

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

DATAMOTION TEXAS, LLC,

Plaintiff,

v.

ZIX CORPORATION,

Defendant.

Civil Action No. 3:16-cv-00362

JURY TRIAL DEMANDED

COMPLAINT FOR PATENT INFRINGEMENT

This is an action for patent infringement in which Plaintiff, DataMotion Texas, LLC (“DataMotion”), by and through its undersigned counsel, submits this Original Complaint against the above-named Defendant, as follows:

NATURE OF THE ACTION

1. This is a patent infringement action to stop Defendant’s infringement of United States Patent Nos. 6,684,248 (the “248 patent”) and 8,447,967 (the “967 patent”) (collectively the “Patents-in-Suit”).

THE PARTIES

2. Plaintiff, DataMotion Texas, LLC, is a Texas company.

3. Upon information and belief, Defendant, Zix Corporation (“Zix”) is a corporation established under the laws of the State of Texas, with its principal place of business located at 2711 North Haskell Avenue, Suite 2200, Dallas, Texas 75204-2960.

JURISDICTION AND VENUE

4. This action arises under the patent laws of the United States, 35 U.S.C. § 1 et seq., including 35 U.S.C. §§ 271, 281, 283, 284, and 285. This Court has subject matter jurisdiction

over this case for patent infringement pursuant to 28 U.S.C. §§ 1331 and 1338(a).

5. The Court has personal jurisdiction over Defendant, including because Defendant has minimum contacts within the State of Texas; Defendant has purposefully availed itself of the privileges of conducting business in the State of Texas; Defendant regularly conducts business within the State of Texas; and Plaintiff's cause of action arises directly from Defendant's business contacts and other activities in the State of Texas, including at least by virtue of Defendant's use, sale and/or offers to sell secured email systems and methods, including those accused systems and methods described herein, which are at least used in and/or accessible in the State of Texas. Further, this Court has general jurisdiction over Defendant, including due to its continuous and systematic contacts with the State of Texas, including because Defendant has committed patent infringement in the State of Texas and because Defendant is incorporated in and resides in the State of Texas.

6. Venue is proper in the Northern District of Texas pursuant to 28 U.S.C. §§ 1391 and 1400(b), including because Defendant has purposefully availed itself of the privileges of conducting business in this District; Defendant regularly conducts business within this District; and Plaintiff's cause of action arises directly from Defendant's business contacts and other activities in this District, including at least by virtue of Defendant's use, sale and/or offers to sell secured email systems and methods which are at least used in and/or accessible in this District. Venue is also proper in this District at least because Defendant resides in this District.

BACKGROUND

A. DataMotion, Inc.

7. DataMotion's affiliated entity, DataMotion, Inc. was founded in 1999 by security software veterans with experience in developing and architecting data security products for

military and enterprise customers. It has grown into a company that now employs 36 people.

8. DataMotion, Inc. is an online communications security company that has invested substantial resources into the development and sale of software for securely delivering data, such as email, files, and other information.

9. DataMotion, Inc. has received accolades in recognition of its groundbreaking technological developments and outstanding service in the field of online security and encryption. Notably, DataMotion has been recognized by Gartner, in its “Platform as a Service: Definition, Taxonomy and Vendor Landscape, 2011,” and was named to CIO Review’s “20 Most Promising Healthcare Consulting Providers” list. DataMotion has received full accreditation by the Direct Trusted Agent Accreditation Program (DTAAP) for HISPs from DirectTrust.org and the Electronic Healthcare Network Accreditation Commission (EHNAC). Additional recognition has come from the SC Magazine Awards, the MSD2D People’s Choice awards, and the Microsoft Partner Network. DataMotion, Inc. has invested a significant amount of financial and intellectual capital into the development of pioneering technologies such as the method for secure transmission of a message via a network where a recipient of the message need not be a party to the network or maintain an active address in the network, which is disclosed in the Patents-in-Suit.

B. The ‘248 Patent

10. On January 27, 2004, the ‘248 patent, entitled “Method of Transferring Data From a Sender to a Recipient During Which a Unique Account for the Recipient is Automatically Created if the Account Does Not Previously Exist” was duly and lawfully issued by the United States Patent and Trademark Office. The claims of the ‘248 patent are entitled to the benefit of the filing date of U.S. Provisional Application No. 60/132,203 filed May 3, 1999, U.S. Provisional Application No. 60/132,790 filed May 6, 1999 and U.S. Provisional Application No. 60/198,033

filed Apr. 18, 2000. *See* attached Exhibit A.

11. The claims of the '248 Patent cover, *inter alia*, methods for providing a secure transfer of data comprising: transferring the data to a secure database server, and upon the sender initiating a transfer of the data to a recipient, causing an inquiry to be made as to whether the recipient has an affiliation with the a network; and upon a determination of no affiliation, causing the network to dynamically create an account for the recipient comprising a storage location; storing data addressed to the recipient in the storage location; providing a notification to the recipient of the data being available; and transferring the data to the recipient upon request.

12. The claims of the '248 Patent also cover, *inter alia*, methods for providing a secure transfer of data comprising: transferring the data, including an address of a recipient, from the sender to a secure database server, causing the secure database server to create a storage location for the recipient; causing the secure database server to place data addressed to the recipient into an assigned storage location; associating the recipient with the storage location via an identifier; providing a notification to the recipient of the data being available, along with access information corresponding to the identifier for retrieving the data, transferring the addressed data to the recipient upon request; and maintaining the storage location and identifier for subsequent data transfers. The technology recited in the claims of the '248 patent provides an inventive concept and does not claim an abstract idea. The inventive concept greatly enhances and facilitates the operation of a network, such that information may be transmitted securely, to a recipient who has not installed any specialized software or previously activated an account on the network. Ex. A. at 3:56-62. For example, the '248 patent describes technology that utilizes existing e-mail systems for notification of a secured message, but provides access to the secured message from a database system located at a secured site. *Id.* at 4:26-29.

13. One inventive component of the '248 patent is the claimed methods comprise providing a secure transfer of data from a sender to an out of network recipient who lacks decryption software.

14. The technology claimed in the '248 patent does not preempt all ways for transferring data securely. For example, certain claims comprise a secure database server located in a sender's network creating an account including a storage location for an addressed recipient, providing a notification to the recipient of addressed data being available at the secure database server, transferring secured data to the addressed recipient upon request; and maintaining said storage location and said identifier for subsequent data transfers.

15. Defendant can securely transfer data without infringing the '248 patent using methods that lack the inventiveness of the claimed invention. For example, the prior art cited on the face of the '248 patent remains available for practice by the Defendant, and the '248 patent claims do not preempt practice of those prior art methods. Further, a message may be encrypted using public/private key encryption. '248 Patent, Column 3, Lines 10-15.

16. The '248 patent claims cannot be practiced by a human alone and there exists no human analogue to the methods claimed in the '248 patent. The claims are specifically directed to the secure transfer of data over a network, using a database server as an intermediary-a process that is only possible in the realm of computer networks.

17. The dependent claims of the '248 patent add additional limitations demonstrating that they are also not directed to any abstract ideas, contain inventive concepts, and do not preempt all ways of securely transferring data. Claims 2, 10, 11, 14, 20, and 21, for example, specifically limit the type of data being transferred. Claims 6, 7, 8, 16, 17, and 18 limit the circumstances in which the secure data transfer is implemented. Claims 3, 4, 5, 13, 15, 23, and 24 contain specific

limitations relating to notifying the recipient of a secure message. Claims 9 and 19 contain specific limitations relating to the use of a wireless terminal by the sender.

18. One of many inventive components of the '248 patent is the claimed set of methods for providing a secure transfer of data from a sender to a recipient over a network to which the recipient is not necessarily a party.

19. The technology claimed in the '248 patent does not preempt all ways for transferring data securely over a network. For example, the claims comprise an intermediate database server. Further, the independent claims require determining whether the addressed recipient has an affiliation with the network. The secure transfer of data need not be accomplished this way. For example, a message may be encrypted using public/private key encryption. *Id.* at 3:10-15.

C. *The '967 Patent*

20. On May 21, 2013, the '967 patent, entitled "Controlled Message Distribution" was duly and lawfully issued by the United States Patent and Trademark Office. The claims of the '967 patent are entitled to the benefit of the filing date of U.S. Provisional Application No. 60/214,934 filed June 29, 2000. *See* attached Exhibit B.

21. The claims of the '967 Patent cover, *inter alia*, methods for transmitting an email comprising the steps of: launching an email application, the email application including an interface; selecting one of a plurality of email transmitting processes via the interface; if the selected email transmitting process requires secure message transmission to a recipient, inserting email content into an electronic message addressed to a server that initiates a secure link with the recipient.

22. The technology recited in the claims of the '967 patent provides an inventive

concept and does not claim an abstract idea. The inventive concept greatly enhances and facilitates the operation of an electronic messaging system, so that, *inter alia*, electronic messages may be transmitted securely to a recipient who has not installed any specialized software. Ex. B at 5:55-61. For example, the '967 patent describes technology that utilizes existing message systems for the sending of a secured message via an interface, but provides access to the secured message from a database system located at a secured site. *Id.* at 5:18-36.

23. One inventive component of the '967 patent is the claimed methods comprise providing a secure transfer of electronic message content from a sender to an out of network recipient who lacks decryption software by selecting an email process from an interface.

24. The technology claimed in the '967 patent does not preempt all ways for transferring message content securely. For example, certain claims comprise selecting an email process to cause a secure server to initiate a secure link to a client computer, providing access to secure electronic message content without the client needing to have decryption software.

25. Defendant can securely transfer message content without infringing the '967 patent using methods that lack the inventiveness of the claimed invention. For example, the prior art cited on the face of the '967 patent remains available for practice by the Defendant, and the '967 patent claims do not preempt practice of those prior art methods. Further, message content may be encrypted using public/private key encryption.

26. The '967 patent claims cannot be practiced by a human alone and there exists no human analogue to the methods claimed in the '967 patent. The claims are specifically directed to the secure transfer of data over a network, using a server as an intermediary-a process that is only possible in the realm of computer networks.

27. The dependent claims of the '967 patent add additional limitations demonstrating

that they are also not directed to any abstract ideas, contain inventive concepts, and do not preempt all ways of securely transferring data. Claims 2 and 5, for example, specifically limit the type of link established between the server and client. Claim 3 limits the locations of the servers. Claim 6 limits the type of data being transferred.

COUNT I – INFRINGEMENT OF U.S. PATENT NO. 6,684,248

28. DataMotion repeats and realleges the allegations of the above paragraphs as if fully set forth herein.

29. DataMotion is the assignee and owner of the right, title and interest in and to the ‘248 patent, including the right to assert all causes of action arising under said patent and the right to any remedies for infringement of it, including recovery of past, present and future damages.

30. Defendant has infringed and is now infringing, including literally, jointly, and/or equivalently, the ‘248 patent, including claims 1, 3, 11, 12, 15, 21, and 22, in this judicial district, the State of Texas, and elsewhere in the United States, in violation of 35 U.S.C. § 271 through actions comprising the practicing, making, using, selling, offering for sale and/or hosting, without authority from Plaintiff, methods for providing a secure transfer of data comprising: transferring the data, including an address of a recipient, from the sender to a secure database server, causing the secure database server to create a storage location for the recipient; causing the secure database server to place data addressed to the recipient into an assigned storage location; associating the recipient with the storage location via an identifier; providing a notification to the recipient of the data being available, along with access information corresponding to the identifier for retrieving the data, transferring the addressed data to the recipient upon request; and maintaining the storage location and identifier for subsequent data transfers.

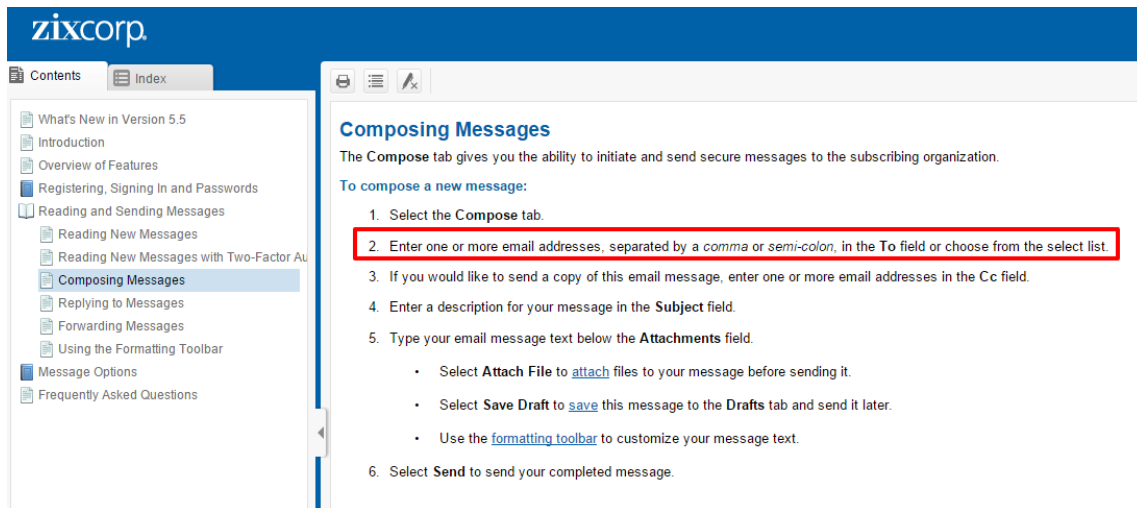
31. An exemplary description of Defendant’s infringement of exemplary independent

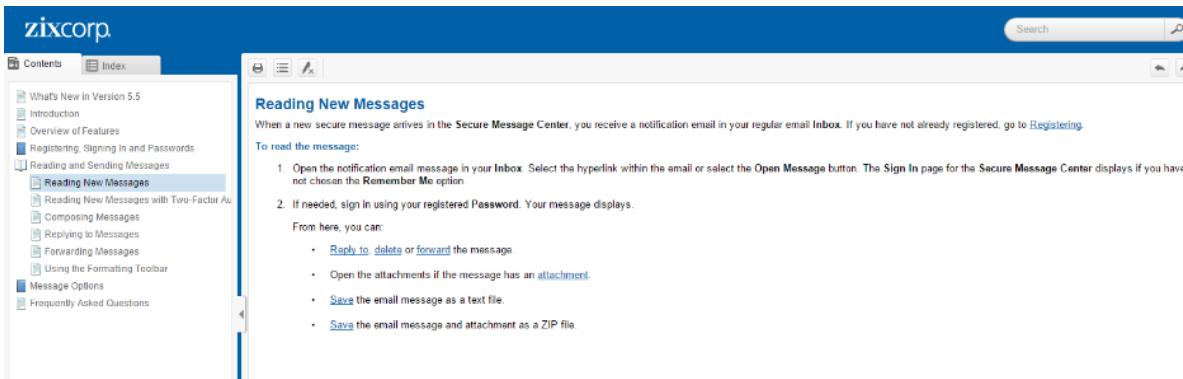
claim 1 of the '248 patent is set forth below (claim language in italics):

(a) *A method for providing a secure transfer of data (e.g., an encrypted email) from a sender to a recipient, comprising the steps of:*

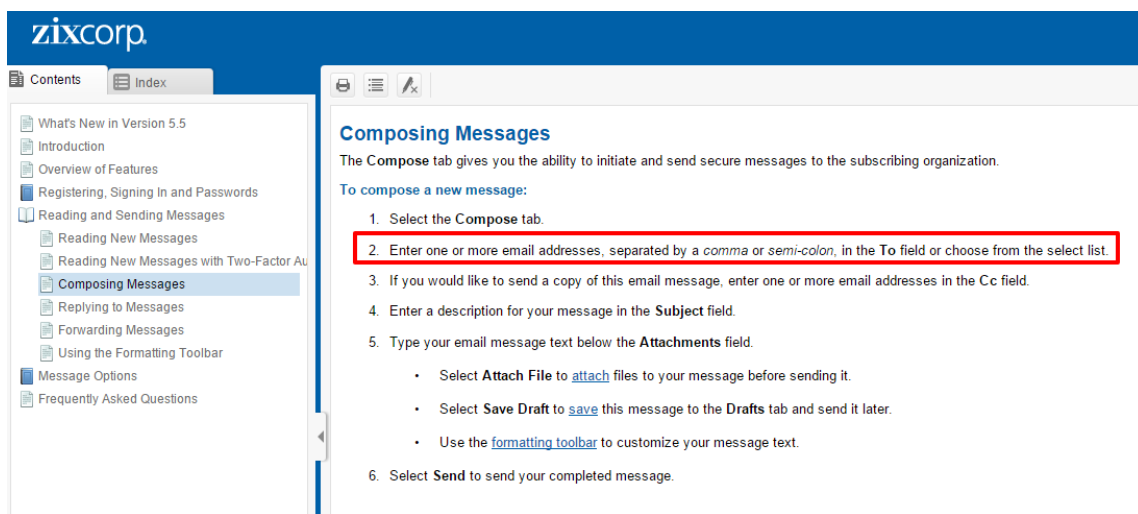


(b) *transferring said data, including an address of at least one recipient, from said sender to a secure database server located in a network serving said sender – the Zix Email Encryption system, which comprises what Zix sometimes refers to as the Zix Portal and/or Zix Message Center, sends encrypted email messages to recipient email addresses.*





When the user sends an email, the recipient's email address is included with the encrypted email.



The Zix Email Encryption system comprises a secure database server comprising one or more individual servers, for example a ZixGateway server and/or a ZixMail Cloud server. Once the recipient receives, and views, the Secure Message and accesses the hyperlink, the recipient is linked to the ZixMail server, which may be the same as, or different from, and working in tangent with, the encryption toolbar server, via HTTP and/or HTTPS (collectively referred to as “HTTPS”),

(c) upon said sender initiating a transfer of said data to said addressed recipient, causing an inquiry to be made as to whether said addressed recipient has an affiliation with said network – when an encrypted email is sent, the Zix Email Encryption system determines whether the recipient's address is within Zix's database (e.g., whether the recipient has a Zix account or is a Zix customer):

Receiving encrypted email is just as easy. When a ZixGateway customer sends encrypted email to another ZixGateway customer, the email and replies are delivered securely and transparently. No extra steps or passwords are needed. Just in case your receiver isn't a ZixGateway user, we use the **Best Method of Delivery** to deliver the encrypted email in the easiest manner.

For recipients who do not have Zix Email Encryption, ZixPort offers a "pull" delivery method for convenient access through a secure, mobile-friendly Web portal. ZixPort sends a notification email that links and "pulls" your recipients to the portal where they can read, reply and reply-all to encrypted messages.

To get started, users go through a one-time registration process. Once registered, the user signs in to view the message and any attachments with easy access anytime, anywhere on any desktop or mobile device. There is no client software to install or maintain, making email encryption easy for any recipient.

(d) *upon a determination of no affiliation, causing said network to dynamically create an account for said addressed recipient, the account including a storage location and an identifier associating said addressed recipient with said storage location – if the recipient is not within the database (i.e., the recipient has no affiliation), the email is encrypted and stored within the Zix Email Encryption system's database, which creates an account dynamically.*

Reading New Messages

When a new secure message arrives in the Secure Message Center, [you receive a notification email in your regular email Inbox](#). If you have not already registered, go to [Registering](#).

To read the message:

1. Open the notification email message in your Inbox. Select the hyperlink within the email or select the **Open Message** button. The Sign In page for the Secure Message Center displays if you have not chosen the **Remember Me** option.
2. If needed, sign in using your registered **Password**. Your message displays.

From here, you can:

- [Reply to](#), [delete](#) or [forward](#) the message.
- Open the attachments if the message has an [attachment](#).
- [Save](#) the email message as a text file.
- [Save](#) the email message and attachment as a ZIP file.

When a message is sent via Secure Message Center, a notification email is sent to the recipient (see example below). **If this is the first time the recipient received an encrypted email from that sender's company, then the recipient will need to create an account (your email address and a password) in order to read the message. If the recipient has previously received encrypted messages from the sender's company, then the recipient will only be required to re-enter their password to open and read the message.**

You have a ZixMessage Center Message from SENDER@DOMAIN:

Click the link below to view your secure message. If your email program does not support active links, please cut and paste the link displayed below into the "Address" or "Location" field of your browser and press "Enter" or "Go".

<https://zixmessagecenter.com/s/e?m=ABDawDyowkwhSe1vSiEiE1zp&em=RECIPIENT%40DOMAIN%2ecom>

Please do not reply to this e-mail. This message was auto-generated by the sender's Zix security system. To reply to the sender, please go to your secure message by clicking on the link above.

This message will expire on Feb 15, 2007 @ 10:45 (CST).

The created account comprises a mailbox within the Zix Email Encryption system which stores the recipient's received encrypted messages for a time period up to 60 days, and the account is ultimately identified by the recipient's username and password, which are used to log in to the account, for example:

Reading New Messages

When a new secure message arrives in the Secure Message Center, [you receive a notification email in your regular email Inbox](#). If you have not already registered, go to [Registering](#).

To read the message:

1. Open the notification email message in your **Inbox**. Select the hyperlink within the email or select the **Open Message** button. The **Sign In** page for the **Secure Message Center** displays if you have not chosen the **Remember Me** option.
2. If needed, sign in using your registered **Password**. Your message displays.

From here, you can:

- [Reply to](#), [delete](#) or [forward](#) the message.
- Open the attachments if the message has an [attachment](#).
- [Save](#) the email message as a text file.
- [Save](#) the email message and attachment as a ZIP file.

When a message is sent via Secure Message Center, a notification email is sent to the recipient (see example below). If this is the first time the recipient received an encrypted email from that sender's company, then the recipient will need to create an account (your email address and a password) in order to read the message. If the recipient has previously received encrypted messages from the sender's company, then the recipient will only be required to re-enter their password to open and read the message.

You have a ZixMessage Center Message from SENDER@DOMAIN:

Click the link below to view your secure message. If your email program does not support active links, please cut and paste the link displayed below into the "Address" or "Location" field of your browser and press "Enter" or "Go".

<https://zixmessagecenter.com/s/e?m=ABDawDyowkwhSe1vSiEiE1zp&em=RECIPIENT%40DOMAIN%2ecom>

Please do not reply to this e-mail. This message was auto-generated by the sender's Zix security system. To reply to the sender, please go to your secure message by clicking on the link above.

This message will expire on Feb 15, 2007 @ 10:45 (CST).

Registering

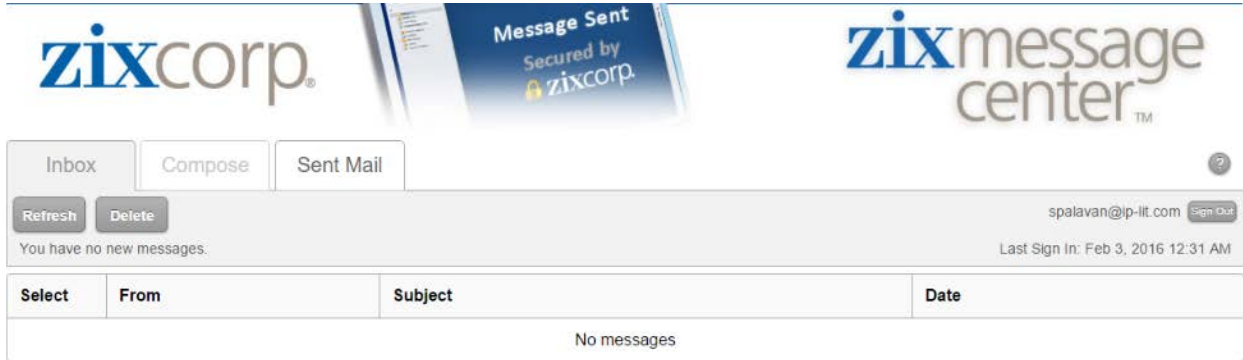
The first time you receive a secure email, you are asked to register at the **Secure Message Center**. Registration is a one-time, quick and easy process. You receive an email message in your email **Inbox** notifying you that you have a message in the **Secure Message Center**.

1. Select the **Open Message** button.

Note: If your email program does not support active links, copy and paste the link provided in the message into your browser.

2. On the **Registration** page, enter a **Password** that complies with the password rules shown.
3. Re-enter your password.
4. If you want to view the **Secure Message Center** in another language, select the language you want from the **Language** drop down box. For more information on using the Language feature, see [Specifying Your Language](#).
5. Select **Register**.

The **Secure Message Center** opens and displays your email message. You now have access to the **Secure Message Center**. You may also register by going directly to the **Secure Message Center Sign In** page and select the **Register** button.



The mailbox is initially associated with the recipient's email address (ultimately with the recipient's email address and password), and is presented to the recipient when he or she logs in, for example:

Signing In

If this is your first time to use the Secure Message Center, you must register before signing in. See [Registering](#) for more information.

To sign in to the **Secure Message Center**:

1. Enter your registered **Email Address**.
2. If you want to view the **Secure Message Center** in another language, select the language you want from the **Language** drop-down box.

Note: For more information on using the Language feature, see [Specifying Your Language](#).

3. Enter your **Password**.

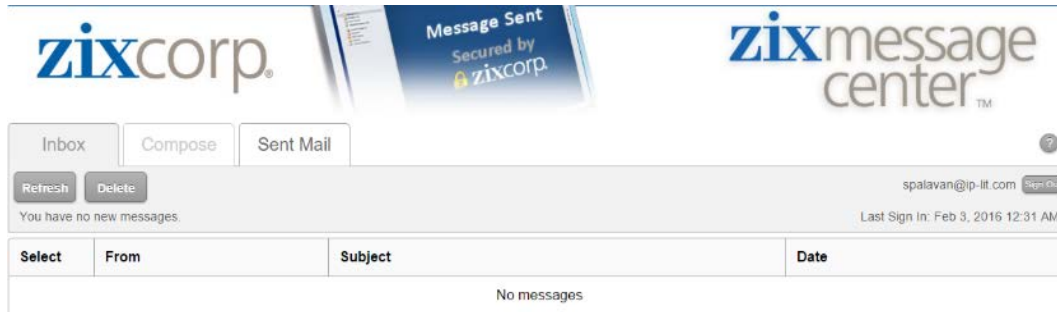
4. Select the **Remember Me** check box if you want to save your sign in information on this computer.

Note: If you **Sign Out**, you will have to re-enter your email address and password the next time you sign in. If you want your password to be saved, close the Internet browser without using **Sign Out**.

5. Select **Sign In**.

If you previously signed into your account, the date and time of your last account access appears on this page as a security precaution.

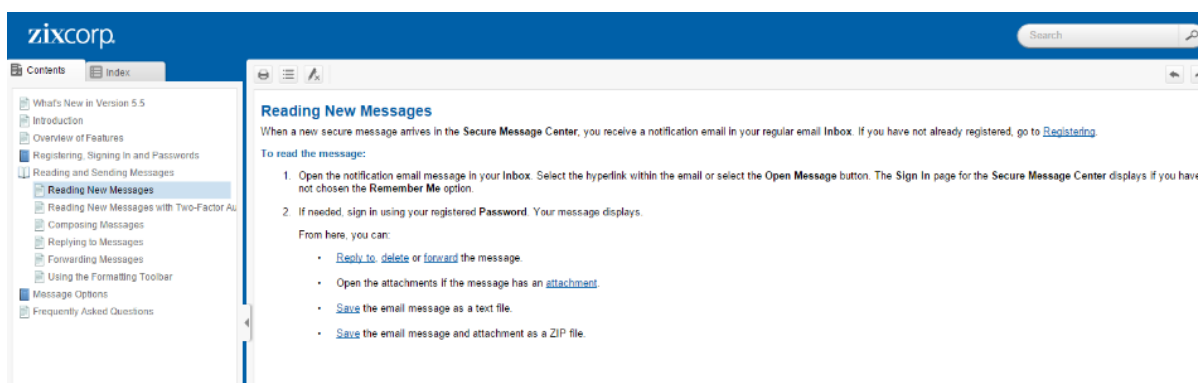
(e) *storing data addressed to said recipient in said storage location* – as the recipient receives encrypted emails, they are stored within the recipient’s Zix message center mailbox until they expire, for example:



18. How long are messages held in the Secure Message Center?

This message retention setting is configured by the company that sent you the email message. A company can set the message expiry to between 7 days (minimum) and 60 days (maximum). Once a secure message has expired, it is permanently deleted and cannot be recovered by ZixCorp. If you need a copy of an expired message, please contact the originator.

(f) *providing a notification to said addressed recipient of said addressed data being available at said secure database server* – the Zix Email Encryption system sends a notification email to notify the recipient of the message being within the recipient’s mailbox in the Zix Email Encryption system, for example:



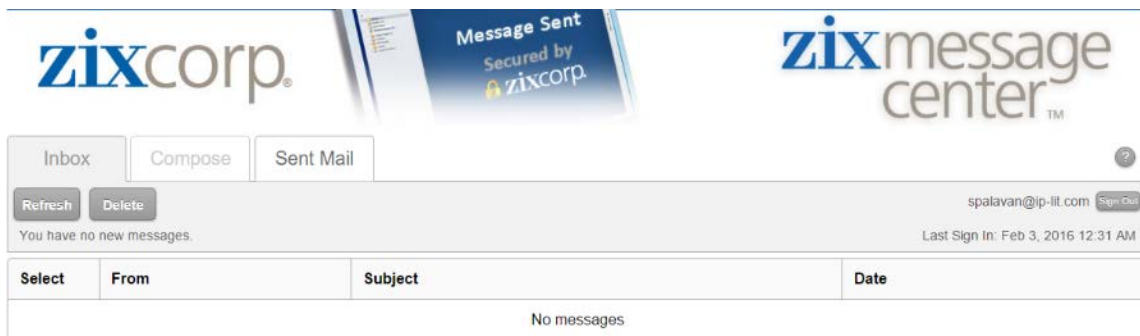
You have a ZixMessage Center Message from SENDER@DOMAIN:

Click the link below to view your secure message. If your email program does not support active links, please cut and paste the link displayed below into the "Address" or "Location" field of your browser and press "Enter" or "Go".

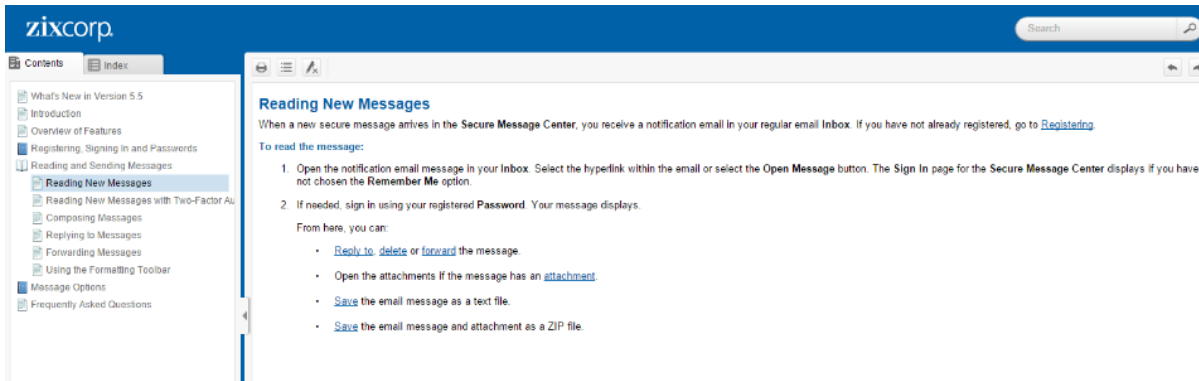
<https://zixmessagecenter.com/s/e?m=ABDawDyowkwhSe1vSiEiE1zp&em=RECIPIENT%40DOMAIN%2ecom>

Please do not reply to this e-mail. This message was auto-generated by the sender's Zix security system. To reply to the sender, please go to your secure message by clicking on the link above.

This message will expire on Feb 15, 2007 @ 10:45 (CST).



(g) *transferring said addressed data to said addressed recipient upon a request from said addressed recipient* – the Zix Email Encryption system provides access to the recipient via a secured link which comprises an HTTPS connection to an associated webmail account, including hosted by the Zix Email Encryption system's server, including a mailbox. When the recipient clicks on the hyperlink in the notification email, he or she is presented with a login prompt which initiates an HTTPS connection with the recipient. Once the recipient is authenticated (i.e., logs in), a verified session with the recipient's device is created with the Zix Email Encryption system, and the original, decrypted email is presented to the recipient via the session in the recipient's mailbox, for example:



You have a ZixMessage Center Message from SENDER@DOMAIN:

Click the link below to view your secure message. If your email program does not support active links, please cut and paste the link displayed below into the "Address" or "Location" field of your browser and press "Enter" or "Go".

<https://zixmessagecenter.com/s/e?m=ABDawDyowkwhSe1vSiEiE1zp&em=RECIPIENT%40DOMAIN%2ecom>

Please do not reply to this e-mail. This message was auto-generated by the sender's Zix security system. To reply to the sender, please go to your secure message by clicking on the link above.


This message will expire on Feb 15, 2007 @ 10:45 (CST).

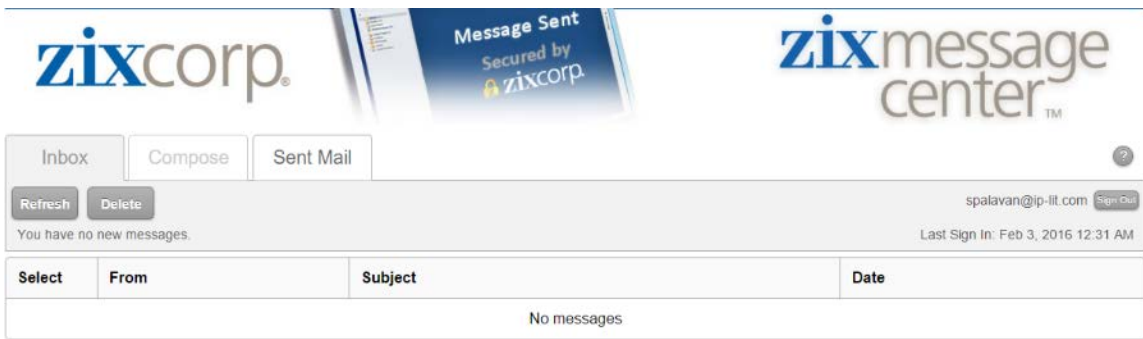
Email Address: *

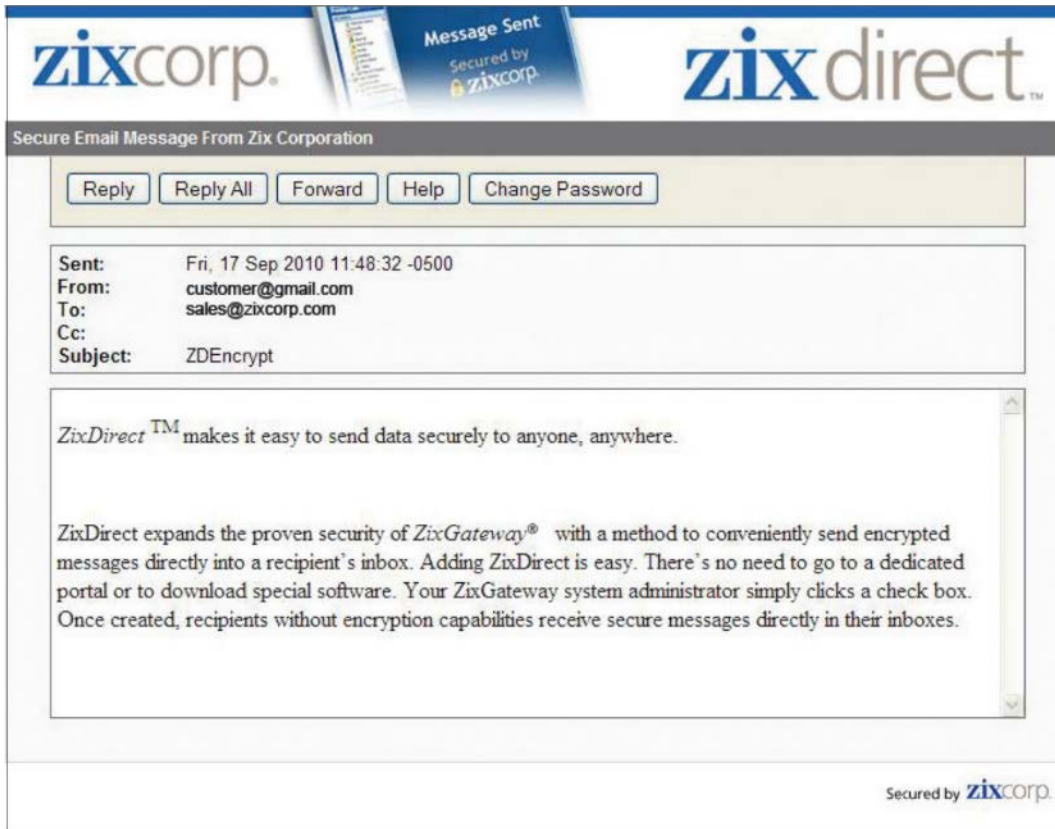
Password: *

Language: Remember Me

Alternative Login Services:







32. An exemplary description of Defendant's infringement of exemplary independent claim 12 of the '248 Patent is set forth below (claim language in italics):

(a) *A method for providing a secure transfer of data (e.g., an encrypted email) from a sender to a recipient, comprising the steps of: - see ¶36(a) above showing the Zix secure message system.*

(b) *transferring said data, including an address of at least one recipient, from said sender to a secure database server located in a network serving said sender – see ¶36(b) above showing a user sending an encrypted email to a recipient, including the recipient's email address.*

(c) *causing said secure database server to create a storage location for said addressed recipient, when no storage location previously exists for said recipient - email is encrypted and stored within the Zix Email Encryption system's database in a storage location for the recipient, for example:*

Reading New Messages

When a new secure message arrives in the Secure Message Center, you receive a notification email in your regular email Inbox. If you have not already registered, go to [Registering](#).

To read the message:

1. Open the notification email message in your Inbox. Select the hyperlink within the email or select the **Open Message** button. The **Sign In** page for the Secure Message Center displays if you have not chosen the **Remember Me** option.
2. If needed, sign in using your registered **Password**. Your message displays.

From here, you can:

- [Reply to](#), [delete](#) or [forward](#) the message.
- Open the attachments if the message has an [attachment](#).
- [Save](#) the email message as a text file.
- [Save](#) the email message and attachment as a ZIP file.

When a message is sent via Secure Message Center, a notification email is sent to the recipient (see example below). If this is the first time the recipient received an encrypted email from that sender's company, then the recipient will need to create an account (your email address and a password) in order to read the message. If the recipient has previously received encrypted messages from the sender's company, then the recipient will only be required to re-enter their password to open and read the message.

When a message is sent via Secure Message Center, a notification email is sent to the recipient (see example below). If this is the first time the recipient received an encrypted email from that sender's company, then the recipient will need to create an account (your email address and a password) in order to read the message. If the recipient has previously received encrypted messages from the sender's company, then the recipient will only be required to re-enter their password to open and read the message.

You have a ZixMessage Center Message from SENDER@DOMAIN:

Click the link below to view your secure message. If your email program does not support active links, please cut and paste the link displayed below into the "Address" or "Location" field of your browser and press "Enter" or "Go".

<https://zixmessagecenter.com/s/e?m=ABDawDyowkwhSe1vSiEiIzp&em=RECIPIENT%40DOMAIN%2ecom>

Please do not reply to this e-mail. This message was auto-generated by the sender's Zix security system. To reply to the sender, please go to your secure message by clicking on the link above.

This message will expire on Feb 15, 2007 @ 10:45 (CST).

(d) causing said secure database server to place data addressed to said recipient into the storage location assigned to said addressed recipient - as the recipient receives encrypted emails, they are stored within the recipient's mailbox until they expire, for example:



18. How long are messages held in the Secure Message Center?

This message retention setting is configured by the company that sent you the email message. A company can set the message expiry to between 7 days (minimum) and 60 days (maximum). Once a secure message has expired, it is permanently deleted and cannot be recovered by ZixCorp. If you need a copy of an expired message, please contact the originator.

(e) *associating said recipient with said storage location via an identifier* - the account is ultimately identified by the recipient's username and password, which are used to log in to the account, for example:

Reading New Messages

When a new secure message arrives in the Secure Message Center, you receive a notification email in your regular email Inbox. If you have not already registered, go to [Registering](#).

To read the message:

1. Open the notification email message in your Inbox. Select the hyperlink within the email or select the **Open Message** button. The **Sign In** page for the Secure Message Center displays if you have not chosen the **Remember Me** option.
2. If needed, sign in using your registered **Password**. Your message displays.

From here, you can:

- [Reply to](#), [delete](#) or [forward](#) the message.
- Open the attachments if the message has an [attachment](#).
- [Save](#) the email message as a text file.
- [Save](#) the email message and attachment as a ZIP file.

When a message is sent via Secure Message Center, a notification email is sent to the recipient (see example below). If this is the first time the recipient received an encrypted email from that sender's company, then the recipient will need to create an account (your email address and a password) in order to read the message. If the recipient has previously received encrypted messages from the sender's company, then the recipient will only be required to re-enter their password to open and read the message.

When a message is sent via Secure Message Center, a notification email is sent to the recipient (see example below). If this is the first time the recipient received an encrypted email from that sender's company, then the recipient will need to create an account (your email address and a password) in order to read the message. If the recipient has previously received encrypted messages from the sender's company, then the recipient will only be required to re-enter their password to open and read the message.

You have a ZixMessage Center Message from SENDER@DOMAIN:

Click the link below to view your secure message. If your email program does not support active links, please cut and paste the link displayed below into the "Address" or "Location" field of your browser and press "Enter" or "Go".

<https://zixmessagecenter.com/s/e?m=ABDawDyowkwhSe1vSiEIEIzp&em=RECIPIENT%40DOMAIN%2ecom>

Please do not reply to this e-mail. This message was auto-generated by the sender's Zix security system. To reply to the sender, please go to your secure message by clicking on the link above.

This message will expire on Feb 15, 2007 @ 10:45 (CST).

Registering

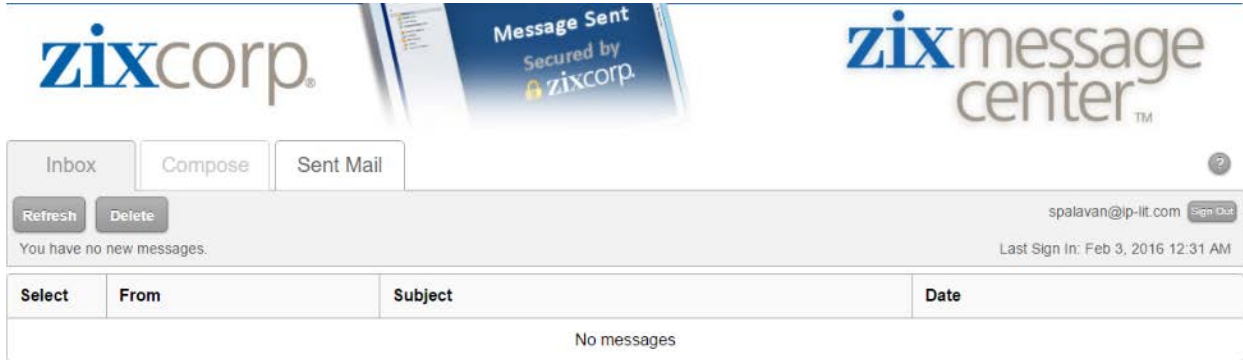
The first time you receive a secure email, you are asked to register at the **Secure Message Center**. Registration is a one-time, quick and easy process. You receive an email message in your email **Inbox** notifying you that you have a message in the **Secure Message Center**.

1. Select the **Open Message** button.

Note: If your email program does not support active links, copy and paste the link provided in the message into your browser.

2. On the **Registration** page, enter a **Password** that complies with the password rules shown.
3. Re-enter your password.
4. If you want to view the **Secure Message Center** in another language, select the language you want from the **Language** drop down box. For more information on using the Language feature, see [Specifying Your Language](#).
5. Select **Register**.

The **Secure Message Center** opens and displays your email message. You now have access to the **Secure Message Center**. You may also register by going directly to the **Secure Message Center Sign In** page and select the **Register** button.



(f) *providing a notification to said addressed recipient of said addressed data being available at said secure database server along with access information corresponding to said identifier for retrieving said addressed data therefrom – see ¶136(f) above showing the Zix Email Encryption system sending a notification email. The Zix Email Encryption system presents the notification, e.g., the sign in prompt, to the recipient, including access information, e.g., a sign-in button for accessing the secured data, for example:*

Reading New Messages

When a new secure message arrives in the **Secure Message Center**, [you receive a notification email in your regular email Inbox](#). If you have not already registered, go to [Registering](#).

To read the message:

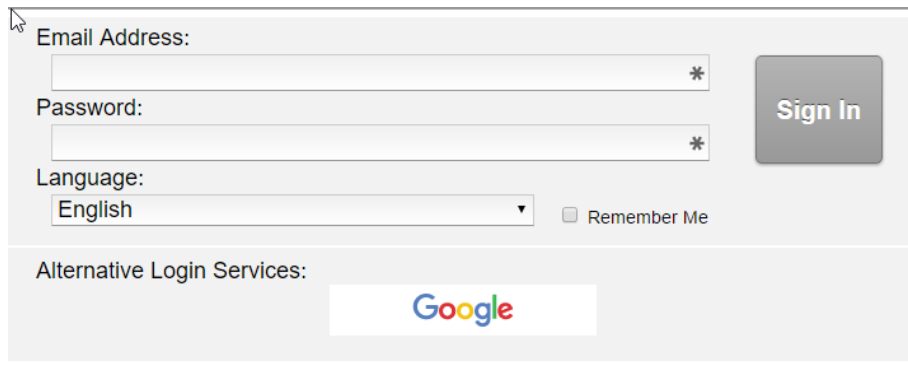
1. Open the notification email message in your **Inbox**. Select the hyperlink within the email or select the **Open Message** button. The **Sign In** page for the **Secure Message Center** displays if you have not chosen the **Remember Me** option.
2. If needed, sign in using your registered **Password**. Your message displays.

From here, you can:

- [Reply to](#), [delete](#) or [forward](#) the message.
- Open the attachments if the message has an [attachment](#).
- [Save](#) the email message as a text file.
- [Save](#) the email message and attachment as a ZIP file.

When a message is sent via **Secure Message Center**, a notification email is sent to the recipient (see example below). If this is the first time the recipient received an encrypted email from that sender's company, then the recipient will need to create an account (your email address and a password) in order to read the message. If the recipient has previously received encrypted messages from the sender's company, then the recipient will only be required to re-enter their password to open and read the message.

When a message is sent via Secure Message Center, a notification email is sent to the recipient (see example below). If this is the first time the recipient received an encrypted email from that sender's company, then the recipient will need to create an account (your email address and a password) in order to read the message. If the recipient has previously received encrypted messages from the sender's company, then the recipient will only be required to re-enter their password to open and read the message.



(g) *transferring said addressed data to said addressed recipient upon a request from said addressed recipient – see ¶36(g) above showing the Zix transferring the decrypted message to the recipient.*


(h) *maintaining said storage location and said identifier for subsequent data transfers – as the recipient receives encrypted emails, they are stored within the recipient's mailbox such that for subsequent viewings of the same encrypted message, or any future encrypted messages, the recipient may log into the mailbox and see all received messages until the message expires, for example:*

Email Address: *

Password: *

Language: English Remember Me

Alternative Login Services:










Inbox Compose Sent Mail

Refresh Delete
spalavan@ip-lit.com [Sign Out](#)

You have no new messages. Last Sign In: Feb 3, 2016 12:31 AM

Select	From	Subject	Date
No messages			


Secure Email Message From Zix Corporation

Reply Reply All Forward Help Change Password

Sent: Fri, 17 Sep 2010 11:48:32 -0500
From: customer@gmail.com
To: sales@zixcorp.com
Cc:
Subject: ZDEncrypt

*ZixDirect*TM makes it easy to send data securely to anyone, anywhere.

ZixDirect expands the proven security of *ZixGateway*[®] with a method to conveniently send encrypted messages directly into a recipient's inbox. Adding ZixDirect is easy. There's no need to go to a dedicated portal or to download special software. Your ZixGateway system administrator simply clicks a check box. Once created, recipients without encryption capabilities receive secure messages directly in their inboxes.

Secured by 

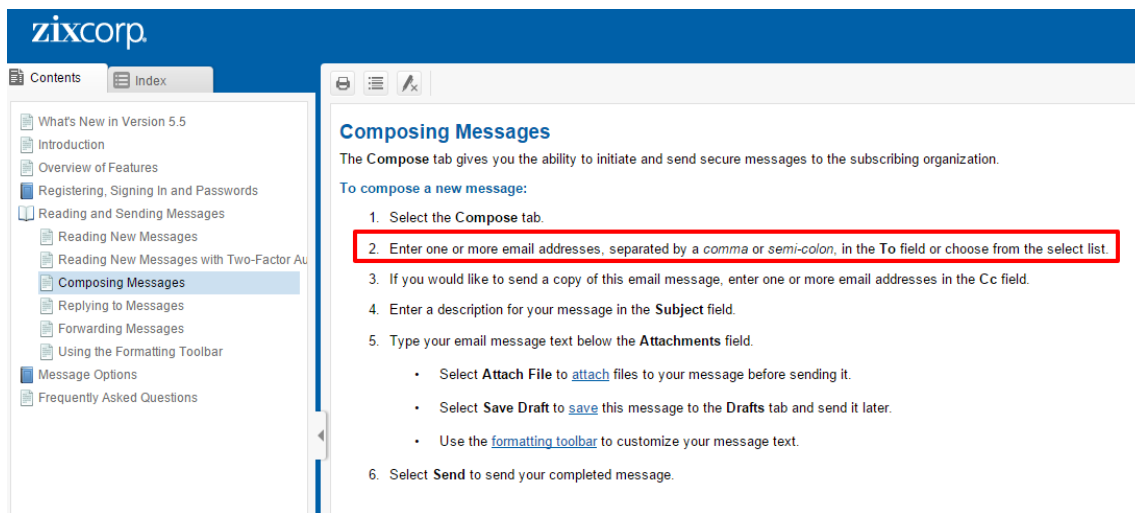
18. How long are messages held in the Secure Message Center?

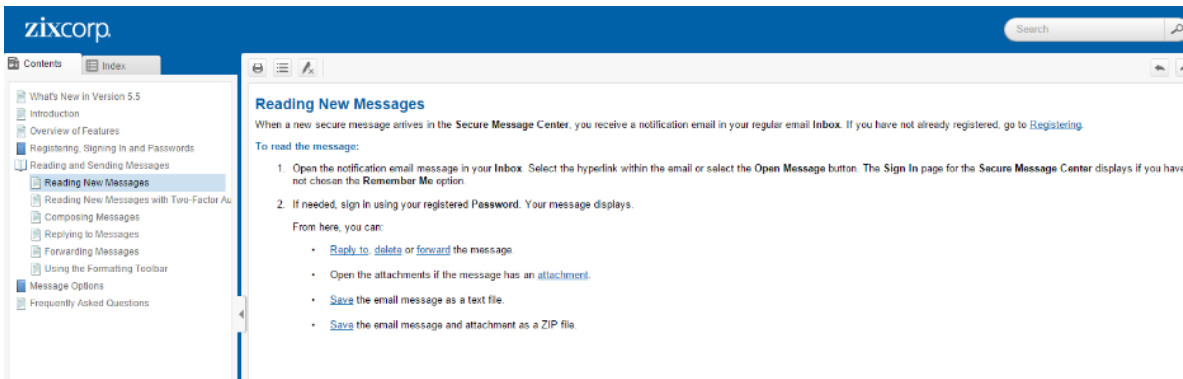
This message retention setting is configured by the company that sent you the email message. A company can set the message expiry to between 7 days (minimum) and 60 days (maximum). Once a secure message has expired, it is permanently deleted and cannot be recovered by ZixCorp. If you need a copy of an expired message, please contact the originator.

33. An exemplary description of Defendant’s infringement of exemplary independent claim 22 of the ’248 Patent is set forth below (claim language in italics):

(a) *In a network, a method of data transfer comprising the steps of: - see ¶36(a) above showing the Zix Email Encryption system permits sending encrypted emails from within a network.*

(b) *upon a sender request to transfer email from the sender to a recipient, determining if a storage location associated with the recipient exists in the network – the Zix Email Encryption system permit a sender to send encrypted data to message recipients, for example:*





When an encrypted email is sent, the Zix Email Encryption system determines whether the recipient's address is within Zix's database (e.g., the recipient has a Zix account or is a Zix customer):

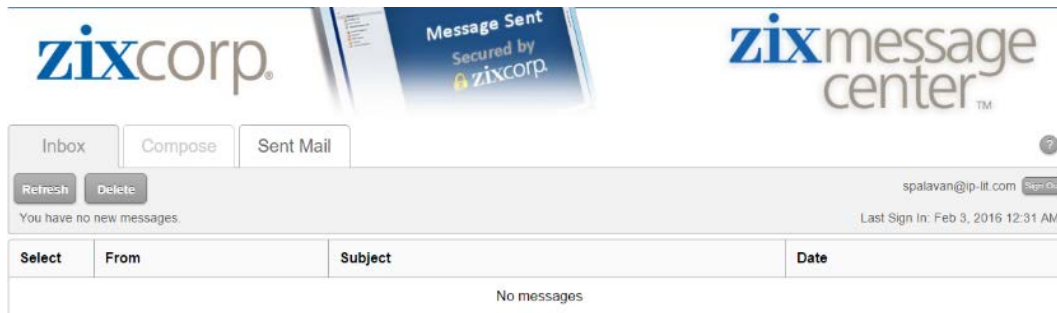
Receiving encrypted email is just as easy. When a ZixGateway customer sends encrypted email to another ZixGateway customer, the email and replies are delivered securely and transparently. No extra steps or passwords are needed. Just in case your receiver isn't a ZixGateway user, we use the **Best Method of Delivery** to deliver the encrypted email in the easiest manner.

For recipients who do not have Zix Email Encryption, ZixPort offers a "pull" delivery method for convenient access through a secure, mobile-friendly Web portal. ZixPort sends a notification email that links and "pulls" your recipients to the portal where they can read, reply and reply-all to encrypted messages.

To get started, users go through a one-time registration process. Once registered, the user signs in to view the message and any attachments with easy access anytime, anywhere on any desktop or mobile device. There is no client software to install or maintain, making email encryption easy for any recipient.

(c) *if no storage location associated with the recipient exists, automatically creating a unique email account for the recipient, the email account including a storage location and an identifier associating the recipient with the storage location – see ¶36(d) showing that the Zix Email Encryption system automatically creates accounts for recipients.*

(d) *storing the email in the storage location - as the recipient receives encrypted emails, they are stored within the recipient's mailbox until they expire, for example:*



18. How long are messages held in the Secure Message Center?

This message retention setting is configured by the company that sent you the email message. A company can set the message expiry to between 7 days (minimum) and 60 days (maximum). Once a secure message has expired, it is permanently deleted and cannot be recovered by ZixCorp. If you need a copy of an expired message, please contact the originator.

(e) *maintaining said unique email account for subsequent data transfers – see ¶37(h)*

showing that the Zix Email Encryption system maintains the recipient’s account, including the mailbox and any received emails.

34. Defendant infringes the ‘248 Patent, including claims 1, 3, 11, 12, 15, 21, and 22, by and through at least their practicing, making, using, offering for sale, selling, and/or hosting of methods comprising at least the Zix SecureMail system, including at least the following products, ZixGateway, ZixVPM, and ZixMail (including a plugin formerly known as ZixSelect), and receiver products, ZixPort and ZixDirect, as well as additional functionality products including Zix Secure Compose, ZixDirectory, and ZixMobility.

35. Additionally, or in the alternative, upon information and belief, Defendant has induced infringement of the ‘248 Patent in this judicial district, the State of Texas, and elsewhere in the United States, by intentionally inducing infringement of the ‘248 Patent, including by aiding or abetting the infringement of its end users and/or customers, including at least Comerica Bank, Comerica Incorporated, Comerica Bank & Trust, N.A. (“Comerica”), Commerce Bancshare, Inc., Commerce Bank (“Commerce”), by and through at least Defendant’s practicing and/or hosting methods comprising at least the above-described Zix Email Encryption system. Upon information

and belief, such aiding and abetting comprises hosting, providing software and/or providing instructions. Upon information and belief, such induced infringement has occurred since Defendant became aware of the '248 Patent, which at a minimum occurred in late May or early June 2015 by virtue of DataMotion's May 28, 2015 patent infringement lawsuits against Commerce and Comerica, and Defendant's inducement of infringement comprises Defendant's knowledge that the induced acts constitute patent infringement.

36. Additionally, or in the alternative, upon information and belief, Defendant contributed to infringement of the '248 patent in this judicial district, the State of Texas, and elsewhere in the United States, by actions comprising making, selling and/or offering for sale the Zix Email Encryption system, which at a minimum is used in practicing the methods of the '248 patent. The Zix Email Encryption system contributes to the direct infringement of the '248 patent by customers and/or other end users in this judicial district, the State of Texas and elsewhere in the United States.

37. Upon information and belief, the Zix Email Encryption system is especially made or especially adapted for uses and practices which constitute infringement of the '248 patent. The Zix Email Encryption system is not a staple article or commodity of commerce suitable for substantial non-infringing uses, including at least because it is especially made or especially adapted for uses and practices which constitute infringement of the '248 patent.

38. As noted above, at a minimum, Defendant became aware of the '248 patent in late May or early June 2015. On information and belief, Defendant's contributory infringement comprises its knowledge that the Zix Email Encryption system is especially made or especially adapted for uses and/or practices which constitute infringement of the '248 patent and it is not a staple article or commodity of commerce suitable for substantial non-infringing uses. Such

knowledge is evidenced by the fact that infringement of the '248 patent from the use of the Zix Email Encryption system is clear, evident, and unmistakable to anyone aware of both the '248 patent and of the details of the uses and practices employed in connection with the Zix Email Encryption system. It is similarly clear, evident, and unmistakable to anyone aware of both the '248 patent and of the details of the uses and practices employed in connection with the Zix Email Encryption system that it is especially made or especially adapted for uses and/or practices which constitute infringement of the '248 patent and it does not comprise a staple article or commodity of commerce suitable for substantial non-infringing uses. Defendant would necessarily be aware of the details of the methods used and practiced in connection with the Zix Email Encryption system at the time it became aware of the '248 patent, and at that point it would necessarily become clear and unmistakable to Defendant that at least its customers and end users were infringing the '248 patent, that the Zix Email Encryption system is, at a minimum, contributing to such infringement, and that the Zix Email Encryption system is especially made or especially adapted for uses and practices which constitute infringement of the '248 patent, and it is not a staple article or commodity of commerce suitable for substantial non-infringing uses. Since Defendant became aware of the '248 patent it has necessarily possessed such knowledge.

39. On information and belief, Defendant has also had at least constructive notice of the '248 Patent pursuant to the Patent Act. Plaintiff reserves the right to take discovery regarding Defendant's first actual notice of the '248 Patent.

40. Each of Defendant's aforesaid activities have been without authority and/or license from Plaintiff.

COUNT II – INFRINGEMENT OF U.S. PATENT NO. 8,447,967

41. DataMotion repeats and realleges the allegations of the above paragraphs as if fully

set forth herein.

42. DataMotion is the assignee and owner of the right, title and interest in and to the '967 patent, including the right to assert all causes of action arising under said patents and the right to any remedies for infringement of them, including the recovery of past, present and future damages.

43. Defendant has infringed and is now infringing, including literally, jointly, and/or equivalently, the '967 Patent, including claims 1 and 3-6, in this judicial district, the State of Texas, and elsewhere in the United States, in violation of 35 U.S.C. § 271 through actions comprising the practicing, making, using, and/or hosting, without authority from Plaintiff, methods for transmitting an email comprising the steps of: launching an email application, the email application including an interface; selecting one of a plurality of email transmitting processes via the interface; if the selected email transmitting process requires secure message transmission to a recipient, inserting email content into an electronic message addressed to a server that initiates a secure link with the recipient.

44. An exemplary description of Defendant's infringement of exemplary independent claim 1 of the '967 Patent is set forth below (claim language in italics):

(a) *An electronic mail system comprising:* - the Zix Email Encryption system comprises an electronic mail system comprising code and data implemented via a software application for at least computers and mobile devices, including providing an interface for selectively initiating an email sending process, for example:

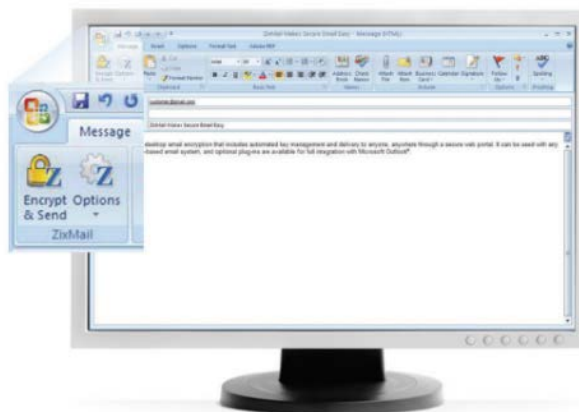


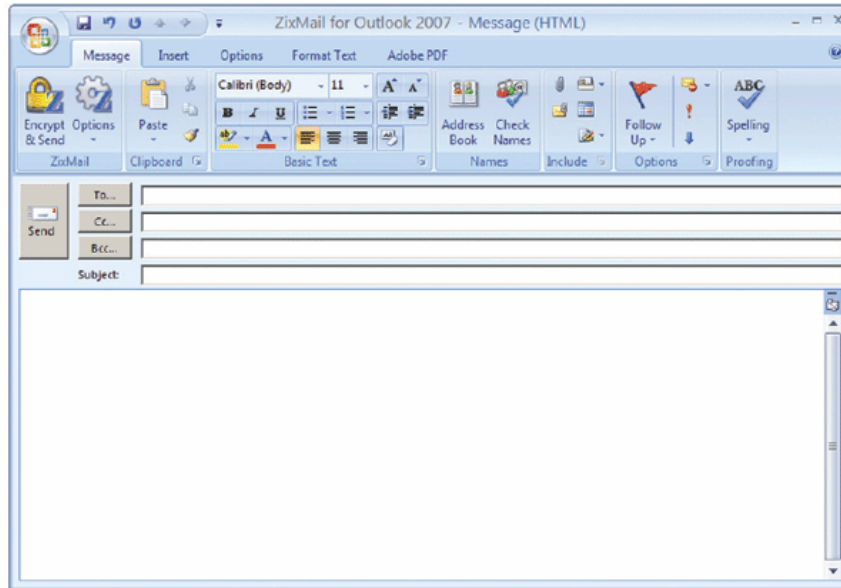
(b) *an email application having an interface for selectively initiating a first email sending process or a second email sending process for an email having content – the Zix Email Encryption system comprises an email application, such as an email plugin or other user application, which allows a user to choose between sending unencrypted and encrypted emails, for example:*

ZixGateway is a policy-based email encryption appliance for enterprise-wide regulatory compliance. It provides company-wide security, content filtering, and management of outbound corporate email. ZixGateway provides the benefits of a secure messaging gateway without having to create and manage encryption keys, by leveraging the world's largest email encryption directory, ZixDirectory. Plus, it's totally transparent to end users.

Outlook Plug-ins

For Microsoft Outlook users, ZixCorp provides a special ZixMail plug-in so you can send and receive encrypted email without ever leaving Outlook. The plug-in integrates the ZixMail functionality directly into Outlook's toolbar. The simple click of a button is all it takes to encrypt or decrypt a message.



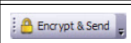
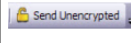



Protecting Confidentiality with ZixSelect

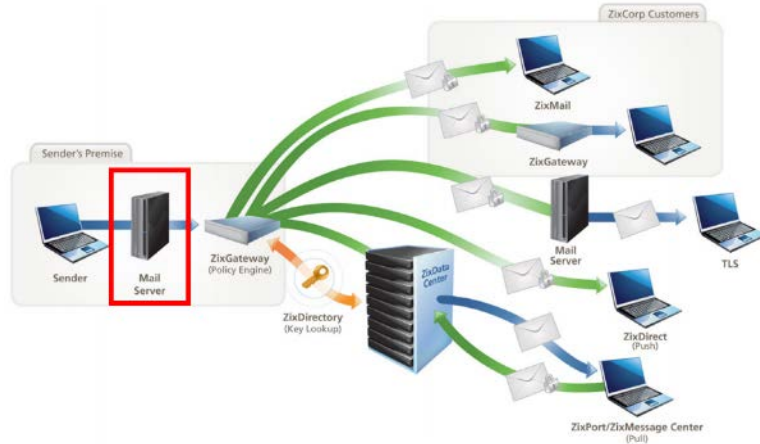
If you work with personal information such as health, financial or other confidential information, you can protect its confidentiality and privacy by using an encrypted email service. The ZixSelect™ client that you install on the **New Mail Message** tool bar of Microsoft Outlook 2003 allows you to protect personal information. The feature allows you to send messages encrypted or unencrypted when used in conjunction with a ZixVPM® appliance. It is dependent upon policy configuration choices made by your system administrator.

Your system administrator sets policies related to the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA) that encrypts email messages that contain personal health or personal finance information. As an added measure, you can use ZixSelect to ensure that specific messages are sent encrypted or unencrypted.

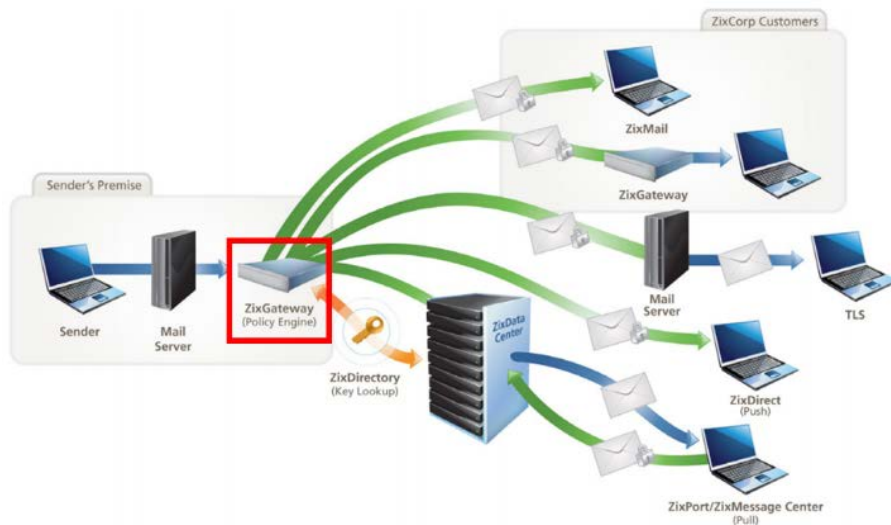
The ZixSelect client works with the ZixVPM appliances installed in your corporate network. This version of ZixSelect gives you two options when sending email messages, in addition to the standard **Microsoft Outlook Send** button:

Icon	Button Name	Description
	Encrypt & Send	To encrypt and send messages containing personal or confidential information.
	Send Unencrypted	To send unencrypted (plaintext) messages that contain personal or confidential information but do not violate corporate confidentiality rules regarding HIPAA or GLBA.
	Send	To send messages that do not contain personal or confidential information.

(c) *a first email server that routes the email content toward an intended recipient without encrypting the email content when the first email sending process being initiated via the interface – the Zix Email Encryption system comprises the user’s existing mail server, e.g., the mail server inside the sender’s work network, which sends unencrypted emails to the recipient, for example:*



(d) a second email server that initiates a secure message transaction for delivering the email content to an intended recipient when the second email sending process being initiated via the interface the secure message transaction including providing secure access to the email content irrespective of whether the intended recipient's email application is decryption enabled – the Zix Email Encryption system comprises an intercepting mail server that processes and encrypts outgoing emails sent to recipients outside of the sender’s network which meet specific criteria, for example:



ZixGateway is a policy-based email encryption appliance for enterprise-wide regulatory compliance. It provides company-wide security, content filtering, and management of outbound corporate email. ZixGateway provides the benefits of a secure messaging gateway without having to create and manage encryption keys, by leveraging the world's largest email encryption directory, ZixDirectory. Plus, it's totally transparent to end users.

The email is encrypted and stored within the ZixPort database, and a notification email is sent to the recipient that the email is waiting for retrieval, with a hyperlink to access the encrypted email, or the email is encrypted and placed in an HTML attachment to a notification email, for example:

Reading New Messages

When a new secure message arrives in the Secure Message Center, [you receive a notification email in your regular email Inbox](#). If you have not already registered, go to [Registering](#).

To read the message:

1. Open the notification email message in your Inbox. Select the hyperlink within the email or select the Open Message button. The Sign In page for the Secure Message Center displays if you have not chosen the Remember Me option.
2. If needed, sign in using your registered Password. Your message displays.

From here, you can:

- [Reply to](#), [delete](#) or [forward](#) the message.
- Open the attachments if the message has an [attachment](#).
- [Save](#) the email message as a text file.
- [Save](#) the email message and attachment as a ZIP file.

When a message is sent via Secure Message Center, a notification email is sent to the recipient (see example below). If this is the first time the recipient received an encrypted email from that sender's company, then the recipient will need to create an account (your email address and a password) in order to read the message. If the recipient has previously received encrypted messages from the sender's company, then the recipient will only be required to re-enter their password to open and read the message.

When a message is sent via Secure Message Center, a notification email is sent to the recipient (see example below). If this is the first time the recipient received an encrypted email from that sender's company, then the recipient will need to create an account (your email address and a password) in order to read the message. If the recipient has previously received encrypted messages from the sender's company, then the recipient will only be required to re-enter their password to open and read the message.

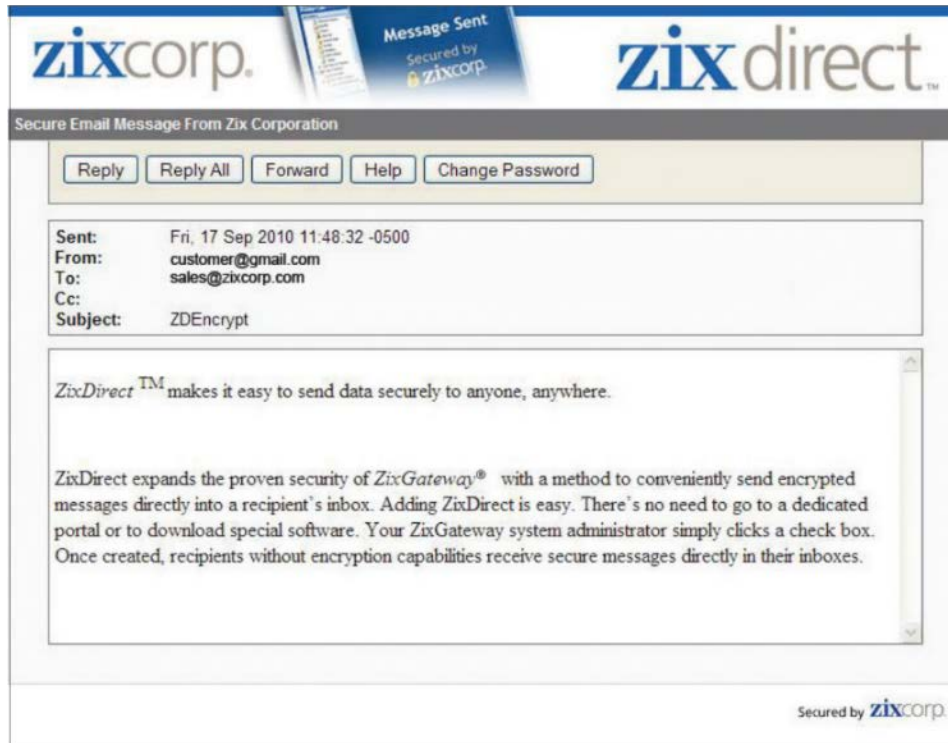
You have a ZixMessage Center Message from SENDER@DOMAIN:

Click the link below to view your secure message. If your email program does not support active links, please cut and paste the link displayed below into the "Address" or "Location" field of your browser and press "Enter" or "Go".

<https://zixmessagecenter.com/s/e?m=ABDawDyowkwhSe1vSiEiE1zp&em=RECIPIENT%40DOMAIN%2ecom>

Please do not reply to this e-mail. This message was auto-generated by the sender's Zix security system. To reply to the sender, please go to your secure message by clicking on the link above.

This message will expire on Feb 15, 2007 @ 10:45 (CST).



Recipient Convenience

ZixDirect is an extension of the ZixCorp *Best Method of Delivery*SM, which determines the most efficient way to deliver secure email based on the sender's policies and the recipient's environment.

With ZixDirect, your ZixGateway administrator creates a policy that "pushes" encrypted email messages directly to the inboxes of users who do not use email encryption. The secure message arrives as an HTML attachment within an email. The user simply clicks on the attachment and enters a password. The message is then decrypted in his/her local Internet browser. Messages are stored encrypted, and the user can open and read them anytime.

Features:

- Automatic retrieval and distribution of encryption keys through the *ZixDirectory*[®]
- Custom branding of messages
- Secure reply, reply all and forward capability
- Protected with AES encryption
- Extension of the proven ZixCorp *Best Method of Delivery*SM

45. An exemplary description of Defendant's infringement of exemplary independent claim 4 of the '967 Patent is set forth below (claim language in italics):

(a) *A method for transmitting an email comprising the steps of:*



(b) *launching an email application, the email application including an interface: - see*

¶45(b) above showing the Zix Email Encryption system email application with an interface.

(c) *selecting one of a plurality of email transmitting processes via the interface - see*

¶45(b) above showing the email application interface of the Zix Email Encryption system allows a user to choose between sending unencrypted and encrypted emails.

(d) *if the selected email transmitting process requires secure message transmission to a recipient, inserting email content into an electronic message addressed to a server that initiates a secure link with the recipient – when the user selects the encrypted message process, the Zix Email Encryption system inserts email content into a notification email sent to the recipient, for example:*

Reading New Messages

When a new secure message arrives in the Secure Message Center, you receive a notification email in your regular email Inbox. If you have not already registered, go to [Registering](#).

To read the message:

1. Open the notification email message in your Inbox. Select the hyperlink within the email or select the **Open Message** button. The **Sign In** page for the **Secure Message Center** displays if you have not chosen the **Remember Me** option.
2. If needed, sign in using your registered **Password**. Your message displays.

From here, you can:

- [Reply to](#), [delete](#) or [forward](#) the message.
- Open the attachments if the message has an [attachment](#).
- [Save](#) the email message as a text file.
- [Save](#) the email message and attachment as a ZIP file.

When a message is sent via Secure Message Center, a notification email is sent to the recipient (see example below). If this is the first time the recipient received an encrypted email from that sender's company, then the recipient will need to create an account (your email address and a password) in order to read the message. If the recipient has previously received encrypted messages from the sender's company, then the recipient will only be required to re-enter their password to open and read the message.

When a message is sent via Secure Message Center, a notification email is sent to the recipient (see example below). If this is the first time the recipient received an encrypted email from that sender's company, then the recipient will need to create an account (your email address and a password) in order to read the message. If the recipient has previously received encrypted messages from the sender's company, then the recipient will only be required to re-enter their password to open and read the message.



46. Defendant infringes the '967 Patent, including claims 1 and 3-6, by and through at least their practicing, making, using, offering for sale, selling, and/or hosting of methods comprising at least the Zix SecureMail system, including at least the following products, ZixGateway, ZixVPM, and ZixMail (including a plugin formerly known as ZixSelect), and receiver products, ZixPort and ZixDirect, as well as additional functionality products including Zix Secure Compose, ZixDirectory, and ZixMobility.

47. Additionally, or in the alternative, upon information and belief, Defendant has induced infringement of the '967 Patent in this judicial district, the State of Texas, and elsewhere in the United States, by intentionally inducing infringement of the '967 Patent, including by aiding or abetting the infringement of its end users and/or customers, including at least Comerica and/or Commerce, by and through at least Defendant's practicing and/or hosting methods comprising at least the above-described Zix Email Encryption system. Upon information and belief, such aiding and abetting comprises hosting, providing software and/or providing instructions. Upon

information and belief, such induced infringement has occurred since Defendant became aware of the '967 Patent, which at a minimum occurred in late May or early June 2015 by virtue of DataMotion's May 28, 2015 patent infringement lawsuits against Commerce and Comerica, and Defendant's inducement of infringement comprises Defendant's knowledge that the induced acts constitute patent infringement.

48. Additionally, or in the alternative, upon information and belief, Defendant contributed to infringement of the '967 patent in this judicial district, the State of Texas, and elsewhere in the United States, by actions comprising making, using, selling, offering for sale and/or hosting the Zix Email Encryption system, which at a minimum is used in practicing the methods of the '967 patent. The Zix Email Encryption system contributes to the direct infringement of the '967 patent by customers and/or other end users in this judicial district, the State of Texas and elsewhere in the United States.

49. Upon information and belief, the Zix Email Encryption system is especially made or especially adapted for uses and practices which constitute infringement of the '967 patent. The Zix Email Encryption system is not a staple article or commodity of commerce suitable for substantial non-infringing uses, including at least because it is especially made or especially adapted for uses and practices which constitute infringement of the '967 patent.

50. As noted above, at a minimum, Defendant became aware of the '967 patent in late May or early June 2015. On information and belief, Defendant's contributory infringement comprises its knowledge that the Zix Email Encryption system is especially made or especially adapted for uses and/or practices which constitute infringement of the '967 patent and it is not a staple article or commodity of commerce suitable for substantial non-infringing uses. Such knowledge is evidenced by the fact that infringement of the '967 patent from the use of the Zix

Email Encryption system is clear, evident, and unmistakable to anyone aware of both the '967 patent and of the details of the uses and practices employed in connection with the Zix Email Encryption system. It is similarly clear, evident, and unmistakable to anyone aware of both the '967 patent and of the details of the uses and practices employed in connection with the Zix Email Encryption system that it is especially made or especially adapted for uses and/or practices which constitute infringement of the '967 patent and it does not comprise a staple article or commodity of commerce suitable for substantial non-infringing uses. Defendant would necessarily be aware of the details of the methods used and practiced in connection with the Zix Email Encryption system at the time it became aware of the '967 patent, and at that point it would necessarily become clear and unmistakable to Defendant that its customers and end users were infringing the '967 patent, that the Zix Email Encryption system is, at a minimum, contributing to such infringement, and that the Zix Email Encryption system is especially made or especially adapted for uses and practices which constitute infringement of the '967 patent, and it is not a staple article or commodity of commerce suitable for substantial non-infringing uses. Since Defendant became aware of the '967 patent it has necessarily possessed such knowledge.

51. On information and belief, Defendant has also had at least constructive notice of the '967 Patent pursuant to the Patent Act. Plaintiff reserves the right to take discovery regarding Defendant's first actual notice of the '967 Patent.

52. Each of Defendant's aforesaid activities have been without authority and/or license from Plaintiff.

DAMAGES

53. By way of its infringing activities, Defendant has caused and continues to cause Plaintiff to suffer damages, and Plaintiff is entitled to recover from Defendant the damages

sustained by Plaintiff as a result of Defendant's wrongful acts in an amount subject to proof at trial, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

54. Defendant's use of DataMotion's patented technology has caused, is causing and will continue to cause DataMotion irreparable harm for which there is no adequate remedy at law, unless enjoined by this Court.

55. Plaintiff also requests that the Court make a finding that this is an exceptional case entitling Plaintiff to recover its attorneys' fees and costs pursuant to 35 U.S.C. § 285.

JURY DEMAND

56. Plaintiff hereby requests a trial by jury pursuant to Rule 38 of the Federal Rules of Civil Procedure on all issues so triable.

PRAYER FOR RELIEF

57. Plaintiff respectfully requests that the Court find in its favor and against Defendant, and that the Court grant Plaintiff the following relief:

- A. An adjudication that one or more claims of the Patent-in-Suit have been directly infringed, either literally and/or under the doctrine of equivalents, by Defendant;
- B. A preliminary and permanent injunction enjoining Defendant and its officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in active concert or participation with it, from making, using, offering to sell, or selling in the United States or importing into the United States any devices, methods or systems that infringe any claim of the '967 patent, or contributing to or inducing the same by others;
- C. An award of damages to be paid by Defendant adequate to compensate DataMotion for

Defendant's past infringement of the '967 patent and any continuing or future infringement through the date such judgment is entered, including interest, costs, expenses and an accounting of all infringing acts including, but not limited to, those acts not presented at trial;

- D. That this Court declare this to be an exceptional case and award Plaintiff reasonable attorneys' fees and costs in accordance with 35 U.S.C. § 285;
- E. A judgment and order requiring Defendant to pay Plaintiff its damages, costs, expenses, fees, and prejudgment and post-judgment interest for Defendant's infringement of the Patent-in-Suit as provided under 35 U.S.C. §§ 284 and/or 285; and
- F. Any and all further relief for which Plaintiff may show itself justly entitled that this Court deems just and proper.

February 9, 2016

Respectfully submitted,

/s/ John J. Edmonds

John J. Edmonds – Lead Counsel

Texas Bar No. 789758

**COLLINS, EDMONDS,
SCHLATHER & TOWER, PLLC**

721 Green River Trail

Fort Worth, Texas 76103

Telephone: (713) 364-5291

Facsimile: (832) 415-2535

Email: jedmonds@ip-lit.com

Of counsel:

Stephen F. Schlather

Texas Bar No. 24007993

Shea N. Palavan

Texas Bar No. 24083616

**COLLINS, EDMONDS,
SCHLATHER & TOWER, PLLC**

1616 South Voss Road, Suite 125

Houston, Texas 77057

Telephone: (281) 501-3425

Facsimile: (832) 415-2535

Email: sschlather@ip-lit.com

spalavan@ip-lit.com

*Attorneys for Plaintiff,
DataMotion Texas, LLC*