a consumer's computer, smartphone, or tablet) or a vendor server in response to a user inputting

authentication information, such as a username and password, while interacting with a first website, such as subdomain of https://www.IKEA.com/, or a microsite comprising https://www.IKEA.com/. For example, the Accused Infrastructures receive a request for access to an information account in response to a successful log-in while interacting with a first website.

57. For example, in response to the request, the Accused Infrastructures authenticate the consumer with the database management system based on the consumer authentication information (*e.g.*, username and password), thereby providing the consumer with access to the information account stored in the central data repository including their saved name and geographic address information. For example, on information and belief, the IKEA Webstore authenticates the consumer with a DBMS, such as DB2, based on a username and password. For example, the consumer is thereby provided with access to information stored in the central data repository, such as the WebSphere Commerce database of the IKEA Webstore. For example, the standard database schema of the WebSphere Commerce database, which is, on information and belief, implemented in the Accused Infrastructures, further shows account profile information to be stored in the central data repository.

58. For example, the Accused Infrastructures practice, in response to authenticating the consumer, automatically managing subsequent authentications of the consumer with the database management system so that the consumer will not be required to again input the consumer authentication information upon initiating a second request for access to the information account while interacting with a subsequent website that is configured to provide access to the information account upon authentication of the consumer. For example, the Accused Infrastructures utilize an authentication token to automatically authenticate a user upon subsequent requests for access to

the information account while accessing with a subsequent website, such as a checkout microsite, subdomains comprising the checkout module of https://www.IKEA.com/.

59. For example, the Accused Infrastructures practice, in response to the first, second, and subsequent requests for access to the information account stored in the central data repository, retrieve one or more consumer information element from the information account by filtering data from the information account with the database management system based on an identification of a website being accessed by the consumer. For example, on information and belief, the Accused Infrastructures retrieve consumer information elements, such as a shipping address, from the information account by filtering data from a user information account. For example, on information and belief, the Accused Infrastructures filter data with a DBMS (*e.g.*, DB2) based on identification of a website being accessed by the consumer, such as the checkout of the IKEA Webstore.

60. On information and belief, the Accused Infrastructures send the retrieved consumer information elements over the distributed electronic network. For example, the Accused Infrastructures send the retrieved information elements over the internet.

61. On information and belief, the Accused Infrastructures parse the retrieved consumer information elements. For example, on information and belief, the Accused Infrastructures parse the retrieved information elements at least according to input field.[6]

62. For example, the Accused Infrastructures practice autopopulating the selected consumer information elements into at least one input field of a web page file. For example, the

6 https://help.hcltechsw.com/commerce/9.0.0/webservices/refs/rwvrestxmlformat.html?hl=parse%2Cinput

selected consumer information elements, such as shipping or payment information, are autopopulated into input fields of a web page file of the IKEA Webstore Checkout.

63. Defendant has indirectly infringed and continues to indirectly infringe one or more claims of the ’875 Patent by knowingly and intentionally inducing others, including end users and service providers of the Accused Infrastructures, to directly infringe, either literally or under the doctrine of equivalents, by making, using, offering to sell, selling, and/or importing into the United States products that include infringing technology, such as the Accused Infrastructure that practice the systems and methods covered by the ’875 Patent.

64. Defendant, with knowledge that these products, or the use thereof, infringe the ’875 Patent knowingly and intentionally induced, and continues to knowingly and intentionally induce, direct infringement of the ’875 Patent by providing these Accused Infrastructure to end users and/or service providers for use in an infringing manner.

65. Defendant induced infringement by others, including end users, with the intent to cause infringing acts by others or, in the alternative, with the belief that there was a high probability that others, including end users, infringe the ’875 Patent, while remaining willfully blind to the infringement.

66. CXT has suffered damages as a result of Defendant’s direct and indirect infringement of the ’875 Patent in an amount to be proved at trial.

67. CXT has suffered, and will continue to suffer, irreparable harm as a result of Defendant’s infringement of the ’875 Patent for which there is no adequate remedy at law, unless Defendant’s infringement is enjoined by this Court

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a jury for all issues so triable.

PRAYER FOR RELIEF

WHEREFORE, CXT prays for relief against Defendant as follows:

a. Entry of judgment declaring that Defendant has directly and/or indirectly infringed one or more claims of each Asserted Patent;

b. Entry of judgment declaring that Defendant's infringement of the Asserted Patents is willful;

c. An order awarding damages sufficient to compensate CXT for Defendant's infringement of the Patents-in-Suit, but in no event less than a reasonable royalty, including supplemental damages post-verdict, together with pre-judgment and post-judgment interest and costs;

d. Enhanced damages pursuant to 35 U.S.C. § 284;

e. Entry of judgment declaring that this case is exceptional and awarding CXT its costs and reasonable attorney fees under 35 U.S.C. § 285;

f. An accounting for acts of infringement;

g. Such other equitable relief which may be requested and to which the Plaintiff is entitled; and

h. Such other and further relief as the Court deems just and proper.

Dated: March17, 2021

Respectfully submitted,

/s/Alfred R. Fabricant

Alfred R. Fabricant
NY Bar No. 2219392
Email: ffabricant@fabricantllp.com
Peter Lambrianakos
NY Bar No. 2894392
Email: plambrianakos@fabricantllp.com
Vincent J. Rubino, III
NY Bar No. 4557435
Email: vrubino@fabricantllp.com

FABRICANT LLP
411 Theodore Fremd Road,
Suite 206 South
Rye, NY 10580
Telephone: (212) 257-5797
Facsimile: (212) 257-5796

Justin Kurt Truelove
Texas Bar No. 24013653
Email: kurt@truelovelawfirm.com
TRUELOVE LAW FIRM, PLLC
100 West Houston
Marshall, Texas 75670
Telephone: (903) 938-8321
Facsimile: (903) 215-8510

ATTORNEYS FOR PLAINTIFF CXT SYSTEMS, INC.