

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

STERLING COMPUTERS CORPORATION,

Plaintiff,

v.

MICROSOFT CORPORATION,

Defendant.

CASE NO. 1:24-cv-00406

JURY TRIAL DEMANDED

**PLAINTIFF STERLING COMPUTERS CORPORATION'S PRELIMINARY
INFRINGEMENT CONTENTIONS AND DISCLOSURES**

Pursuant to Paragraph 5 of the Amended Agreed Scheduling Order (ECF 36-1), Plaintiff Sterling Computers Corporation (“Sterling”), hereby produces the following Preliminary Infringement Contentions, including the initial claim chart attached hereto as Exhibit A for Defendant Microsoft Corporation, relating to each known accused product to the asserted claims each such product infringes for U.S. Patent. No. 8,073,911 (hereinafter the “‘911 Patent”):

As set forth in **Exhibit A**, Plaintiff alleges that Microsoft’s Exchange Online product, which Microsoft has manufactured, offered for sale, and sold, infringes Claims 1-7 and 9-12 of the ‘911 Patent.

Plaintiff provides these claim charts before claim constructions proceedings have begun and before fact and expert discovery has begun.

Plaintiff’s contentions are not an admission, adoption, or waiver of any particular claim construction, and Plaintiff reserves all rights with respect to claim construction. This initial claim chart is based on information reasonably and presently available to Plaintiff without the benefit of any discovery. Plaintiff reserves the right to modify, amend, retract, and or supplement this claim chart as additional information becomes available to Plaintiff. For example, in accordance with

the Scheduling Order, Plaintiff reserves the right to modify, amend, retract, and or supplement these contentions (1) following Defendant's production of technical documents, including, without limitation, software, (2) following Plaintiff's identification of relevant, new material after these preliminary contentions were served (including, but not limited to, information discovered or identified during discovery and following issuance of the *Markman* order and any other claim constructions), and (3) when Final Infringement Contentions are due.

Plaintiff contends that Defendant has directly infringed and continues to directly infringe, literally and/or under the doctrine of equivalents, the asserted claims of each of the Patents-in-Suit in violation of 35 U.S.C. § 271(a). Plaintiff contends that each element of the asserted claims is literally met. To the extent, however, that any claim element is found not be met literally, Plaintiff contends that the accused product embodies such claim elements under the doctrine of equivalents because there are no substantial differences for each claim element, and the accused product performs substantially the same function, in substantially the same way, to achieve substantially the same result. Plaintiff reserves the right to supplement these Preliminary Infringement Contentions to include contentions under the doctrine of equivalents after receiving any non-infringement defense by Defendant. Plaintiff also reserves the right to supplement these Preliminary Infringement Contentions to assert induced infringement and/or contributory infringement.

Based upon information available to Plaintiff at this time, the earliest priority date for each asserted claim is at least as early as approximately December 12, 2003 – i.e., six months prior to the filing date of the provisional application (filed on May 12, 2004). This disclosure is based on information reasonably and presently available to Plaintiff. Plaintiff reserves the right to modify, amend, retract, and or supplement this disclosure as additional information becomes available to

Plaintiff, including following Plaintiff's identification of relevant, new material after this disclosure was served. Based upon Plaintiff's investigation to date, other than the file history (which is being produced along with this disclosure), Plaintiff does not possess any additional documents evidencing conception and reduction to practice, but Plaintiff is attempting to obtain such documentation, including from third parties. Plaintiff will promptly produce any such documentation to the extent Plaintiff obtains it.

Dated: October 11, 2024

Respectfully submitted,

By: /s/Devan V. Padmanabhan
Devan V. Padmanabhan (admitted *Pro Hac Vice*)
devan@paddalawgroup.com
Britta Loftus (admitted *Pro Hac Vice*)
britta@paddalawgroup.com
Paul Robbennolt (admitted *Pro Hac Vice*)
paul@paddalawgroup.com
Sri Sankaran (admitted *Pro Hac Vice*)
sri@paddalawgroup.com
PADMANABHAN & DAWSON, P.L.L.C.
9800 Shelard Parkway, Suite 120
Minneapolis, MN 55441
Tel: (612) 444-3601
Fax: (612) 444-31958

Christopher V. Goodpastor
Texas State Bar No. 00791991
cgoodpastor@dinovoprice.com
Adam G. Price
Texas State Bar No. 24027750
aprice@dinovoprice.com
Gabriel R. Gervery
Texas State Bar No. 24072112
ggervey@dinovoprice.com
Michael D. French
Texas State Bar No. 24116392
mfrench@dinovoprice.com
DINOVO PRICE LLP
7000 N. MoPac Expressway, Suite 350

Austin, Texas 78731
Tel: (512) 539-2626
Fax: (512) 727-6691

*Attorneys for Plaintiff
Sterling Computers Corporation*

EXHIBIT A

Claim Chart for Microsoft Exchange Online

'911 Patent Claims

Claim Limitation	Microsoft Exchange Online
1. A computerized messaging server in an electronic messaging system, comprising:	Microsoft Exchange Online meets the recited language. Microsoft Exchange Online is an electronic messaging system comprising a computerized messaging server. Microsoft Exchange Online is a cloud-based platform that provides messages to users through email and calendar clients such as Outlook. Exchange Online “Microsoft Exchange Online is a cloud based messaging platform that delivers email, calendar, contacts, and tasks. Users with an Exchange Online license connect to Exchange Online through email and calendar clients like, Outlook desktop, Outlook on the web and Outlook mobile app to access email and collaboration functionality, including shared mailboxes, shared calendars and global address lists.” - https://learn.microsoft.com/en-us/exchange/exchange-online¹ Messaging records management in Exchange Online “Messaging records management (MRM) is the records management technology in Exchange Server and Exchange Online that helps organizations manage email lifecycle and reduce the legal risks associated with email. Deploying MRM can help your organization in several ways: • Meet business requirements: ... • Meet legal and regulatory requirements: Many organizations have a legal or regulatory requirement to store messages for a designated period and remove messages older than that period. Storing messages longer than necessary may increase your organization's legal or financial risks. • Increase user productivity:” - https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/messaging-records-management

¹ The entire guide can be found at <https://learn.microsoft.com/pdf?url=https%3A%2F%2Flearn.microsoft.com%2Fen-us%2Fexchange%2Fonlinetoc%2Ftoc.json>. Sterling reserves the right to cite to additional information from the guide to further support its analysis.

Claim Limitation	Microsoft Exchange Online
a messaging module adapted to control a message database storing messages sent among users of the messaging system,	Microsoft Exchange Online meets this limitation. Microsoft Exchange Online has a module that controls a message database storing messages sent among users of the messaging system. “Messaging records management (MRM) is the records management technology in Exchange Server and Exchange Online that helps organizations manage email lifecycle and reduce the legal risks associated with email.” - https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/messaging-records-management In particular, a messaging module applies “mail flow rules” to control messages sent among users. “Mail flow rules are similar to the Inbox rules that are available in Outlook and Outlook on the web (formerly known as Outlook Web App). The main difference is mail flow rules take action on messages while they're in transit, not after the message is delivered to the mailbox. Mail flow rules contain a richer set of conditions, exceptions, and actions, which provides you with the flexibility to implement many types of messaging policies.” - https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rules

Claim Limitation	Microsoft Exchange Online
at least one of the sent messages stored in the message database comprising a message container containing relational references pointing to a plurality of sent submessages stored externally to the message container in the message database,	Microsoft Exchange Online meets this limitation. In Microsoft Exchange Online, at least one of the sent messages stored in the message database comprises a message container containing relational references pointing to a plurality of sent submessages stored externally to the message container in the message database. The plurality of submessages refers to the inventive object-based messaging system discussed above. Each submessage is a unique object. “In the context of Exchange, conversations are a way to group and manage a related set of email messages. They can also provide a way to view related messages. Exchange defines conversations based on the Message-ID value of the first email message in a thread. All replies and related messages reference the original message's Message-ID header in their References and In-Reply-To headers. Additionally, inside the SOAP envelope, for each message received in a mailbox, Exchange sets specific properties and elements.” - https://learn.microsoft.com/en-us/exchange/client-developer/exchange-web-services/how-to-work-with-conversations-by-using-ews-in-exchange
at least one of the sent submessages being one of a reply to and a forward of other sent submessages of the sent message;	Microsoft Exchange Online meets this limitation. In Microsoft Exchange Online, at least one of the sent submessages include a reply to and a forward of other sent submessages of the sent message. Sent and forwarded submessages are routine.

and a governance module adapted to control a governance policy database storing a compliance policy describing rules applicable to the sent submessages,	Microsoft Exchange Online includes a module adapted to control a governance policy database storing a compliance policy describing rules applicable to submessages. Retention tags and policies are applicable to the sent submessages. Retention tags “As illustrated in the preceding figure, retention tags are used to apply retention settings to folders and individual items such as e-mail messages and voice mail.” Retention policies “To apply one or more retention tags to a mailbox, you must add them to a retention policy and then apply the policy to mailboxes.” - https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/retention-tags-and-policies You can also create and deploy retention tags that Outlook 2010 and later and Outlook on the web (formerly known as Outlook Web App) users can use to apply to folders or individual messages. After they're created, you add retention tags to a retention policy and then apply the policy to users.” https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/messaging-records-management “Retention tags allow users to tag their own mailbox folders and individual items for retention.” - https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/retention-tags-and-policies The mail flow rules are rules applicable to sent submessages. The compliance policy describes those rules. The compliance policy is stored in a governance policy database. “<u>Mail flow rule components</u> A mail flow rule is made of conditions, exceptions, actions, and properties: • <u>Conditions: Identify the messages that you want to apply the actions to. Some conditions examine message header fields (for example, the To, From, or Cc fields). Other conditions examine message properties (for</u>
---	--

Claim Limitation	Microsoft Exchange Online
	example, the message subject, body, attachments, message size, or message classification). Most conditions require you to specify a comparison operator (for example, equals, doesn't equal, or contains) and a value to match. * * * • Exceptions: Optionally identify the messages that the actions shouldn't apply to. The same message identifiers that are available in conditions are also available in exceptions. Exceptions override conditions and prevent the rule actions from being applied to a message, even if the message matches all of the configured conditions. * * * • Actions: Specify what to do to messages that match the conditions in the rule, and don't match any of the exceptions. There are many actions available, such as rejecting, deleting, or redirecting messages, adding additional recipients, adding prefixes in the message subject, or inserting disclaimers in the message body. * * * • Properties: Specify other rules settings that aren't conditions, exceptions or actions. For example, when the rule should be applied, whether to enforce or test the rule, and the time period when the rule is active.” -- https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rules

the governance module further adapted to determine rules described by the compliance policy that are applicable to ones of the plurality of sent submessages, wherein different rules of the compliance policy are applicable to different ones of the plurality of sent submessages;	Microsoft Exchange Online meets this limitation. The governance module in Microsoft Exchange Online is adapted to determine rules described by the compliance policy that are applicable to ones of the plurality of sent submessages, wherein different rules of the compliance policy are applicable to different ones of the plurality of sent submessages. Different mail flow rules can apply to different sent submessages. “Conditions” identify the messages to which certain actions apply. -- https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rules (“Conditions: Identify the messages that you want to apply the actions to.”). Conditions can require examination of message header fields, such as the “to,” “from,” or “cc” fields. So, for example, different rules may apply to different sent submessages based on the identity of the sender, the identity of the recipient, etc. <u>Id.</u> (“Some conditions examine message header fields (for example, the To, From, or Cc fields).”) Messaging Records Management strategy “Individual messages can have a different retention tag than the one applied to the folder in which they're located. ... The following figure illustrates the tasks involved in implementing this strategy. 1. Create Retention Tags ... Personal Tags Personal tags are used ... to apply retention settings to custom folders and individual items such as email messages. ... 4. Apply Retention Policies ... Different sets of users can have different retention policies.” https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/retention-tags-and-policies “You can also create and deploy retention tags that Outlook 2010 and later and Outlook on the web (formerly known as Outlook Web App) users can use to apply to folders or individual messages. After they're created, you add retention tags to a retention policy and then apply the policy to users.”
--	--

Claim Limitation	Microsoft Exchange Online
	https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/messaging-records-management “Retention tags allow users to tag their own mailbox folders and individual items for retention.” - https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/retention-tags-and-policies

Claim Limitation	Microsoft Exchange Online
wherein the messaging system is utilized by a set of entities in a population structure and wherein a rule of the compliance policy includes one or more rule elements describing whether the rule is applicable to a sent submessage, at least one of the rule elements selected from the group consisting of: a source element describing a population structure entity that is a source of the sent submessage;	Microsoft Exchange Online meets this limitation. In Microsoft Exchange Online, the messaging system is utilized by a set of entities in a population structure and wherein a rule of the compliance policy includes one or more rule elements describing whether the rule is applicable to a sent submessage, and at least one of the rule elements selected from the group consisting of: a source element describing a population structure entity that is a source of the sent submessage; a target element describing a population structure entity that is a recipient of the sent submessage; and a rank describing a ranking of the rule relative to other rules in the compliance policy. The messaging system is utilized by a set of entities in a population structure, and a rule of the compliance policy includes one or more rule elements. For example: “Allow users to classify messages: In this strategy, you implement MRM policies that include a baseline retention setting for all messages but allow users to classify messages based on business or regulatory requirements. In this case, users become an important part of your records management strategy - often they have the best understanding of a message's retention value. 1. Users can apply different retention settings to messages that need to be retained for a longer or shorter period. You can implement this policy using a combination of the following: • A DPT for the mailbox • Personal tags that users can apply to custom folders or individual messages • (Optional) Additional RPTs to expire items in specific default folders.” - https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/messaging-records-management As noted above, whether a rule is applicable to a sent submessage may be determined by who sent it, i.e. the source of the sent submessage. https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rules

Claim Limitation	Microsoft Exchange Online
a target element describing a population structure entity that is a recipient of the sent submessage;	In Microsoft Exchange Online, the messaging system is utilized by a set of entities in a population structure and wherein a rule of the compliance policy includes one or more rule elements describing whether the rule is applicable to a sent submessage, and at least one of the rule elements selected from the group consisting of: a source element describing a population structure entity that is a source of the sent submessage; a target element describing a population structure entity that is a recipient of the sent submessage; and a rank describing a ranking of the rule relative to other rules in the compliance policy. As noted above, whether a rule is applicable to a sent submessage may be determined by who received it, i.e., the recipient of the sent submessage. <u>Id.</u>
and a rank describing a ranking of the rule relative to other rules in the compliance policy.	In Microsoft Exchange Online, the messaging system is utilized by a set of entities in a population structure and wherein a rule of the compliance policy includes one or more rule elements describing whether the rule is applicable to a sent submessage, and at least one of the rule elements selected from the group consisting of: a source element describing a population structure entity that is a source of the sent submessage; a target element describing a population structure entity that is a recipient of the sent submessage; and a rank describing a ranking of the rule relative to other rules in the compliance policy. The “priority” property of the mail flow rule describes the ranking of one rule relative to other rules in the compliance policy. “Priority[:] Indicates the order that the rules are applied to messages. The default priority is based on when the rule is created (older rules have a higher priority than newer rules, and higher priority rules are processed before lower priority rules). You change the rule priority in the EAC by moving the rule up or down in the list of rules. In the PowerShell, you set the priority number (0 is the highest priority). For example, if you have one rule to reject messages that include a credit card number, and another one requiring approval, you'll want the reject rule to happen first, and stop applying other rules.” -- https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rules

2. The messaging server of claim 1, wherein the compliance policy describes a population structure of end-users of the messaging system, a set of jobcodes with which the sent submessages can be classified, and a set of rules applicable to the population structure, jobcodes, and sent submessages.	Microsoft Exchange Online meets this limitation. The compliance policy describes a population structure of end-users of the messaging system, a set of jobcodes with which the sent submessages can be classified, and a set of rules applicable to the population structure, jobcodes, and sent submessages. The compliance policy describes a population structure of end-users of the messaging system, a set of jobcodes (see, e.g., conditions, exceptions, properties, below) with which the sent submessages can be classified, a set of rules applicable to the population structure (see, e.g., actions, below), and sent submessages. <u>“Mail flow rule components</u> A mail flow rule is made of conditions, exceptions, actions, and properties: • Conditions: Identify the messages that you want to apply the actions to. Some conditions examine message header fields (for example, the To, From, or Cc fields). Other conditions examine message properties (for example, the message subject, body, attachments, message size, or message classification). Most conditions require you to specify a comparison operator (for example, equals, doesn't equal, or contains) and a value to match. * * * • Exceptions: Optionally identify the messages that the actions shouldn't apply to. The same message identifiers that are available in conditions are also available in exceptions. Exceptions override conditions and prevent the rule actions from being applied to a message, even if the message matches all of the configured conditions. * * * • Actions: Specify what to do to messages that match the conditions in the rule, and don't match any of the exceptions. There are many actions available, such as rejecting, deleting, or redirecting messages, adding additional recipients, adding prefixes in the message subject, or inserting disclaimers in the message body. * * * • Properties: Specify other rules settings that aren't conditions, exceptions or actions. For example, when the rule should be applied, whether to enforce or test the rule, and the time period when the rule is active.” -- https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rules “In Exchange Online, you can use messaging records management (MRM) retention policies to manage email lifecycle. Retention policies are applied by creating retention tags, adding them to a retention policy, and applying the policy to mailbox users.” - https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/create-a-retention-policy
---	--

Claim Limitation	Microsoft Exchange Online
	“You can also create and deploy retention tags that Outlook 2010 and later and Outlook on the web (formerly known as Outlook Web App) users can use to apply to folders or individual messages. After they're created, you add retention tags to a retention policy and then apply the policy to users.” https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/messaging-records-management “Retention tags allow users to tag their own mailbox folders and individual items for retention.” - https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/retention-tags-and-policies

Claim Limitation	Microsoft Exchange Online
3. The messaging server of claim 2, wherein a jobcode describes a set of jobcode rules applicable to all sent submessages classified with the jobcode.	Microsoft Exchange Online meets this limitation. The jobcode describes a set of jobcode rules applicable to all sent submessages that are classified with the jobcode. For examples, conditions, exceptions or properties, describe a set of rules applicable to all submessages that meet that classification. <u>“Mail flow rule components</u> A mail flow rule is made of conditions, exceptions, actions, and properties: • Conditions: Identify the messages that you want to apply the actions to. Some conditions examine message header fields (for example, the To, From, or Cc fields). Other conditions examine message properties (for example, the message subject, body, attachments, message size, or message classification). Most conditions require you to specify a comparison operator (for example, equals, doesn't equal, or contains) and a value to match. * * * • Exceptions: Optionally identify the messages that the actions shouldn't apply to. The same message identifiers that are available in conditions are also available in exceptions. Exceptions override conditions and prevent the rule actions from being applied to a message, even if the message matches all of the configured conditions. * * * • Actions: Specify what to do to messages that match the conditions in the rule, and don't match any of the exceptions. There are many actions available, such as rejecting, deleting, or redirecting messages, adding additional recipients, adding prefixes in the message subject, or inserting disclaimers in the message body. * * * • Properties: Specify other rules settings that aren't conditions, exceptions or actions. For example, when the rule should be applied, whether to enforce or test the rule, and the time period when the rule is active.” -- https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rules

Claim Limitation	Microsoft Exchange Online
4. The messaging server of claim 2, wherein the messaging module is further adapted to receive an indication of a jobcode and of a sent submessage from an end-user, and is further adapted to associate the jobcode with the sent submessage responsive to receipt of the indication of the jobcode from the end-user.	Microsoft Exchange Online meets this limitation. The messaging module is adapted to receive an indication of a jobcode and of a sent submessage from and end user. “Mail flow rules are similar to the Inbox rules that are available in Outlook and Outlook on the web (formerly known as Outlook Web App). The main difference is mail flow rules take action on messages while they're in transit, not after the message is delivered to the mailbox. Mail flow rules contain a richer set of conditions, exceptions, and actions, which provides you with the flexibility to implement many types of messaging policies.” - https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rules The messaging module is further adapted to associate the jobcode with the sent submessage in response to the received indication of jobcode from the end user. “Mail flow rule components A mail flow rule is made of conditions, exceptions, actions, and properties: • Conditions: Identify the messages that you want to apply the actions to. Some conditions examine message header fields (for example, the To, From, or Cc fields). Other conditions examine message properties (for example, the message subject, body, attachments, message size, or message classification). Most conditions require you to specify a comparison operator (for example, equals, doesn't equal, or contains) and a value to match. * * * • Exceptions: Optionally identify the messages that the actions shouldn't apply to. The same message identifiers that are available in conditions are also available in exceptions. Exceptions override conditions and prevent the rule actions from being applied to a message, even if the message matches all of the configured conditions. * * * • Actions: Specify what to do to messages that match the conditions in the rule, and don't match any of the exceptions. There are many actions available, such as rejecting, deleting, or redirecting messages, adding additional recipients, adding prefixes in the message subject, or inserting disclaimers in the message body. * * * • Properties: Specify other rules settings that aren't conditions, exceptions or actions. For example, when the rule should be applied, whether to enforce or test the rule, and the time period when the rule is active.” -- https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rules

Claim Limitation	Microsoft Exchange Online
5. The messaging server of claim 1, wherein the rules described by the compliance policy include one or more types of rules from the set consisting of: communication rules describing which population structure entities can communicate with other population structure entities via the messaging system; and readership rules describing which population structure entities can read messages from other population structure entities via the messaging system.	Microsoft Exchange Online meets this limitation. The compliance policy includes one or more of communication rules describing which population structure entities can communicate with others, and readership rules, describing which population structure entities can read messages from others. “In Exchange Online organizations or standalone Exchange Online Protection (EOP) organizations without Exchange Online mailboxes, actions in mail flow rules (also known as transport rules) specify what you want to do to messages that match conditions of the rule. For example, you can create a rule that forwards messages from specific senders to a moderator, or adds a disclaimer or personalized signature to all outbound messages.” https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rule-actions For example, one of the actions that can be applied using mail flow rules in Exchange Online is “Block the message > reject the message and include an explanation” (i.e., “readership rules”) and “Redirect the message to” (“Redirects the message to the specified recipients. The message isn't delivered to the original recipients, and no notification is sent to the sender or the original recipients.”) (i.e., “communication rules”). See https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rule-actions

Claim Limitation	Microsoft Exchange Online
6. The messaging server of claim 1, wherein the rules described by the compliance policy include one or more types of rules from the set consisting of: validity rules describing a time period for which a sent submessage or entity in the population structure is useable; and retention rules describing a time period after which a sent submessage or entity in the population structure should be deleted from the messaging system.	Microsoft Exchange Online meets this limitation. The rules described by the compliance policy include one or more of validity rules describing a time period for which a sent submessage or entity in the population structure is useable, and retention rules describing a time period after which a sent submessage or entity should be deleted from the messaging system. “In Exchange Online, you can use messaging records management (MRM) retention policies to manage email lifecycle. Retention policies are applied by creating retention tags, adding them to a retention policy, and applying the policy to mailbox users.” https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/create-a-retention-policy Retention tags “[R]etention tags are used to apply retention settings to folders and individual items such as e-mail messages and voice mail. These settings specify how long a message remains in a mailbox and the action to be taken when the message reaches the specified retention age. When a message reaches its retention age, it's moved to the user's archive mailbox or deleted.” https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/retention-tags-and-policies “Retention tags allow users to tag their own mailbox folders and individual items for retention.” - https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/retention-tags-and-policies

Claim Limitation	Microsoft Exchange Online
7. The messaging server of claim 1, wherein the governance policy database further stores at least one prior compliance policy active at a time prior to a time at which the compliance policy was active, and wherein the sent submessages of the stored messages are associated with a compliance policy that was active at a time that content of the sent submessages was created.	Microsoft Exchange Online meets this limitation. The mail flow rule components include Properties, and Properties include the time period when different rules are active. Therefore, different rules and compliance policies may be effective and applied as appropriate to a specific message. <u>“Mail flow rule components</u> A mail flow rule is made of conditions, exceptions, actions, and properties: • <u>Conditions:</u> Identify the messages that you want to apply the actions to. Some conditions examine message header fields (for example, the To, From, or Cc fields). Other conditions examine message properties (for example, the message subject, body, attachments, message size, or message classification). Most conditions require you to specify a comparison operator (for example, equals, doesn't equal, or contains) and a value to match. * * * • <u>Exceptions:</u> Optionally identify the messages that the actions shouldn't apply to. The same message identifiers that are available in conditions are also available in exceptions. Exceptions override conditions and prevent the rule actions from being applied to a message, even if the message matches all of the configured conditions. * * * • <u>Actions:</u> Specify what to do to messages that match the conditions in the rule, and don't match any of the exceptions. There are many actions available, such as rejecting, deleting, or redirecting messages, adding additional recipients, adding prefixes in the message subject, or inserting disclaimers in the message body. * * * • <u>Properties:</u> Specify other rules settings that aren't conditions, exceptions or actions. For example, when the rule should be applied, whether to enforce or test the rule, and the time period when the rule is active.” -- https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rules

9. The messaging server of claim 1, wherein the rules described by the compliance policy include search rules describing which population structure entities can view which sent submessages when searching the sent submessages stored by the messaging system.	Microsoft Exchange Online meets this limitation. The compliance policy includes rules describing which population structure entities can view which submessages, when searching the sent submessages stored by the system. “Exchange Online includes a large set of predefined permissions, based on the Role Based Access Control (RBAC) permissions model, which you can use right away to easily grant permissions to your admins and users. You can use the permissions features in Exchange Online to get your new organization up and running quickly.” https://learn.microsoft.com/en-us/exchange/permissions-exo/permissions-exo “In Exchange Online organizations or standalone Exchange Online Protection (EOP) organizations without Exchange Online mailboxes, actions in mail flow rules (also known as transport rules) specify what you want to do to messages that match conditions of the rule. For example, you can create a rule that forwards messages from specific senders to a moderator, or adds a disclaimer or personalized signature to all outbound messages.” https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rule-actions For example, one of the actions that can be applied using mail flow rules in Exchange Online is “Block the message > reject the message and include an explanation” (i.e., “readership rules”) and “Redirect the message to” (“Redirects the message to the specified recipients. The message isn't delivered to the original recipients, and no notification is sent to the sender or the original recipients.”) (i.e., “communication rules”). See https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rule-actions Requirements to configure permissions filtering • To run the compliance security filter cmdlets, you have to be a member of the Organization Management role group in the compliance portal. For more information, see Permissions in the Security & Compliance Center. • You have to connect to both Exchange Online and Security & Compliance PowerShell to use the compliance security filter cmdlets. This is necessary because these cmdlets require access to mailbox properties, which is why you have to connect to Exchange Online PowerShell. See the steps in the next section. • See the More information section for additional information about search permissions filters.
---	---

Claim Limitation	Microsoft Exchange Online
	• Search permissions filtering is applicable to inactive mailboxes, which means you can use mailbox and mailbox content filtering to limit who can search an inactive mailbox. See the More information section for additional information about permissions filtering and inactive mailboxes. • Search permissions filtering can't be used to limit who can search public folders in Exchange. https://learn.microsoft.com/en-us/purview/ediscovery-permissions-filtering-for-content-search <u>How does search permissions filtering work?</u> The permissions filter is appended to the search query when a search is run. The permissions filter is joined to the search query by the AND Boolean operator. The query logic for the search query and the permissions filter would look like this: <pre> text Copy <SearchQuery> AND <PermissionsFilter> </pre> For example, you have a permissions filter that allows Bob to perform all search actions on the mailboxes of members of the Workers distribution group. Then Bob runs a search on all mailboxes in the organization with the search query sender:jerry@adatum.com. Because the permissions filter and the search query are logically combined by an AND operator, the search returns any message sent by jerry@adatum.com to any member of the Workers distribution group. https://learn.microsoft.com/en-us/purview/ediscovery-permissions-filtering-for-content-search#more-information
10. A computer program product having a non-transitory computer-readable medium having embodied thereon program code for use in an electronic messaging	Microsoft Exchange Online meets the recited language. Microsoft Exchange Online is a computer program product having a non-transitory computer-readable medium having program coded embodied on it. The program code is for use in an electronic messaging system.

Claim Limitation	Microsoft Exchange Online
system, the program code comprising:	Microsoft Exchange Online is a cloud-based platform that provides messages to users through email and calendar clients such as Outlook. “Microsoft Exchange Online is a cloud based messaging platform that delivers email, calendar, contacts, and tasks. Users with an Exchange Online license connect to Exchange Online through email and calendar clients like, Outlook desktop, Outlook on the web and Outlook mobile app to access email and collaboration functionality, including shared mailboxes, shared calendars and global address lists.” -- https://learn.microsoft.com/en-us/exchange/exchange-online Messaging records management in Exchange Online “Messaging records management (MRM) is the records management technology in Exchange Server and Exchange Online that helps organizations manage email lifecycle and reduce the legal risks associated with email. Deploying MRM can help your organization in several ways: • Meet business requirements: ... • Meet legal and regulatory requirements: Many organizations have a legal or regulatory requirement to store messages for a designated period and remove messages older than that period. Storing messages longer than necessary may increase your organization's legal or financial risks. • Increase user productivity:” - https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/messaging-records-management
a messaging module adapted to control a message database storing messages sent among users of the messaging system to at least one other end user of the messaging system,	Microsoft Exchange Online meets this limitation. Microsoft Exchange Online has a module that controls a message database storing messages sent among users of the messaging system to at least one other end user of the messaging system. “Messaging records management (MRM) is the records management technology in Exchange Server and Exchange Online that helps organizations manage email lifecycle and reduce the legal risks associated with email.” - https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/messaging-records-management

Claim Limitation	Microsoft Exchange Online
	In particular, a messaging module applies “mail flow rules” to control messages sent among users. “Mail flow rules are similar to the Inbox rules that are available in Outlook and Outlook on the web (formerly known as Outlook Web App). The main difference is mail flow rules take action on messages while they're in transit, not after the message is delivered to the mailbox. Mail flow rules contain a richer set of conditions, exceptions, and actions, which provides you with the flexibility to implement many types of messaging policies.” -- https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rules
at least one of the sent messages comprising a message container containing relational references pointing to a plurality of sent submessages stored in the message database externally to the message container in the message database,	Microsoft Exchange Online meets this limitation. In Microsoft Exchange Online, at least one of the sent messages includes a message container containing relational references pointing to a plurality of sent submessages stored in the message database externally to the message container in the message database. The plurality of submessages refers to the inventive object-based messaging system discussed above. Each submessage is a unique object. “In the context of Exchange, conversations are a way to group and manage a related set of email messages. They can also provide a way to view related messages. Exchange defines conversations based on the Message-ID value of the first email message in a thread. All replies and related messages reference the original message's Message-ID header in their References and In-Reply-To headers. Additionally, inside the SOAP envelope, for each message received in a mailbox, Exchange sets specific properties and elements.” - https://learn.microsoft.com/en-us/exchange/client-developer/exchange-web-services/how-to-work-with-conversations-by-using-ews-in-exchange
at least one of the sent submessages being one	Microsoft Exchange Online meets this limitation.

Claim Limitation	Microsoft Exchange Online
of a reply to and a forward of other sent submessages of the sent message;	In Microsoft Exchange Online, at least one of the sent submessages is a reply to and a forward of other sent submessages of the sent message. Sent and forwarded submessages are routine.
and a governance module adapted to control a governance policy database storing a compliance policy describing rules applicable to the sent submessages,	Microsoft Exchange Online meets this limitation. Microsoft Exchange Online includes a module adapted to control a governance policy database storing a compliance policy describing rules applicable to submessages. Retention tags and policies are applicable to the sent submessages. Retention tags “As illustrated in the preceding figure, retention tags are used to apply retention settings to folders and individual items such as e-mail messages and voice mail.” Retention policies “To apply one or more retention tags to a mailbox, you must add them to a retention policy and then apply the policy to mailboxes.” - https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/retention-tags-and-policies “You can also create and deploy retention tags that Outlook 2010 and later and Outlook on the web (formerly known as Outlook Web App) users can use to apply to folders or individual messages. After they're created, you add retention tags to a retention policy and then apply the policy to users.” https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/messaging-records-management “Retention tags allow users to tag their own mailbox folders and individual items for retention.” - https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/retention-tags-and-policies

Claim Limitation	Microsoft Exchange Online
	The mail flow rules are rules applicable to sent submessages. The compliance policy describes those rules. The compliance policy is stored in a governance policy database. <u>“Mail flow rule components</u> A mail flow rule is made of conditions, exceptions, actions, and properties: • Conditions: Identify the messages that you want to apply the actions to. Some conditions examine message header fields (for example, the To, From, or Cc fields). Other conditions examine message properties (for example, the message subject, body, attachments, message size, or message classification). Most conditions require you to specify a comparison operator (for example, equals, doesn't equal, or contains) and a value to match. . * * * • Exceptions: Optionally identify the messages that the actions shouldn't apply to. The same message identifiers that are available in conditions are also available in exceptions. Exceptions override conditions and prevent the rule actions from being applied to a message, even if the message matches all of the configured conditions. * * * • Actions: Specify what to do to messages that match the conditions in the rule, and don't match any of the exceptions. There are many actions available, such as rejecting, deleting, or redirecting messages, adding additional recipients, adding prefixes in the message subject, or inserting disclaimers in the message body. * * * • Properties: Specify other rules settings that aren't conditions, exceptions or actions. For example, when the rule should be applied, whether to enforce or test the rule, and the time period when the rule is active.” -- https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rules
the governance module further adapted to determine rules described	Microsoft Exchange Online meets this limitation.

Claim Limitation	Microsoft Exchange Online
by the compliance policy that are applicable to ones of the plurality of sent submessages, wherein different rules of the compliance policy are applicable to different ones of the plurality of sent submessages;	The governance module in Microsoft Exchange Online is adapted to determine rules described by the compliance policy that are applicable to ones of the plurality of sent submessages, and different rules of the compliance policy are applicable to different ones of the plurality of sent submessages. Different mail flow rules can apply to different sent submessages. “Conditions” identify the messages to which certain actions apply. <u>Id.</u> (“Conditions: Identify the messages that you want to apply the actions to.”). Conditions can require examination of message header fields, such as the “to,” “from,” or “cc” fields. So, for example, different rules may apply to different sent submessages based on the identity of the sender, the identity of the recipient, etc. <u>Id.</u> (“Some conditions examine message header fields (for example, the To, From, or Cc fields).”) Messaging Records Management strategy “Individual messages can have a different retention tag than the one applied to the folder in which they're located. ... The following figure illustrates the tasks involved in implementing this strategy. 1. Create Retention Tags ... Personal Tags Personal tags are used ... to apply retention settings to custom folders and individual items such as email messages. ... 4. Apply Retention Policies ... Different sets of users can have different retention policies.” https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/retention-tags-and-policies “You can also create and deploy retention tags that Outlook 2010 and later and Outlook on the web (formerly known as Outlook Web App) users can use to apply to folders or individual messages. After they're created, you add retention tags to a retention policy and then apply the policy to users.”

Claim Limitation	Microsoft Exchange Online
	https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/messaging-records-management “Retention tags allow users to tag their own mailbox folders and individual items for retention.” - https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/retention-tags-and-policies
wherein the messaging system is utilized by a set of entities in a population structure and wherein a rule of the compliance policy includes one or more rule elements describing whether the rule is applicable to a sent submessage, at least one of the rule elements selected from the group consisting of: a source element describing a population structure entity that is a source of the sent submessage;	Microsoft Exchange Online meets this limitation. The messaging system of Microsoft Exchange Online is utilized by a set of entities in a population structure, and a rule of the compliance policy includes one or more rule elements describing whether the rule is applicable to a sent submessage, at least one of the rule elements selected from the group consisting of: a source element describing a population structure entity that is a source of the sent submessage, a target element describing a population structure entity that is a recipient of the sent submessage, and a rank describing a ranking of the rule relative to other rules in the compliance policy. The messaging system is utilized by a set of entities in a population structure, and a rule of the compliance policy includes one or more rule elements. For example: “Allow users to classify messages: In this strategy, you implement MRM policies that include a baseline retention setting for all messages but allow users to classify messages based on business or regulatory requirements. In this case, users become an important part of your records management strategy - often they have the best understanding of a message's retention value. 2. Users can apply different retention settings to messages that need to be retained for a longer or shorter period. You can implement this policy using a combination of the following: • A DPT for the mailbox • Personal tags that users can apply to custom folders or individual messages • (Optional) Additional RPTs to expire items in specific default folders.” - https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/messaging-records-management

Claim Limitation	Microsoft Exchange Online
	As noted above, whether a rule is applicable to a sent submessage may be determined by who sent it, i.e. the source of the sent submessage. https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/retention-tags-and-policies “You can also create and deploy retention tags that Outlook 2010 and later and Outlook on the web (formerly known as Outlook Web App) users can use to apply to folders or individual messages. After they're created, you add retention tags to a retention policy and then apply the policy to users.” https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/messaging-records-management “Retention tags allow users to tag their own mailbox folders and individual items for retention.” - https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/retention-tags-and-policies
a target element describing a population structure entity that is a recipient of the sent submessage;	Microsoft Exchange Online meets this limitation. The messaging system of Microsoft Exchange Online is utilized by a set of entities in a population structure, and a rule of the compliance policy includes one or more rule elements describing whether the rule is applicable to a sent submessage, at least one of the rule elements selected from the group consisting of: a source element describing a population structure entity that is a source of the sent submessage, a target element describing a population structure entity that is a recipient of the sent submessage, and a rank describing a ranking of the rule relative to other rules in the compliance policy. As noted above, whether a rule is applicable to a sent submessage may be determined by who received it, i.e., the recipient of the sent submessage. <u>Id.</u>
and a rank describing a ranking of the rule relative to other rules in the compliance policy.	Microsoft Exchange Online meets this limitation. The messaging system of Microsoft Exchange Online is utilized by a set of entities in a population structure, and a rule of the compliance policy includes one or more rule elements describing whether the rule is applicable to a sent submessage, at least one of the rule elements selected from the group consisting of: a source element describing a population structure entity that is a source of the sent submessage, a target element describing a population structure

Claim Limitation	Microsoft Exchange Online
	entity that is a recipient of the sent submessage, and a rank describing a ranking of the rule relative to other rules in the compliance policy. The “priority” property of the mail flow rule describes the ranking of one rule relative to other rules in the compliance policy. “Priority[:] Indicates the order that the rules are applied to messages. The default priority is based on when the rule is created (older rules have a higher priority than newer rules, and higher priority rules are processed before lower priority rules). You change the rule priority in the EAC by moving the rule up or down in the list of rules. In the PowerShell, you set the priority number (0 is the highest priority). For example, if you have one rule to reject messages that include a credit card number, and another one requiring approval, you'll want the reject rule to happen first, and stop applying other rules.” -- https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rules
11. The computer program product of claim 10, wherein the rules described by the compliance policy include one or more types of rules from the set consisting of: communication rules describing which population structure entities can communicate with other population structure entities via the messaging system;	Microsoft Exchange Online meets this limitation. The compliance policy includes one or more of communication rules describing which population structure entities can communicate with others, readership rules describing which population structure entities can read messages from others, action rules describing actions a population structure entity can perform on a message component, and search rules describing which population structure entities can view which message components when searching the message components stored by the messaging system. “In Exchange Online organizations or standalone Exchange Online Protection (EOP) organizations without Exchange Online mailboxes, actions in mail flow rules (also known as transport rules) specify what you want to do to messages that match conditions of the rule. For example, you can create a rule that forwards messages from specific senders to a moderator, or adds a disclaimer or personalized signature to all outbound messages.” https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rule-actions For example, one of the actions that can be applied using mail flow rules in Exchange Online is “Block the message > reject the message and include an explanation” (i.e., “readership rules”) and “Redirect the message to” (“Redirects the

Claim Limitation	Microsoft Exchange Online
readership rules describing which population structure entities can read messages from other population structure entities via the messaging system; action rules describing actions a population structure entity can perform on a message component in the messaging system; and search rules describing which population structure entities can view which message components when searching the messaging components stored by the messaging system.	message to the specified recipients. The message isn't delivered to the original recipients, and no notification is sent to the sender or the original recipients.”) (i.e., “communication rules”). See https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rule-actions “Exchange Online includes a large set of predefined permissions, based on the Role Based Access Control (RBAC) permissions model, which you can use right away to easily grant permissions to your admins and users. You can use the permissions features in Exchange Online to get your new organization up and running quickly.” https://learn.microsoft.com/en-us/exchange/permissions-exo/permissions-exo “In Exchange Online organizations or standalone Exchange Online Protection (EOP) organizations without Exchange Online mailboxes, actions in mail flow rules (also known as transport rules) specify what you want to do to messages that match conditions of the rule. For example, you can create a rule that forwards messages from specific senders to a moderator, or adds a disclaimer or personalized signature to all outbound messages.” https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rule-actions For example, one of the actions that can be applied using mail flow rules in Exchange Online is “Block the message > reject the message and include an explanation” (i.e., “readership rules”) and “Redirect the message to” (“Redirects the message to the specified recipients. The message isn't delivered to the original recipients, and no notification is sent to the sender or the original recipients.”) (i.e., “communication rules”). See https://learn.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/mail-flow-rule-actions Requirements to configure permissions filtering • To run the compliance security filter cmdlets, you have to be a member of the Organization Management role group in the compliance portal. For more information, see Permissions in the Security & Compliance Center. • You have to connect to both Exchange Online and Security & Compliance PowerShell to use the compliance security filter cmdlets. This is necessary because these cmdlets require access to mailbox properties, which is why you have to connect to Exchange Online PowerShell. See the steps in the next section. • See the More information section for additional information about search permissions filters.

Claim Limitation	Microsoft Exchange Online
	• Search permissions filtering is applicable to inactive mailboxes, which means you can use mailbox and mailbox content filtering to limit who can search an inactive mailbox. See the More information section for additional information about permissions filtering and inactive mailboxes. • Search permissions filtering can't be used to limit who can search public folders in Exchange. https://learn.microsoft.com/en-us/purview/ediscovery-permissions-filtering-for-content-search <u>How does search permissions filtering work?</u> The permissions filter is appended to the search query when a search is run. The permissions filter is joined to the search query by the AND Boolean operator. The query logic for the search query and the permissions filter would look like this: <pre> text Copy <SearchQuery> AND <PermissionsFilter> </pre> For example, you have a permissions filter that allows Bob to perform all search actions on the mailboxes of members of the Workers distribution group. Then Bob runs a search on all mailboxes in the organization with the search query sender:jerry@adatum.com. Because the permissions filter and the search query are logically combined by an AND operator, the search returns any message sent by jerry@adatum.com to any member of the Workers distribution group. https://learn.microsoft.com/en-us/purview/ediscovery-permissions-filtering-for-content-search#more-information
12. The computer program product of claim 10, wherein the rules described by the compliance policy include one or more	Microsoft Exchange Online meets this limitation. The rules described by the compliance policy include one or more of validity rules describing a time period for which a sent submessage or entity in the population structure is useable, and retention rules describing a time period after which a sent submessage or entity should be deleted from the messaging system.

Claim Limitation	Microsoft Exchange Online
types of rules from the set consisting of: validity rules describing a time period for which a sent submessage or entity in the population structure is useable; and retention rules describing whether a sent submessage or entity in the population structure should be deleted from the messaging system.	“In Exchange Online, you can use messaging records management (MRM) retention policies to manage email lifecycle. Retention policies are applied by creating retention tags, adding them to a retention policy, and applying the policy to mailbox users.” https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/create-a-retention-policy Retention tags “[R]etention tags are used to apply retention settings to folders and individual items such as e-mail messages and voice mail. These settings specify how long a message remains in a mailbox and the action to be taken when the message reaches the specified retention age. When a message reaches its retention age, it's moved to the user's archive mailbox or deleted.” https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/retention-tags-and-policies “You can also create and deploy retention tags that Outlook 2010 and later and Outlook on the web (formerly known as Outlook Web App) users can use to apply to folders or individual messages. After they're created, you add retention tags to a retention policy and then apply the policy to users.” https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/messaging-records-management “Retention tags allow users to tag their own mailbox folders and individual items for retention.” - https://learn.microsoft.com/en-us/exchange/security-and-compliance/messaging-records-management/retention-tags-and-policies