Ex. A-11 — Invalidity of the ’934 Patent in view of Microsoft Accounts (“MSA”)

This chart is subject to all reservations, objections, and disclaimers in Microsoft’s Invalidity Contentions and any amendment, supplement, or modification thereof, which are incorporated herein by reference in their entirety.

Microsoft Accounts (“MSA”) qualifies as prior art to U.S. Patent No. 12,218,934 (“the ’934 patent”) at least under AIA 35 U.S.C. §§ 102 and/or 103. To the extent Plaintiff asserts that the ’934 patent is entitled to an earlier priority date pre-dating the AIA, MSA is prior art to the ’934 patent under pre-AIA 35 U.S.C. §§ 102 and/or 103. MSA was known to others, in public use, sold, and offered for sale, and described in printed publications at least by October 28, 2008, and thus is available as prior art to the ’934 patent at least under post-AIA 35 U.S.C. §§ 102 and/or 103 and, to the extent Plaintiff is unable to establish that the ’934 patent is entitled to a pre-AIA priority date, under re-AIA 35 U.S.C. §§ 102(a),(b), and (g) and 103.

MSA anticipates the Asserted Claims of the ’934 patent (claims 1, 3, 5, 9, 11, and 13, as set forth in Plaintiff’s preliminary infringement contentions served on November 24, 2025, which Microsoft Disputes) that are allegedly practiced by features of Entra ID (“Accused Features”). However, the accused features were conceived and developed by Microsoft and were known and in public use before October 19, 2017. Accordingly, if the accused features of Entra ID are found to infringe any Asserted Claim then those features anticipate the Asserted Claims for the same reason. For example, the functionalities in Entra ID that Qomplx accuses of infringement (*see* Qomplx’s Contentions) were in existence as part of MSA before the ’934 patent’s priority date, and thus, MSA predates and anticipates the ’934 patent under Qomplx’s interpretation of the claims, which Microsoft disputes. Microsoft does not admit that the accused Microsoft Entra ID product practices the asserted claims of the ’934 patent; rather, to the extent Qomplx bases its infringement allegations on certain functionalities in Entra ID, those functionalities existed in MSA and predate the priority date for the ’934 patent.

To the extent it is found that MSA does not expressly disclose certain limitations in the Asserted Claims, such limitations are at least implicitly or inherently disclosed based on the scope of claims asserted by Plaintiff. Moreover, to the extent it is found that MSA does not anticipate the Asserted Claims, MSA renders obvious the Asserted Claims, either alone or in combination with one or more of the prior art references identified in the cover pleading, in the chart of secondary references (Ex. A–103), and other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.

For example, aspects of the MSA system are described in technical documents, source code, patents, and physical devices, which reflect a single system. Microsoft reserves the right to supplement and/or amend these contentions with additional information during discovery.

For example, aspects of the MSA system are disclosed in the following:

- PCQuest, *Microsoft Authenticator App Is About to Release*, available at https://www.pcquest.com/microsoft-authenticator-app-is-about-to-release-on-august-15th/ (hereinafter, “PCQuest”);
- *Behind the Curtains Authentication to Azure with a Microsoft Live Account*, available at https://journeyofthegeek.com/2016/04/02/behind-the-curtains-authentication-to-azure-with-a-microsoft-live-account/ (hereinafter “Behind the Curtains”);
- Microsoft, *Understand Microsoft Accounts*, available at https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-microsoft-accounts (hereinafter “Understand Microsoft Accounts”);

Qomplx LLC, Exhibit 2006
Page 2006 - 1
IPR2026-00182, Microsoft Corp. v. Qomplx LLC

- ZDNet, *New Microsoft Authenticator App to Roll Out*, available at https://www.zdnet.com/article/new-microsoft-authenticator-app-to-roll-out-starting-august-15/ (hereinafter, "ZDNet");
- Elcomsoft, *Microsoft Two-Factor Authentication: Always There*, https://web.archive.org/web/20180122203044/https://blog.elcomsoft.com/2016/12/microsoft-two-factor-authentication-always-there/ (hereinafter, "MSA 2FA Always There");
- Microsoft, *Windows Server 2012*, available at https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/jj884082(v=ws.11) (hereinafter "Windows Server 2012");
- Microsoft, *Microsoft Authenticator Coming August 15th*, available at https://web.archive.org/web/20170113234208/https://blogs.technet.microsoft.com/enterprisemobility/2016/07/25/microsoft-authenticator-coming-august-15th/ (hereinafter "Microsoft Authenticator Announcement").

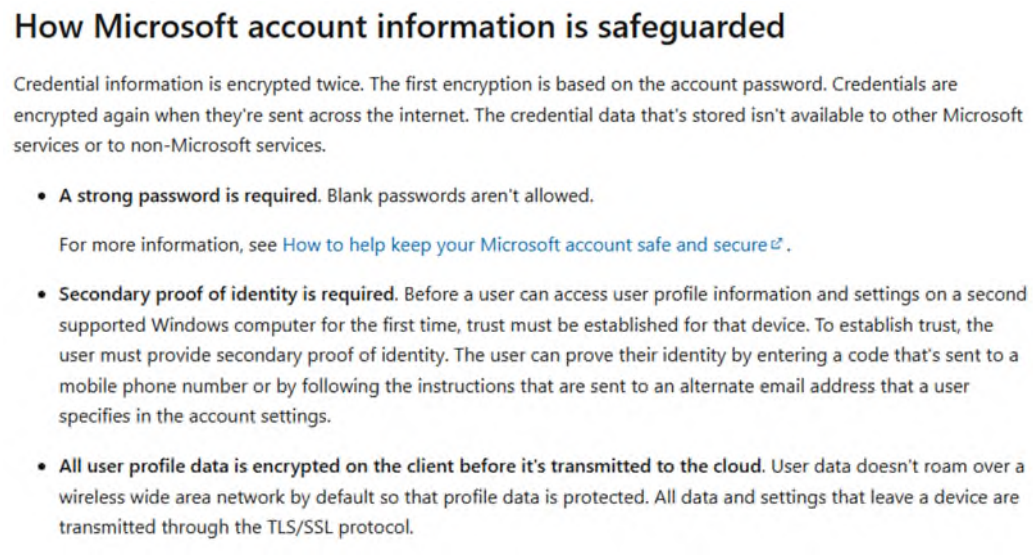
In these contentions, Microsoft has relied in part on Plaintiff's infringement contentions. In those contentions, Plaintiff appears to pursue overly broad claim constructions in an effort to assert infringement where none exists, and to accuse products that do not infringe the claims. Microsoft's assertion that a particular limitation is disclosed by a prior art reference and/or is disclosed in a particular manner may be based in part on Plaintiff's apparent claim interpretations. In relying on Plaintiff's apparent claim interpretations, Microsoft does not admit that Plaintiff's apparent claim interpretations are supportable or proper or that the claim limitations in question are definite or otherwise amenable to construction.

In addition, citations to portions of any reference in this chart are examples only. Microsoft will rely on the entirety of the references cited in this chart to show that the Asserted Claims are invalid.

Discovery is ongoing and Microsoft will update this chart pursuant to Federal Rule of Civil Procedure 26(e), the Local Rules, and the Orders of record in this matter, subject to further investigation and discovery regarding the reference, the Court's construction of the claims at issue, and discovery generally, including third-party discovery.

U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
1[pre] A computer system configured to execute software instructions stored on nontransitory machine-readable storage media, wherein the software instructions comprise instructions that:	To the extent the preamble is limiting, under Plaintiff's contentions, MSA expressly or inherently discloses "[a] computer system configured to execute software instructions stored on nontransitory machine-readable storage media," as interpreted by Qomplx in its infringement contentions. For example:

U.S. Pat. No. 12,218,934	Exemplary citations to MSA
	## What is a Microsoft account? Microsoft sites, services, properties, and computers running Windows 10 can use a Microsoft account as a way to identify a user. A Microsoft account previously was called a Windows Live ID. A Microsoft account has user-defined secrets and consists of a unique email address and a password. When a user signs in with a Microsoft account, the device is connected to cloud services. The user can share many of their settings, preferences, and apps across devices. ## How a Microsoft account works A user can use a Microsoft account to sign in to websites that support this service by using a single set of credentials. A user's credentials are validated by a Microsoft account authentication server that's associated with a website. Microsoft Store is an example of this association. When a new user signs in to a website that's enabled to use Microsoft accounts, the user is redirected to the nearest authentication server, which asks for a username and password. Windows uses the Schannel Security Support Provider to open a Transport Level Security/Secure Sockets Layer (TLS/SSL) connection for this function. Users have the option to use Credential Manager to store their credentials. When a user signs in to a website that's enabled to use a Microsoft account, a time-limited cookie is installed on their computer. The cookie includes a triple-DES encrypted ID tag. The encrypted ID tag has been agreed upon between the authentication server and the website. The ID tag is sent to the website, and the website places another time-limited encrypted HTTP cookie on the user's computer. While the cookie is valid, the user isn't required to enter a username and password. If a user actively signs out of their Microsoft account, these cookies are removed. Understand Microsoft Accounts

U.S. Pat. No. 12,218,934	Exemplary citations to MSA
	 Understand Microsoft Accounts To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[1a] receive a request to authenticate a client, wherein the request comprises an identifier and a password,	Under Plaintiff's contentions, MSA expressly or inherently discloses "receive a request to authenticate a client, wherein the request comprises an identifier and a password," as interpreted by Qomplx in its infringement contentions. For example:

U.S. Pat. No. 12,218,934	Exemplary citations to MSA
	## What is a Microsoft account? Microsoft sites, services, properties, and computers running Windows 10 can use a Microsoft account as a way to identify a user. A Microsoft account previously was called a Windows Live ID. A Microsoft account has user-defined secrets and consists of a unique email address and a password. When a user signs in with a Microsoft account, the device is connected to cloud services. The user can share many of their settings, preferences, and apps across devices. ## How a Microsoft account works A user can use a Microsoft account to sign in to websites that support this service by using a single set of credentials. A user's credentials are validated by a Microsoft account authentication server that's associated with a website. Microsoft Store is an example of this association. When a new user signs in to a website that's enabled to use Microsoft accounts, the user is redirected to the nearest authentication server, which asks for a username and password. Windows uses the Schannel Security Support Provider to open a Transport Level Security/Secure Sockets Layer (TLS/SSL) connection for this function. Users have the option to use Credential Manager to store their credentials. When a user signs in to a website that's enabled to use a Microsoft account, a time-limited cookie is installed on their computer. The cookie includes a triple-DES encrypted ID tag. The encrypted ID tag has been agreed upon between the authentication server and the website. The ID tag is sent to the website, and the website places another time-limited encrypted HTTP cookie on the user's computer. While the cookie is valid, the user isn't required to enter a username and password. If a user actively signs out of their Microsoft account, these cookies are removed. Understand Microsoft Accounts

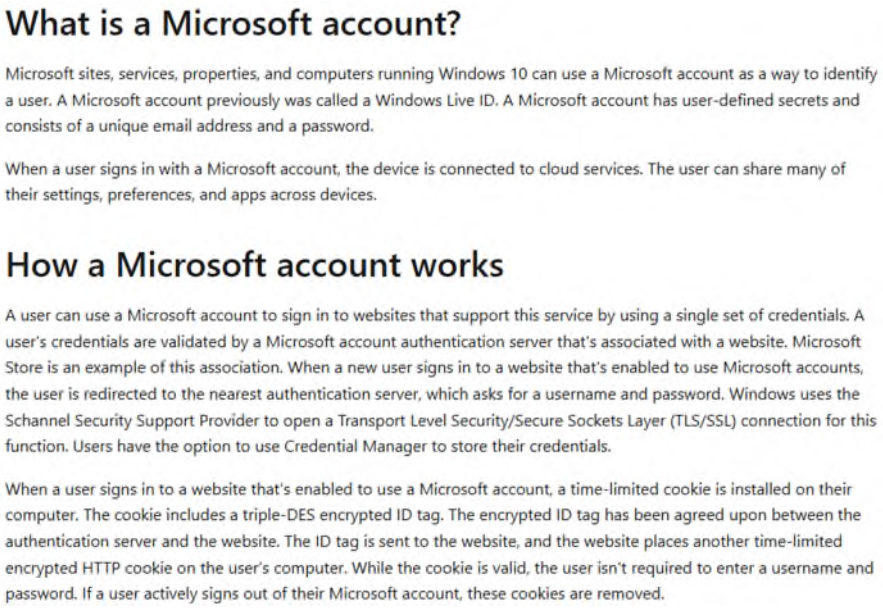
U.S. Pat. No. 12,218,934	Exemplary citations to MSA
	Overview of Using a Microsoft Account to Logon to Windows A Microsoft account—an email address and password—is a new way to sign in to any PC running Windows 8 or Windows RT or later. You might already have a Microsoft account. If you use other Microsoft services like Messenger, Hotmail or Xbox LIVE, the email address and password you use to sign in are a Microsoft account. If you have an existing Windows Live ID, that's the same thing: "Microsoft account" is the new name for what used to be called a "Windows Live ID." When you sign in with a Microsoft account, your PC is connected to the cloud, and many of the settings, preferences, and apps associated with your user account can "follow" a user between different PCs Signing up for a new Microsoft account for this feature to work is not a requirement. Many online services use a "string" like someone@example.com to represent a user name, even though that string looks like an email address. For example, when you order books at an online bookstore, your user name may look like an email address, even though your online book seller does not manage your email. The someone@example.com address is just a convenient way of identifying you, since most Internet users these days have email addresses. Your email account and password will still be managed by whatever email provider you choose, and the user name and password provided is used to synchronize and manage your settings and state across Windows PCs, even if you haven't signed up for Hotmail or other Microsoft services that use this ID. During the initial Windows user setup process, users are now prompted to optionally choose to create a new Microsoft account (formerly known as a Windows Live ID) or use an existing ID for login. If you choose to create a new account, you can use any email address you want as your new ID, and then create your unique password. Local Windows account functionality has not been removed and is still an option in managed environments. In order to download apps from the Windows Store a Microsoft account is required. Windows Server 2012

U.S. Pat. No. 12,218,934	Exemplary citations to MSA
	Hello Everyone! Today we are going to take an in-depth look at how Microsoft handles the authentication of a Microsoft Live account to a Microsoft Azure resource. The user experience may seem simple enough, but behind the scenes there is a lot going on with a number of federated authentication and authorization standards and protocols. We will use Fiddler and some online JWT decoders to capture what is going on. For this scenario we will be using a Microsoft Live account with a username of dumactmstest@gmail.com that is not configured with MFA. The resource at Microsoft Azure we will be attempting to access is the Microsoft Azure Management Portal. The first step is to navigate the browser to https://manage.windowsazure.com/ which will redirect us to https://login.microsoft.com with an OAuth 2.0 authorization request included in the header. Let's take a closer look at the authorization request: Behind the Curtain

U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
	The browser is directed to another URI at https://login.live.com where the browser posts the WS-Federation request and the user authenticates using forms-based authentication by providing a username and password. After authentication the user's browser is directed back to a URI at https://login.microsoftonline.com where the user posts result of the WS-Federation authentication request. Let's break down the interesting portions of the SAML assertion contained in the WS-Federation authentication response. • The claim below shows the user authenticated with a password. • <saml:AuthenticationStatement AuthenticationInstant="2016-04-01T23:53:00Z" AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password"> • Ever wonder what your Microsoft account UPN looks like behind the scenes? Well here you go. • <saml:Subject><saml:NameIdentifier Format="http://schemas.xmlsoap.org/claims/UPN">00037FFEE3497D1E@Live.com</saml:NameIdentifier></saml:Subject> • This claim indicates that the accounts credentials do not exist within Azure Active Directory. • <saml:Attribute AttributeName="Managed" AttributeNamespace="http://schemas.xmlsoap.org/claims"> <saml:AttributeValue>FALSE</saml:AttributeValue></saml:Attribute> • I'm assuming this is some unique identifier of the Microsoft Live account. • <saml:Attribute AttributeName="CID" AttributeNamespace="http://schemas.xmlsoap.org/claims"> <saml:AttributeValue>7f5c85a988a96054</saml:AttributeValue> </saml:Attribute> • Here is the email address associated with the account. We see here that MS assigns each Microsoft Live account a unique user principal name but allows the user to use the email address as a the identifier to improve the user experience. • <saml:Attribute AttributeName="EmailAddress" AttributeNamespace="http://schemas.xmlsoap.org/claims"> <saml:AttributeValue>dumactmstest@gmail.com</saml:AttributeValue> </saml:Attribute> Behind the Curtain To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[1b] store, in a multidimensional time-series database, information about the request,	Under Plaintiff's contentions, MSA expressly or inherently discloses "store, in a multidimensional time-series database, information about the request," as interpreted by Qomplx in its infringement contentions. For example:

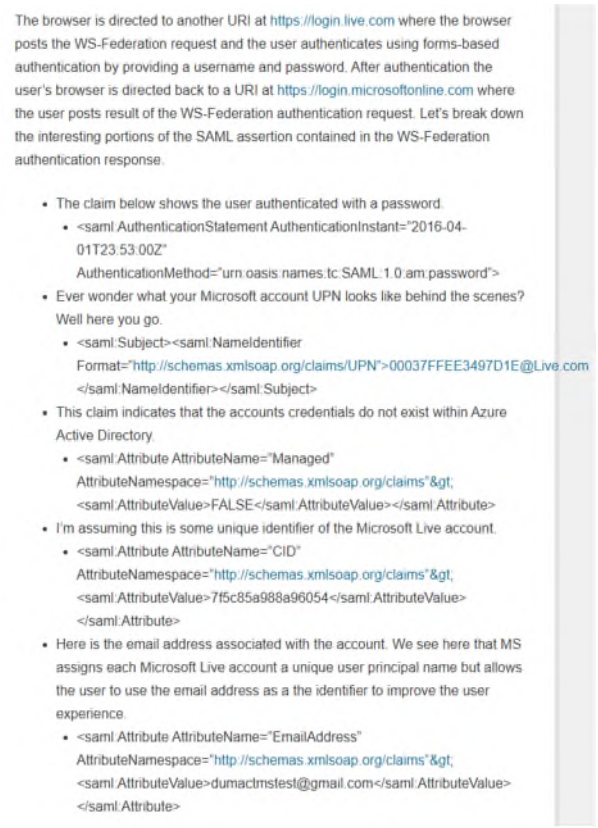
U.S. Pat. No. 12,218,934	Exemplary citations to MSA
	## What is a Microsoft account? Microsoft sites, services, properties, and computers running Windows 10 can use a Microsoft account as a way to identify a user. A Microsoft account previously was called a Windows Live ID. A Microsoft account has user-defined secrets and consists of a unique email address and a password. When a user signs in with a Microsoft account, the device is connected to cloud services. The user can share many of their settings, preferences, and apps across devices. ## How a Microsoft account works A user can use a Microsoft account to sign in to websites that support this service by using a single set of credentials. A user's credentials are validated by a Microsoft account authentication server that's associated with a website. Microsoft Store is an example of this association. When a new user signs in to a website that's enabled to use Microsoft accounts, the user is redirected to the nearest authentication server, which asks for a username and password. Windows uses the Schannel Security Support Provider to open a Transport Level Security/Secure Sockets Layer (TLS/SSL) connection for this function. Users have the option to use Credential Manager to store their credentials. When a user signs in to a website that's enabled to use a Microsoft account, a time-limited cookie is installed on their computer. The cookie includes a triple-DES encrypted ID tag. The encrypted ID tag has been agreed upon between the authentication server and the website. The ID tag is sent to the website, and the website places another time-limited encrypted HTTP cookie on the user's computer. While the cookie is valid, the user isn't required to enter a username and password. If a user actively signs out of their Microsoft account, these cookies are removed. Understand Microsoft Accounts

U.S. Pat. No. 12,218,934	Exemplary citations to MSA
	 Windows Server 2012 To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[1c] determine whether the password corresponds to a user account identified by the identifier,	Under Plaintiff's contentions, MSA expressly or inherently discloses "determine whether the password corresponds to a user account identified by the identifier," as interpreted by Qomplx in its infringement contentions.

U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
	For example:  ## What is a Microsoft account? Microsoft sites, services, properties, and computers running Windows 10 can use a Microsoft account as a way to identify a user. A Microsoft account previously was called a Windows Live ID. A Microsoft account has user-defined secrets and consists of a unique email address and a password. When a user signs in with a Microsoft account, the device is connected to cloud services. The user can share many of their settings, preferences, and apps across devices. ## How a Microsoft account works A user can use a Microsoft account to sign in to websites that support this service by using a single set of credentials. A user's credentials are validated by a Microsoft account authentication server that's associated with a website. Microsoft Store is an example of this association. When a new user signs in to a website that's enabled to use Microsoft accounts, the user is redirected to the nearest authentication server, which asks for a username and password. Windows uses the Schannel Security Support Provider to open a Transport Level Security/Secure Sockets Layer (TLS/SSL) connection for this function. Users have the option to use Credential Manager to store their credentials. When a user signs in to a website that's enabled to use a Microsoft account, a time-limited cookie is installed on their computer. The cookie includes a triple-DES encrypted ID tag. The encrypted ID tag has been agreed upon between the authentication server and the website. The ID tag is sent to the website, and the website places another time-limited encrypted HTTP cookie on the user's computer. While the cookie is valid, the user isn't required to enter a username and password. If a user actively signs out of their Microsoft account, these cookies are removed. Understand Microsoft Accounts

U.S. Pat. No. 12,218,934	Exemplary citations to MSA
	Overview of Using a Microsoft Account to Logon to Windows A Microsoft account—an email address and password—is a new way to sign in to any PC running Windows 8 or Windows RT or later. You might already have a Microsoft account. If you use other Microsoft services like Messenger, Hotmail or Xbox LIVE, the email address and password you use to sign in are a Microsoft account. If you have an existing Windows Live ID, that's the same thing: "Microsoft account" is the new name for what used to be called a "Windows Live ID." When you sign in with a Microsoft account, your PC is connected to the cloud, and many of the settings, preferences, and apps associated with your user account can "follow" a user between different PCs Signing up for a new Microsoft account for this feature to work is not a requirement. Many online services use a "string" like someone@example.com to represent a user name, even though that string looks like an email address. For example, when you order books at an online bookstore, your user name may look like an email address, even though your online book seller does not manage your email. The someone@example.com address is just a convenient way of identifying you, since most Internet users these days have email addresses. Your email account and password will still be managed by whatever email provider you choose, and the user name and password provided is used to synchronize and manage your settings and state across Windows PCs, even if you haven't signed up for Hotmail or other Microsoft services that use this ID. During the initial Windows user setup process, users are now prompted to optionally choose to create a new Microsoft account (formerly known as a Windows Live ID) or use an existing ID for login. If you choose to create a new account, you can use any email address you want as your new ID, and then create your unique password. Local Windows account functionality has not been removed and is still an option in managed environments. In order to download apps from the Windows Store a Microsoft account is required. Windows Server 2012

U.S. Pat. No. 12,218,934	Exemplary citations to MSA
	Hello Everyone! Today we are going to take an in-depth look at how Microsoft handles the authentication of a Microsoft Live account to a Microsoft Azure resource. The user experience may seem simple enough, but behind the scenes there is a lot going on with a number of federated authentication and authorization standards and protocols. We will use Fiddler and some online JWT decoders to capture what is going on. For this scenario we will be using a Microsoft Live account with a username of dumactmstest@gmail.com that is not configured with MFA. The resource at Microsoft Azure we will be attempting to access is the Microsoft Azure Management Portal. The first step is to navigate the browser to https://manage.windowsazure.com/ which will redirect us to https://login.microsoft.com with an OAuth 2.0 authorization request included in the header. Let's take a closer look at the authorization request: Behind the Curtain

U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
	 Behind the Curtain To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.

U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
[1d] determine whether an additional verification is required to grant access,	Under Plaintiff's contentions, MSA expressly or inherently discloses "determine whether an additional verification is required to grant access," as interpreted by Qomplx in its infringement contentions. For example: *See* [1f] and [1g] **How Microsoft account information is safeguarded** Credential information is encrypted twice. The first encryption is based on the account password. Credentials are encrypted again when they're sent across the internet. The credential data that's stored isn't available to other Microsoft services or to non-Microsoft services. • **A strong password is required**. Blank passwords aren't allowed. For more information, see How to help keep your Microsoft account safe and secure. • **Secondary proof of identity is required**. Before a user can access user profile information and settings on a second supported Windows computer for the first time, trust must be established for that device. To establish trust, the user must provide secondary proof of identity. The user can prove their identity by entering a code that's sent to a mobile phone number or by following the instructions that are sent to an alternate email address that a user specifies in the account settings. • **All user profile data is encrypted on the client before it's transmitted to the cloud**. User data doesn't roam over a wireless wide area network by default so that profile data is protected. All data and settings that leave a device are transmitted through the TLS/SSL protocol. Understand Microsoft Accounts If the user decides to enable the full protection provided by two-factor authentication, nothing will really change except that secondary verification will take place at every attempt to sign in to a Microsoft Account. In a way, this all means that two-factor authentication for Microsoft Accounts is always there. Whether the user has the switch "enabled" or "disabled" only affects the scope of protection: "enabled" two-factor authentication protects all sign-in requests, while if the additional protection is "disabled" it only protects against suspicious sign-in activities and highly sensitive operations such as restoring data from a cloud backup and syncing Internet Explorer/Edge passwords with a new device.

U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
	MSA 2FA Always There To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[1e] wherein determining whether the additional verification is required to grant access comprises:	Under Plaintiff's contentions, MSA expressly or inherently discloses "wherein determining whether the additional verification is required to grant access comprises," as interpreted by Qomplx in its infringement contentions. For example: *See* [1f] and [1g] If the user decides to enable the full protection provided by two-factor authentication, nothing will really change except that secondary verification will take place at every attempt to sign in to a Microsoft Account. In a way, this all means that two-factor authentication for Microsoft Accounts is always there. Whether the user has the switch "enabled" or "disabled" only affects the scope of protection: "enabled" two-factor authentication protects all sign-in requests, while if the additional protection is "disabled" it only protects against suspicious sign-in activities and highly sensitive operations such as restoring data from a cloud backup and syncing Internet Explorer/Edge passwords with a new device. MSA 2FA Always There To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.

U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
[1f] retrieving, from the multidimensional time-series database, historical information about previous access requests associated with the user account, and	Under Plaintiff's contentions, MSA expressly or inherently discloses "retrieving, from the multidimensional time-series database, historical information about previous access requests associated with the user account," as interpreted by Qomplx in its infringement contentions. For example: **How Microsoft account information is safeguarded** Credential information is encrypted twice. The first encryption is based on the account password. Credentials are encrypted again when they're sent across the internet. The credential data that's stored isn't available to other Microsoft services or to non-Microsoft services. • **A strong password is required**. Blank passwords aren't allowed. For more information, see How to help keep your Microsoft account safe and secure. • **Secondary proof of identity is required**. Before a user can access user profile information and settings on a second supported Windows computer for the first time, trust must be established for that device. To establish trust, the user must provide secondary proof of identity. The user can prove their identity by entering a code that's sent to a mobile phone number or by following the instructions that are sent to an alternate email address that a user specifies in the account settings. • **All user profile data is encrypted on the client before it's transmitted to the cloud**. User data doesn't roam over a wireless wide area network by default so that profile data is protected. All data and settings that leave a device are transmitted through the TLS/SSL protocol. Understand Microsoft Accounts

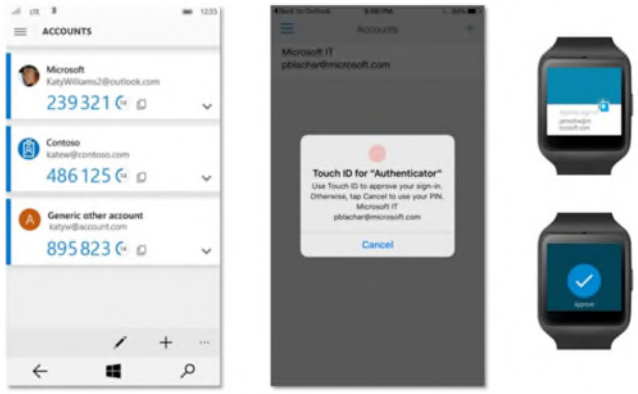
U.S. Pat. No. 12,218,934	Exemplary citations to MSA
	Microsoft employs a somewhat unique approach to two-factor authentication. Even if the user does not want to use two-factor authentication and does not set up any secondary authentication methods, in some circumstances Microsoft would still prompt to confirm account login. Just like Google, the company would verify unusual sign-in activities occurring from a new device in another country. However, it's not just that. Microsoft would also try to verify Microsoft Account activities once the user attempts to restore a new phone (Windows Phone 8.1 or Windows 10 Mobile) from OneDrive backup. Interestingly, Microsoft would do exactly the same verification if one sets up an account on a new PC (desktop, laptop or tablet) and attempts to restore from OneDrive backup. If no two-factor authentication is configured but the user has a trusted phone number and the device being set up is a new phone, Microsoft will attempt to send a text message to that phone. Interestingly, the SMS will be automatically processed by the setup tool; no user interaction would be required when setting up that phone. What's so unique about this setup is the ability for the user to configure all possible two-factor authentication methods (SMS, push, TOTP etc.) without actually ENABLING two-factor authentication. For example, one can set up offline authentication with Authenticator app (made by Google, Microsoft, or one of the many third parties) as well as prompt-based authentication with Microsoft Authenticator (available for Google, iOS and both versions of Windows 10). The second authentication factor will NOT be normally prompted. However, if Microsoft detects unusual sign-in activity, or if the user attempts performing a highly sensitive operation (restoring from a cloud backup, syncing passwords), the system will then request additional verification with any method. MSA 2FA Always There To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.

U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
[1g] determining, based at least on the historical information, whether the user account is associated with a previous access request to a network resource, wherein the previous access request to the network resource is anomalous relative to a baseline profile of access requests;	Under Plaintiff's contentions, MSA expressly or inherently discloses "determining, based at least on the historical information, whether the user account is associated with a previous access request to a network resource, wherein the previous access request to the network resource is anomalous relative to a baseline profile of access requests," as interpreted by Qomplx in its infringement contentions. For example: **How Microsoft account information is safeguarded** Credential information is encrypted twice. The first encryption is based on the account password. Credentials are encrypted again when they're sent across the internet. The credential data that's stored isn't available to other Microsoft services or to non-Microsoft services. • **A strong password is required**. Blank passwords aren't allowed. For more information, see How to help keep your Microsoft account safe and secure. • **Secondary proof of identity is required**. Before a user can access user profile information and settings on a second supported Windows computer for the first time, trust must be established for that device. To establish trust, the user must provide secondary proof of identity. The user can prove their identity by entering a code that's sent to a mobile phone number or by following the instructions that are sent to an alternate email address that a user specifies in the account settings. • **All user profile data is encrypted on the client before it's transmitted to the cloud**. User data doesn't roam over a wireless wide area network by default so that profile data is protected. All data and settings that leave a device are transmitted through the TLS/SSL protocol. Understand Microsoft Accounts

U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
	Microsoft employs a somewhat unique approach to two-factor authentication. Even if the user does not want to use two-factor authentication and does not set up any secondary authentication methods, in some circumstances Microsoft would still prompt to confirm account login. Just like Google, the company would verify unusual sign-in activities occurring from a new device in another country. However, it's not just that. Microsoft would also try to verify Microsoft Account activities once the user attempts to restore a new phone (Windows Phone 8.1 or Windows 10 Mobile) from OneDrive backup. Interestingly, Microsoft would do exactly the same verification if one sets up an account on a new PC (desktop, laptop or tablet) and attempts to restore from OneDrive backup. If no two-factor authentication is configured but the user has a trusted phone number and the device being set up is a new phone, Microsoft will attempt to send a text message to that phone. Interestingly, the SMS will be automatically processed by the setup tool; no user interaction would be required when setting up that phone. What's so unique about this setup is the ability for the user to configure all possible two-factor authentication methods (SMS, push, TOTP etc.) without actually ENABLING two-factor authentication. For example, one can set up offline authentication with Authenticator app (made by Google, Microsoft, or one of the many third parties) as well as prompt-based authentication with Microsoft Authenticator (available for Google, iOS and both versions of Windows 10). The second authentication factor will NOT be normally prompted. However, if Microsoft detects unusual sign-in activity, or if the user attempts performing a highly sensitive operation (restoring from a cloud backup, syncing passwords), the system will then request additional verification with any method. MSA 2FA Always There To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.

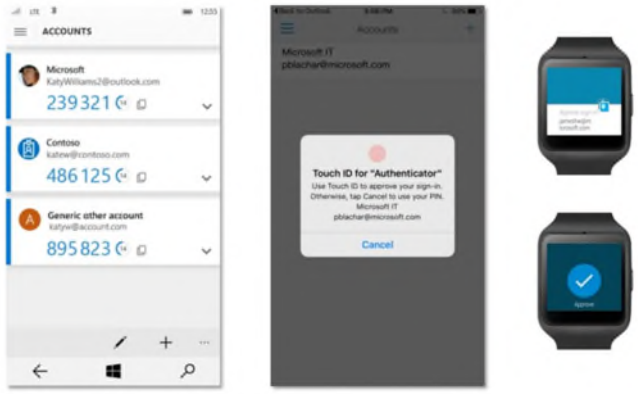
U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
[1h] based on the additional verification being required to grant access: [1i] select an additional verification method from a plurality of verification methods	Under Plaintiff's contentions, MSA expressly or inherently discloses "based on the additional verification being required to grant access: select an additional verification method from a plurality of verification methods," as interpreted by Qomplx in its infringement contentions. For example: *See* claim [1i], [1j], [1k]. Microsoft employs a somewhat unique approach to two-factor authentication. Even if the user does not want to use two-factor authentication and does not set up any secondary authentication methods, in some circumstances Microsoft would still prompt to confirm account login. Just like Google, the company would verify unusual sign-in activities occurring from a new device in another country. However, it's not just that. Microsoft would also try to verify Microsoft Account activities once the user attempts to restore a new phone (Windows Phone 8.1 or Windows 10 Mobile) from OneDrive backup. Interestingly, Microsoft would do exactly the same verification if one sets up an account on a new PC (desktop, laptop or tablet) and attempts to restore from OneDrive backup. If no two-factor authentication is configured but the user has a trusted phone number and the device being set up is a new phone, Microsoft will attempt to send a text message to that phone. Interestingly, the SMS will be automatically processed by the setup tool; no user interaction would be required when setting up that phone. What's so unique about this setup is the ability for the user to configure all possible two-factor authentication methods (SMS, push, TOTP etc.) without actually ENABLING two-factor authentication. For example, one can set up offline authentication with Authenticator app (made by Google, Microsoft, or one of the many third parties) as well as prompt-based authentication with Microsoft Authenticator (available for Google, iOS and both versions of Windows 10). The second authentication factor will NOT be normally prompted. However, if Microsoft detects unusual sign-in activity, or if the user attempts performing a highly sensitive operation (restoring from a cloud backup, syncing passwords), the system will then request additional verification with any method. MSA 2FA Always There

U.S. Pat. No. 12,218,934	Exemplary citations to MSA
	Microsoft Account: Delivery Options Microsoft offers plenty of delivery options for secondary authentication. This includes: » A code sent to backup email address (Microsoft or non-Microsoft email addresses supported) » Text message sent to a trusted phone number » Identity verification app: interactive prompt (similar to Google Prompt) delivered to Microsoft Authenticator apps on Windows, Android and iOS » Previously, Microsoft Account app was used on Android for the same purpose » Microsoft Authenticator app integrates interactive authentication functionality for Microsoft Accounts with TOTP for third-party accounts » App-specific passwords » An email is sent every time the user attempts to sign in from an app or device not supporting two-factor authentication, suggests using app-specific password » If Microsoft knows such apps or devices are used, an app-specific password will be generated and displayed automatically as the user sets up two-factor authentication for the first time » Alerts are delivered to trusted emails and phone numbers » Printable recovery code (for reinstating account access) MSA 2FA Always There To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[1j] cause the client to be prompted to complete the additional verification method, and	Under Plaintiff's contentions, MSA expressly or inherently discloses "cause the client to be prompted to complete the additional verification method," as interpreted by Qomplx in its infringement contentions. For example:

U.S. Pat. No. 12,218,934	Exemplary citations to MSA
	Microsoft will begin rolling out its new unified "Microsoft Authenticator" app across a variety of mobile apps stores starting August 15.  Credit: Microsoft The new Microsoft Authenticator will combine different pieces of Microsoft's current set of authenticator apps into a new single app that will work with both Microsoft accounts and Azure Active Directory accounts. The new app is meant for both consumer and enterprise customers. ZDNet The coming app will allow users to simply click an "approve" button in a notification to complete their two-factor authentications. The coming app will support wearables including Apple Watch and Samsung Gear, and will support fingerprint-based approvals instead of passcodes on iPhones and Android phones. (I'm asking about support for Microsoft Band and Windows Phones, since Microsoft's post on this mentions neither.) / read this ZDNet

U.S. Pat. No. 12,218,934	Exemplary citations to MSA
	Microsoft Account: Delivery Options Microsoft offers plenty of delivery options for secondary authentication. This includes: » A code sent to backup email address (Microsoft or non-Microsoft email addresses supported) » Text message sent to a trusted phone number » Identity verification app: interactive prompt (similar to Google Prompt) delivered to Microsoft Authenticator apps on Windows, Android and iOS » Previously, Microsoft Account app was used on Android for the same purpose » Microsoft Authenticator app integrates interactive authentication functionality for Microsoft Accounts with TOTP for third-party accounts » App-specific passwords » An email is sent every time the user attempts to sign in from an app or device not supporting two-factor authentication, suggests using app-specific password » If Microsoft knows such apps or devices are used, an app-specific password will be generated and displayed automatically as the user sets up two-factor authentication for the first time » Alerts are delivered to trusted emails and phone numbers » Printable recovery code (for reinstating account access) MSA 2FA Always There

U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
	Microsoft Identity Verification App: Push and TOTP Microsoft implements push-based authentication prompt via its proprietary Microsoft Authenticator app. Historically, Microsoft offered this authentication experience exclusively on the Android platform via the Microsoft Account app. Ironically, this very functionality was not available on Microsoft's own mobile operating system, Windows Phone 8.1 and later Windows 10 Mobile. It was only recently that Microsoft has released a proper Microsoft Authenticator app with an interactive authentication prompt. In this case, it's a simple "Yes" or "No" prompt with no additional code displayed or required. Each prompt has its own unique identifier allowing the user to see if the request comes from the login session they are trying to authenticate. This type of authentication is server-based. Confirming the request automatically verifies sign-in session. Interestingly, Microsoft Authenticator operates differently across platforms. Android and iOS devices must be unlocked in order for the user to access the prompt. Windows 10 Mobile devices will display the authentication prompt and allow the user to confirm the request even if the phone is locked. This is one major security issue with Microsoft's implementation on Windows 10 Mobile smartphones. MSA 2FA Always There To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[1k] determine whether the additional verification method has been completed correctly.	Under Plaintiff's contentions, MSA expressly or inherently discloses "determine whether the additional verification method has been completed correctly," as interpreted by Qomplx in its infringement contentions. For example:

U.S. Pat. No. 12,218,934	Exemplary citations to MSA
	Microsoft will begin rolling out its new unified "Microsoft Authenticator" app across a variety of mobile apps stores starting August 15.  Credit: Microsoft The new Microsoft Authenticator will combine different pieces of Microsoft's current set of authenticator apps into a new single app that will work with both Microsoft accounts and Azure Active Directory accounts. The new app is meant for both consumer and enterprise customers. ZDNet The coming app will allow users to simply click an "approve" button in a notification to complete their two-factor authentications. The coming app will support wearables including Apple Watch and Samsung Gear, and will support fingerprint-based approvals instead of passcodes on iPhones and Android phones. (I'm asking about support for Microsoft Band and Windows Phones, since Microsoft's post on this mentions neither.) / read this ZDNet

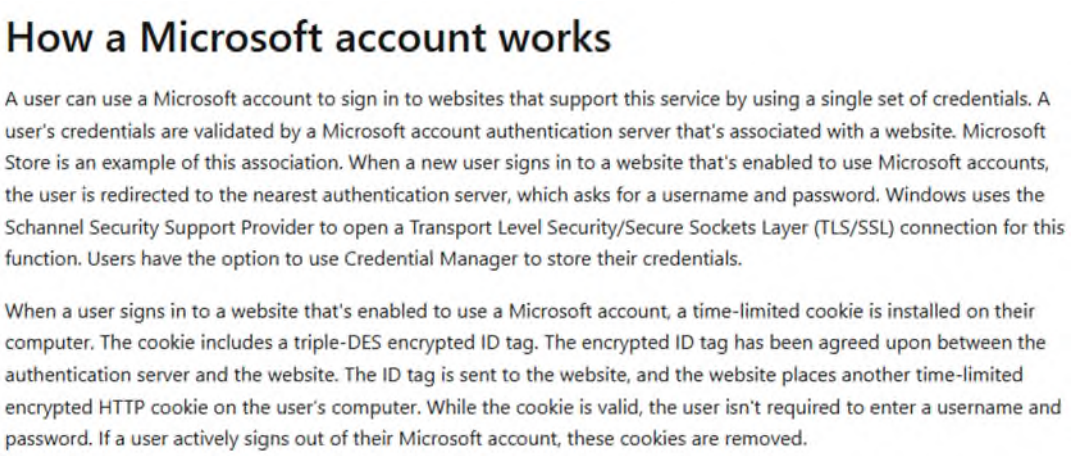
U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
	To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
2. The computer system of claim 1, wherein the historical information about previous access requests associated with the user account comprises historical information about previous requests to authenticate, wherein the previous requests to authenticate comprise the identifier.	Under Plaintiff's contentions, MSA expressly or inherently discloses "[t]he computer system of claim 1, wherein the historical information about previous access requests associated with the user account comprises historical information about previous requests to authenticate, wherein the previous requests to authenticate comprise the identifier," as interpreted by Qomplx in its infringement contentions. For example: *See* [1f] and [1g] To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
4. The computer system of claim 1, wherein determining whether the additional verification is required to grant access further comprises processing an external threat intelligence feed.	Under Plaintiff's contentions, MSA expressly or inherently discloses "[t]he computer system of claim 1, wherein determining whether the additional verification is required to grant access further comprises processing an external threat intelligence feed," as interpreted by Qomplx in its infringement contentions. For example: *See* Claim 1 To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
5[a] The computer system of claim 1, wherein the software instructions further comprise instructions that:	Under Plaintiff's contentions, MSA expressly or inherently discloses "[t]he computer system of claim 1, wherein the software instructions further comprise instructions that: based on the additional verification being required to grant access: determine that a probable cyberattack is detected," as interpreted by Qomplx in its infringement contentions.

Qomplx LLC, Exhibit 2006
Page 2006 - 27
IPR2026-00182, Microsoft Corp. v. Qomplx LLC

U.S. Pat. No. 12,218,934	Exemplary citations to MSA
based on the additional verification being required to grant access: determine that a probable cyberattack is detected, and	For example: *See* Claim 1 Microsoft employs a somewhat unique approach to two-factor authentication. Even if the user does not want to use two-factor authentication and does not set up any secondary authentication methods, in some circumstances Microsoft would still prompt to confirm account login. Just like Google, the company would verify unusual sign-in activities occurring from a new device in another country. However, it's not just that. Microsoft would also try to verify Microsoft Account activities once the user attempts to restore a new phone (Windows Phone 8.1 or Windows 10 Mobile) from OneDrive backup. Interestingly, Microsoft would do exactly the same verification if one sets up an account on a new PC (desktop, laptop or tablet) and attempts to restore from OneDrive backup. If no two-factor authentication is configured but the user has a trusted phone number and the device being set up is a new phone, Microsoft will attempt to send a text message to that phone. Interestingly, the SMS will be automatically processed by the setup tool; no user interaction would be required when setting up that phone. What's so unique about this setup is the ability for the user to configure all possible two-factor authentication methods (SMS, push, TOTP etc.) without actually ENABLING two-factor authentication. For example, one can set up offline authentication with Authenticator app (made by Google, Microsoft, or one of the many third parties) as well as prompt-based authentication with Microsoft Authenticator (available for Google, iOS and both versions of Windows 10). The second authentication factor will NOT be normally prompted. However, if Microsoft detects unusual sign-in activity, or if the user attempts performing a highly sensitive operation (restoring from a cloud backup, syncing passwords), the system will then request additional verification with any method. MSA 2FA Always There To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.

U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
[5b] provide an alert,	Under Plaintiff's contentions, MSA expressly or inherently discloses "provide an alert," as interpreted by Qomplx in its infringement contentions. For example: » Alerts are delivered to trusted emails and phone numbers MSA 2FA Always There **Microsoft account security information** A user can add security information to their Microsoft account through the Accounts interface on computers running supported versions of Windows. In Accounts, the user can update the security information that they provided when they created their account. This security information includes an alternate email address or phone number so that if their password is compromised or forgotten, a verification code can be sent to verify their identity. A user can potentially use their Microsoft account to store corporate data on a personal OneDrive or email app. A safe practice is for the account owner to keep this security information up-to-date. Understanding Microsoft Accounts To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[5c] wherein the alert includes the identifier and an indicator that a probable cyberattack is detected, and	Under Plaintiff's contentions, MSA expressly or inherently discloses "wherein the alert includes the identifier and an indicator that a probable cyberattack is detected," as interpreted by Qomplx in its infringement contentions. For example: *See* [5b] and Claim 1. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.

U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
[5d] wherein the alert is designated to be provided to an administrator of the network	Under Plaintiff's contentions, MSA expressly or inherently discloses "wherein the alert is designated to be provided to an administrator of the network," as interpreted by Qomplx in its infringement contentions. For example: *See* [5b] and Claim 1. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
9. The computer system of claim 1, wherein the computer system comprises a plurality of physical computing machines.	Under Plaintiff's contentions, MSA expressly or inherently discloses "[t]he computer system of claim 1, wherein the computer system comprises a plurality of physical computing machines," as interpreted by Qomplx in its infringement contentions. For example: It was only recently that Microsoft has released a proper Microsoft Authenticator app with an interactive authentication prompt. In this case, it's a simple "Yes" or "No" prompt with no additional code displayed or required. Each prompt has its own unique identifier allowing the user to see if the request comes from the login session they are trying to authenticate. This type of authentication is server-based. Confirming the request automatically verifies sign-in session. MSA 2FA Always There

U.S. Pat. No. 12,218,934	Exemplary citations to MSA
	 Understand Microsoft Accounts To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
11[pre]. A method implemented on a computer system connected to a network, the method comprising:	To the extent the preamble is limiting, under Plaintiff's contentions, MSA expressly or inherently discloses "[a] method implemented on a computer system connected to a network," as interpreted by Qomplx in its infringement contentions. For example: *See* claim [1pre] To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.

U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
[11a] receiving a request to authenticate a client, wherein the request comprises an identifier and a password,	Under Plaintiff's contentions, MSA expressly or inherently discloses "receiving a request to authenticate a client, wherein the request comprises an identifier and a password," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1a]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[11b] storing, in a multidimensional time-series database, information about the request,	Under Plaintiff's contentions, MSA expressly or inherently discloses "storing, in a multidimensional time-series database, information about the request," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1b]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[11c] determining whether the password corresponds to a user account identified by the identifier,	Under Plaintiff's contentions, MSA expressly or inherently discloses "determining whether the password corresponds to a user account identified by the identifier," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1c]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[11d] determining whether an additional verification is required to grant access,	Under Plaintiff's contentions, MSA expressly or inherently discloses "determining whether an additional verification is required to grant access," as interpreted by Qomplx in its infringement contentions. For example:

U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
	See above at claim [1d]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[11e] wherein determining whether the additional verification is required to grant access comprises:	Under Plaintiff's contentions, MSA expressly or inherently discloses "wherein determining whether the additional verification is required to grant access comprises," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1e]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[11f] retrieving, from the multidimensional time-series database, historical information about previous access requests associated with the user account,	Under Plaintiff's contentions, MSA expressly or inherently discloses "retrieving, from the multidimensional time-series database, historical information about previous access requests associated with the user account," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1f]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[11g] determining, based at least on the historical information, whether the user account is associated with a previous access request to a network resource, wherein the previous access request to the network resource is	Under Plaintiff's contentions, MSA expressly or inherently discloses "determining, based at least on the historical information, whether the user account is associated with a previous access request to a network resource, wherein the previous access request to the network resource is anomalous relative to a baseline profile of access requests," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1g]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to

U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
anomalous relative to a baseline profile of access requests; and,	them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[11h] to require based on the additional verification being required to grant access:	Under Plaintiff's contentions, MSA expressly or inherently discloses "to require based on the additional verification being required to grant access," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1h], [1i], [1j], and [1k]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[11i] selecting an additional verification method from a plurality of verification methods	Under Plaintiff's contentions, MSA expressly or inherently discloses "selecting an additional verification method from a plurality of verification methods," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1i] To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[11j] causing the client to be prompted to complete the additional verification method, and	Under Plaintiff's contentions, MSA expressly or inherently discloses " causing the client to be prompted to complete the additional verification method," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1j]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.

U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
[11k] determining whether the additional verification method has been completed correctly.	Under Plaintiff's contentions, MSA expressly or inherently discloses " determining whether the additional verification method has been completed correctly," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1k]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
12. The method of claim 11, wherein the historical information about previous access requests associated with the user account comprises historical information about previous requests to authenticate, wherein the previous requests to authenticate comprise the identifier.	Under Plaintiff's contentions, MSA expressly or inherently discloses "[t]he method of claim 11, wherein the historical information about previous access requests associated with the user account comprises historical information about previous requests to authenticate, wherein the previous requests to authenticate comprise the identifier," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim 2. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
14. The method of claim 11, wherein determining whether the additional verification is required to grant access further comprises processing an external threat intelligence feed.	Under Plaintiff's contentions, MSA expressly or inherently discloses "[t]he method of claim 11, wherein determining whether the additional verification is required to grant access further comprises processing an external threat intelligence feed," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim 4. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
15[a] The method of claim 11, further comprising: require based on the additional verification being	Under Plaintiff's contentions, MSA expressly or inherently discloses "[t]he method of claim 11, further comprising: require based on the additional verification being required to grant access: determining that a probable cyberattack is detected," as interpreted by Qomplx in its infringement contentions. For example:

U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
required to grant access: determining that a probable cyberattack is detected, and	*See* above at claim [5a]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[15b] delivering an alert,	Under Plaintiff's contentions, MSA expressly or inherently discloses "delivering an alert," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [5b]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[15c] wherein the alert includes the identifier and an indicator that a probable cyberattack is detected, and	Under Plaintiff's contentions, MSA expressly or inherently discloses "wherein the alert includes the identifier and an indicator that a probable cyberattack is detected," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [5c]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[15d] wherein the alert is designated to be delivered to an administrator of the network.	Under Plaintiff's contentions, MSA expressly or inherently discloses "wherein the alert is designated to be delivered to an administrator of the network," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [5d]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to

U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
	them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
18[pre]. A computer system is configured to execute software instructions stored on nontransitory machine-readable storage media, wherein the software instructions comprise instructions that:	To the extent the preamble is limiting, under Plaintiff's contentions, MSA expressly or inherently discloses "[a] computer system is configured to execute software instructions stored on nontransitory machine-readable storage media," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim 1[pre]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[18a] receive a request to authenticate a client, wherein the request comprises an identifier and a password,	Under Plaintiff's contentions, MSA expressly or inherently discloses "receive a request to authenticate a client, wherein the request comprises an identifier and a password," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1a]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[18b] store, in a multidimensional time-series database, information about the request,	Under Plaintiff's contentions, MSA expressly or inherently discloses "store, in a multidimensional time-series database, information about the request," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1b]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.

U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
[18c] determine whether the password corresponds to a user account identified by the identifier,	Under Plaintiff's contentions, MSA expressly or inherently discloses "determine whether the password corresponds to a user account identified by the identifier," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1c]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[18d] determine whether an additional verification is required to grant access,	Under Plaintiff's contentions, MSA expressly or inherently discloses "determine whether an additional verification is required to grant access," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1d]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[18e] wherein determining whether the additional verification is required to grant access comprises:	Under Plaintiff's contentions, MSA expressly or inherently discloses "wherein determining whether the additional verification is required to grant access comprises," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1e]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[18f] retrieving, from the multidimensional time-series database, historical information about previous access requests	Under Plaintiff's contentions, MSA expressly or inherently discloses "retrieving, from the multidimensional time-series database, historical information about previous access requests associated with the user account," as interpreted by Qomplx in its infringement contentions. For example:

U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
associated with the user account, and	*See* above at claim [1f]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[18g] determining, based at least on the historical information, whether the user account is associated with a plurality of requests to authenticate comprising a brute force attack; and,	Under Plaintiff's contentions, MSA expressly or inherently discloses "determining, based at least on the historical information, whether the user account is associated with a plurality of requests to authenticate comprising a brute force attack," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1g]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[18h] based on the additional verification being required to grant access:	Under Plaintiff's contentions, MSA expressly or inherently discloses "based on the additional verification being required to grant access," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1h]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[18i] select an additional verification method from a plurality of verification methods,	Under Plaintiff's contentions, MSA expressly or inherently discloses "select an additional verification method from a plurality of verification methods," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1i]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.

U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
[18j] cause the client to be prompted to complete the additional verification method, and	Under Plaintiff's contentions, MSA expressly or inherently discloses "cause the client to be prompted to complete the additional verification method," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1j]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[18k] determine whether the additional verification method has been completed correctly.	Under Plaintiff's contentions, MSA expressly or inherently discloses "determine whether the additional verification method has been completed correctly," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1k]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
20. The computer system of claim 18 wherein determining whether the additional verification is required to grant access further comprises processing an external threat intelligence feed.	Under Plaintiff's contentions, MSA expressly or inherently discloses "[t]he computer system of claim 18 wherein determining whether the additional verification is required to grant access further comprises processing an external threat intelligence feed," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim 4. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[21a] The computer system of claim 18, wherein the software instructions further comprise	Under Plaintiff's contentions, MSA expressly or inherently discloses "The computer system of claim 18, wherein the software instructions further comprise instructions that: based on the additional verification being

U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
instructions that: based on the additional verification being required to grant access: determine that a probable cyberattack is detected, and	required to grant access: determine that a probable cyberattack is detected," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [5a]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[21b] provide an alert,	Under Plaintiff's contentions, MSA expressly or inherently discloses "provide an alert," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [5b]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[21c] wherein the alert includes the identifier and an indicator that a probable cyberattack is detected, and	Under Plaintiff's contentions, MSA expressly or inherently discloses "wherein the alert includes the identifier and an indicator that a probable cyberattack is detected," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [5c]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[21d] wherein the alert is designated to be provided to an administrator of the network.	Under Plaintiff's contentions, MSA expressly or inherently discloses "wherein the alert is designated to be provided to an administrator of the network," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [5d].

U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
	To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
24. The computer system of claim 18, wherein the computer system comprises a plurality of physical computing machines.	Under Plaintiff's contentions, MSA expressly or inherently discloses "[t]he computer system of claim 18, wherein the computer system comprises a plurality of physical computing machines," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim 9. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
26[pre]. A method implemented on a computer system connected to a network, the method comprising:	To the extent the preamble is limiting, under Plaintiff's contentions, MSA expressly or inherently discloses "[a] method implemented on a computer system connected to a network," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim 1[pre]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[26a] receiving a request to authenticate a client, wherein the request comprises an identifier and a password,	Under Plaintiff's contentions, MSA expressly or inherently discloses "receiving a request to authenticate a client, wherein the request comprises an identifier and a password," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1a]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.

U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
[26b] storing, in a multidimensional time-series database, information about the request,	Under Plaintiff's contentions, MSA expressly or inherently discloses "storing, in a multidimensional time-series database, information about the request," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1b]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[26c] determining whether the password corresponds to a user account identified by the identifier,	Under Plaintiff's contentions, MSA expressly or inherently discloses "determining whether the password corresponds to a user account identified by the identifier," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1c]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[26d] determining whether an additional verification is required to grant access,	Under Plaintiff's contentions, MSA expressly or inherently discloses "determining whether an additional verification is required to grant access," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1d]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[26e] wherein determining whether the additional verification is required to grant access comprises:	Under Plaintiff's contentions, MSA expressly or inherently discloses "wherein determining whether the additional verification is required to grant access comprises," as interpreted by Qomplx in its infringement contentions. For example:

U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
	See above at claim [1e]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[26f] retrieving, from the multidimensional time-series database, historical information about previous access requests associated with the user account, and	Under Plaintiff's contentions, MSA expressly or inherently discloses "retrieving, from the multidimensional time-series database, historical information about previous access requests associated with the user account," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1f]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[26g] determining, based at least on the historical information, whether the user account is associated with a plurality of requests to authenticate comprising a brute force attack; and,	Under Plaintiff's contentions, MSA expressly or inherently discloses "determining, based at least on the historical information, whether the user account is associated with a plurality of requests to authenticate comprising a brute force attack," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [18g]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[26h] based on the additional verification being required to grant access:	Under Plaintiff's contentions, MSA expressly or inherently discloses "based on the additional verification being required to grant access," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1h]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.

U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
[26i] selecting an additional verification method from a plurality of verification methods,	Under Plaintiff's contentions, MSA expressly or inherently discloses "selecting an additional verification method from a plurality of verification methods," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1i]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[26j] causing the client to be prompted to complete the additional verification method, and	Under Plaintiff's contentions, MSA expressly or inherently discloses "causing the client to be prompted to complete the additional verification method," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1j]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[26k] determining whether the additional verification method has been completed correctly.	Under Plaintiff's contentions, MSA expressly or inherently discloses "determining whether the additional verification method has been completed correctly," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [1k]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
28. The method of claim 26, wherein determining whether the additional verification is required to grant access further comprises	Under Plaintiff's contentions, MSA expressly or inherently discloses "[t]he method of claim 26, wherein determining whether the additional verification is required to grant access further comprises processing an external threat intelligence feed," as interpreted by Qomplx in its infringement contentions. For example:

U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
processing an external threat intelligence feed.	*See* above at claim 4. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
29[a] The method of claim 26, further comprising: based on the additional verification being required to grant access: determining that a probable cyberattack is detected, and	Under Plaintiff's contentions, MSA expressly or inherently discloses "The method of claim 26, further comprising: based on the additional verification being required to grant access: determining that a probable cyberattack is detected," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [5a]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art
[29b] delivering an alert,	Under Plaintiff's contentions, MSA expressly or inherently discloses "delivering an alert," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [5b]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[29c] wherein the alert includes the identifier and an indicator that a probable cyberattack is detected, and	Under Plaintiff's contentions, MSA expressly or inherently discloses "wherein the alert includes the identifier and an indicator that a probable cyberattack is detected," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [5c]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to

U.S. Pat. No. 12,218,934	**Exemplary citations to** MSA
	them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[29d] wherein the alert is designated to be delivered to an administrator of the network.	Under Plaintiff's contentions, MSA expressly or inherently discloses "wherein the alert is designated to be delivered to an administrator of the network," as interpreted by Qomplx in its infringement contentions. For example: *See* above at claim [5d]. To the extent that MSA does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of MSA , those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in Microsoft's other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.