

Ex. B-10 — Invalidity of the '426 Patent in view of Microsoft Azure Active Directory (“Azure AD”)

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

Microsoft Azure Active Directory (“Azure AD”), qualifies as prior art to U.S. Patent No. 12,231,426 (“the '426 patent”) at least under AIA 35 U.S.C. §§ 102 and/or 103. To the extent Plaintiff asserts that the '426 patent is entitled to an earlier priority date pre-dating the AIA, Azure AD is prior art to the '426 patent under pre-AIA 35 U.S.C. §§ 102 and/or 103. Azure AD 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 '426 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 '426 patent is entitled to a pre-AIA priority date, under re-AIA 35 U.S.C. §§ 102(a),(b), and (g) and 103.

Azure AD anticipates the Asserted Claims of the '426 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)¹ were in existence as part of Azure AD before the '426 patent’s priority date, and thus, Azure AD predates and anticipates the '426 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 '426 patent; rather, to the extent Qomplx bases its infringement allegations on certain functionalities in Entra ID, those functionalities existed in Azure AD and predate the priority date for the '426 patent.

To the extent it is found that Azure AD 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 Azure AD does not anticipate the Asserted Claims, Azure AD 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. B–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 Azure AD 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 Azure AD system are disclosed in the following:

- Microsoft, *What is Azure Multi-Factor Authentication*, available at <https://web.archive.org/web/20160314054531/https://azure.microsoft.com/en-us/documentation/articles/multi-factor-authentication/> (herein after “What is Azure Multi Factor Authentication”)

¹ Qomplx’s infringement contentions reference Microsoft Entra ID. As of October 1, 2023, Microsoft Azure Active Directory was renamed Microsoft Entra ID.

- Microsoft, *Azure Active Directory Identity Protection*, available at <https://web.archive.org/web/20160419012327/https://azure.microsoft.com/en-us/documentation/articles/active-directory-identityprotection/?rnd=1> (herein after “Azure Active Directory Identity Protection”)
- Microsoft, *Securing access to Office 365 and other apps connected to Azure Active Directory*, available at <https://web.archive.org/web/20160421011004/https://azure.microsoft.com/en-us/documentation/articles/active-directory-conditional-access/> (herein after “Securing access to Office 365”)
- Microsoft, *Getting started with the Azure AD Reporting API*, available at <https://web.archive.org/web/20160408012325/https://azure.microsoft.com/en-us/documentation/articles/active-directory-reporting-api-getting-started/> (herein after “Azure AD Reporting API”)
- Microsoft, *Azure Active Directory reporting - preview*, available at <https://web.archive.org/web/20161114133555/https://azure.microsoft.com/en-us/documentation/articles/active-directory-reporting-azure-portal/> (herein after “Azure Active Directory reporting”)
- Microsoft, *Authentication Scenarios for Azure AD*, available at <https://web.archive.org/web/20160326203756/https://azure.microsoft.com/en-us/documentation/articles/active-directory-authentication-scenarios/> (herein after “Authentication Scenarios for Azure AD”)
- Microsoft, *Administer your Azure AD directory*, available at <https://web.archive.org/web/20160327030629/https://azure.microsoft.com/en-us/documentation/articles/active-directory-administer/> (herein after “Administer you Azure AD Directory”)
- Microsoft, *Azure Active Directory*, available at [https://learn.microsoft.com/en-us/previous-versions/azure/azure-services/mt168838\(v=azure.100\)](https://learn.microsoft.com/en-us/previous-versions/azure/azure-services/mt168838(v=azure.100)) (herein after “Azure Active Directory”)
- Microsoft, *Azure Active Directory for the Old-School AD Admin*, available at <https://techcommunity.microsoft.com/blog/coreinfrastructureandsecurityblog/azure-active-directory-for-the-old-school-ad-admin/257709> (herein after “Azure Active Directory for the Old-School AD Admin”)

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.

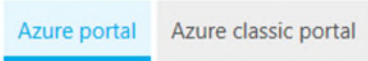
<p>U.S. Pat. No. 12,231,426</p>	<p>Exemplary citations to Azure AD</p>
<p>1 [pre]. A computer system configured to execute software instructions stored on nontransitory machine-readable storage media, wherein the software instructions comprise instructions that:</p>	<p>To the extent the preamble is limiting, under Plaintiff’s contentions, Azure AD 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:</p> <div data-bbox="583 300 1619 917" style="background-color: #333; color: #fff; padding: 10px;"> <h2 style="margin: 0;">Azure Active Directory</h2> <p style="margin: 0;">Azure Active Directory (Azure AD) provides an easy way for businesses to manage identity and access, both in the cloud and on-premises. Your users can use the same work or school account for single sign-on to any cloud and on-premises web application. Your users can use their favorite devices, including iOS, Mac OS X, Android, and Windows. Your organization can protect sensitive data and applications both on-premises and in the cloud with integrated multi-factor authentication ensuring secure local and remote access. Azure AD extends your on-premises directories so that information workers can use a single organizational account to securely and consistently access their corporate resources. Azure AD also offers comprehensive reports, analytics, and self-service capabilities to reduce costs and enhance security. The Azure AD SLA ensures that your business runs smoothly at all times and can be scaled to enterprise levels.</p> </div> <p>Microsoft, <i>Azure Active Directory</i></p>

<p>U.S. Pat. No. 12,231,426</p>	<p>Exemplary citations to Azure AD</p>
	<p>How can I get an Azure AD directory?</p> <p>Azure AD provides the core directory and identity management capabilities behind most of Microsoft's cloud services, including:</p> <ul style="list-style-type: none"> • Azure • Microsoft Office 365 • Microsoft Dynamics CRM Online • Microsoft Intune <p>You will get an Azure AD directory when you sign up for any of these Microsoft cloud services. You can create additional directories as needed. For example, you might maintain your first directory as a production directory and then create another directory for testing or staging.</p> <p>Microsoft, <i>Administer your Azure AD directory</i></p> <p>To the extent that Azure AD 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 Azure AD, 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.</p>
<p>[1a] receive a request to authenticate a client, wherein the request comprises a first identifier and a password,</p>	<p>Under Plaintiff's contentions, Azure AD expressly or inherently discloses "receive a request to authenticate a client, wherein the request comprises a first identifier and a password," as interpreted by Qomplx in its infringement contentions. For example:</p>

Exemplary citations to Azure AD

Security tokens issued by Azure AD contain claims, or assertions of information about the subject that has been authenticated. These claims can be used by the application for various tasks. For example, they can be used to validate the token, identify the subject's directory tenant, display user information, determine the subject's authorization, and so on. The claims present in any given security token are dependent upon the type of token, the type of credential used to authenticate the user, and the application configuration. A brief description of each type of claim emitted by Azure AD is provided in the table below. For more information, refer to [Supported Token and Claim Types](#).

First Name	Provides the given name of the user as set in Azure AD.
Groups	Contains object Ids of Azure AD groups the user is a member of.
Identity Provider	Records the identity provider that authenticated the subject of the token.
Issued At	Records the time at which the token was issued, often used for token freshness.
Issuer	Identifies the STS that emitted the token as well as the Azure AD tenant.
Last Name	Provides the surname of the user as set in Azure AD.
Name	Provides a human readable value that identifies the subject of the token.
Object Id	Contains an immutable, unique identifier of the subject in Azure AD.
Roles	Contains friendly names of Azure AD Application Roles that the user has been granted.
Scope	Indicates the permissions granted to the client application.
Subject	Indicates the principal about which the token asserts information.
Tenant Id	Contains an immutable, unique identifier of the directory tenant that issued the token.
Token Lifetime	Defines the time interval within which a token is valid.

<p>U.S. Pat. No. 12,231,426</p>	<p>Exemplary citations to Azure AD</p>
	<p>Microsoft, <i>Authentication Scenarios for Azure AD</i></p> <hr/> <p>Authentication Method Indicates how the subject of the token was authenticated (password, certificate, etc.).</p> <hr/> <p><i>Id.</i></p> <p>To the extent that Azure AD 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 Azure AD, 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.</p>
<p>[1b] store, in a multidimensional time-series database, information about the request,</p>	<p>Under Plaintiff’s contentions, Azure AD 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:</p>  <p><i>This documentation is part of the Azure Active Directory Reporting Guide.</i></p> <p>With reporting in the Azure Active Directory preview, you get all the information you need to determine how your environment is doing. What’s in the preview?</p> <p>There are two main areas of reporting:</p> <ul style="list-style-type: none"> • Sign-in activities – Information about the usage of managed applications and user sign-in activities • Audit logs - System activity information about users and group management, your managed applications and directory activities <p>Depending on the scope of the data you are looking for, you can access these reports either by clicking Users and groups or Enterprise applications in the services list in the Azure portal.</p> <p>Microsoft, <i>Azure Active Directory reporting</i>.</p>

<p>U.S. Pat. No. 12,231,426</p>	<p>Exemplary citations to Azure AD</p>
	<p>Azure Active Directory provides a variety of activity, security and audit reports. This data can be consumed through the Azure portal, but can also be very useful in a many other applications, such as SIEM systems, audit, and business intelligence tools.</p> <p>The Azure AD Reporting APIs provide programmatic access to these data through a set of REST-based APIs that can be called from a variety programming languages and tools.</p> <p>This article will walk you through the process of calling the Azure AD Reporting APIs using PowerShell. You can modify the sample PowerShell script to access data from any of the available reports in JSON, XML or text format, as your scenario requires.</p> <p>To use this sample, you will need an Azure Active Directory</p> <p>Microsoft, <i>Azure AD Reporting API.</i></p> <p>Security tokens issued by Azure AD contain claims, or assertions of information about the subject that has been authenticated. These claims can be used by the application for various tasks. For example, they can be used to validate the token, identify the subject's directory tenant, display user information, determine the subject's authorization, and so on. The claims present in any given security token are dependent upon the type of token, the type of credential used to authenticate the user, and the application configuration. A brief description of each type of claim emitted by Azure AD is provided in the table below. For more information, refer to Supported Token and Claim Types.</p>

Exemplary citations to Azure AD

Authentication Method	Indicates how the subject of the token was authenticated (password, certificate, etc.).
First Name	Provides the given name of the user as set in Azure AD.
Groups	Contains object Ids of Azure AD groups the user is a member of.
Identity Provider	Records the identity provider that authenticated the subject of the token.
Issued At	Records the time at which the token was issued, often used for token freshness.
Issuer	Identifies the STS that emitted the token as well as the Azure AD tenant.
Last Name	Provides the surname of the user as set in Azure AD.
Name	Provides a human readable value that identifies the subject of the token.
Object Id	Contains an immutable, unique identifier of the subject in Azure AD.
Roles	Contains friendly names of Azure AD Application Roles that the user has been granted.
Scope	Indicates the permissions granted to the client application.
Subject	Indicates the principal about which the token asserts information.
Tenant Id	Contains an immutable, unique identifier of the directory tenant that issued the token.

Authentication Scenarios for Azure AD.

U.S. Pat. No. 12,231,426	Exemplary citations to Azure AD
	To the extent that Azure AD 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 Azure AD, 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 first user account identified by the first identifier	Under Plaintiff's contentions, Azure AD expressly or inherently discloses "determine whether the password corresponds to a first user account identified by the first identifier," as interpreted by Qomplx in its infringement contentions. For example:

Exemplary citations to Azure AD

First Name	Provides the given name of the user as set in Azure AD.
Groups	Contains object Ids of Azure AD groups the user is a member of.
Identity Provider	Records the identity provider that authenticated the subject of the token.
Issued At	Records the time at which the token was issued, often used for token freshness.
Issuer	Identifies the STS that emitted the token as well as the Azure AD tenant.
Last Name	Provides the surname of the user as set in Azure AD.
Name	Provides a human readable value that identifies the subject of the token.
Object Id	Contains an immutable, unique identifier of the subject in Azure AD.
Roles	Contains friendly names of Azure AD Application Roles that the user has been granted.
Scope	Indicates the permissions granted to the client application.
Subject	Indicates the principal about which the token asserts information.
Tenant Id	Contains an immutable, unique identifier of the directory tenant that issued the token.
Token Lifetime	Defines the time interval within which a token is valid.

Microsoft, *Authentication Scenarios for Azure AD*

Authentication Method	Indicates how the subject of the token was authenticated (password, certificate, etc.).
-----------------------	---

Id.

U.S. Pat. No. 12,231,426	Exemplary citations to Azure AD
	<p>To the extent that Azure AD 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 Azure AD, 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.</p>
<p>[1d] determine whether an additional verification is required to grant access,</p>	<p>Under Plaintiff’s contentions, Azure AD expressly or inherently discloses “determine whether an additional verification is required to grant access,” as interpreted by Qomplx in its infringement contentions.</p> <p>For example: <i>See</i> [1e], [1f], 1[g].</p> <p>To the extent that Azure AD 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 Azure AD, 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.</p>
<p>[1e] wherein determining whether the additional verification is required to grant access comprises:</p>	<p>Under Plaintiff’s contentions, Azure AD expressly or inherently discloses “wherein determining whether the additional verification is required to grant access comprises,” as interpreted by Qomplx in its infringement contentions.</p> <p>For example: <i>See</i> [1f], 1[g].</p> <p>To the extent that Azure AD 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 Azure AD, 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.</p>

<p>U.S. Pat. No. 12,231,426</p>	<p>Exemplary citations to Azure AD</p>
<p>[1f] retrieving, from the multidimensional time-series database, historical information about previous access requests associated with the first user account, and</p>	<p>Under Plaintiff’s contentions, Azure AD expressly or inherently discloses “retrieving, from the multidimensional time-series database, historical information about previous access requests associated with the first user account,” as interpreted by Qomplx in its infringement contentions.</p> <p>For example: <i>See</i> [1g]</p> <p>To the extent that Azure AD 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 Azure AD, 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.</p>
<p>[1g] determining, based at least on the historical information, whether the first user account is associated with a previous request to authenticate, wherein the previous request to authenticate comprised a second identifier not associated with the first user account; and,</p>	<p>Under Plaintiff’s contentions, Azure AD expressly or inherently discloses “determining, based at least on the historical information, whether the first user account is associated with a previous request to authenticate, wherein the previous request to authenticate comprised a second identifier not associated with the first user account; and,” as interpreted by Qomplx in its infringement contentions.</p> <p>For example:</p> <p><i>Why conditional access?</i></p> <p>The conditional access control capabilities in Azure Active Directory offers simple ways for companies to secure their resources both in the cloud and on-premises. Whether you need something like "prevent access to my resources using a stolen password" or "require a healthy, managed device for accessing my enterprise content", Azure Active Directory meets your needs.</p> <p><i>How is conditional access control enforced?</i></p> <p>With conditional access control, Azure Active Directory checks the specific conditions you choose when authenticating a user, before allowing access to an application. Once those conditions are met, the user is authenticated and allowed access to the application.</p>

U.S. Pat. No. 12,231,426	Exemplary citations to Azure AD
	<p>Microsoft, <i>Securing access to Office 365</i>.</p> <hr/> <p>Azure Active Directory Identity Protection is a security service that provides a consolidated view into risk events and potential vulnerabilities affecting your organization's identities. Microsoft has been securing cloud-based identities for over a decade, and with Azure AD Identity Protection, Microsoft is making these same protection systems available to enterprise customers. Identity Protection leverages existing Azure AD's anomaly detection capabilities (available through Azure AD's Anomalous Activity Reports), and introduces new risk event types that can detect anomalies in real-time.</p> <p>Microsoft, <i>Azure Active Directory Identity Protection</i>.</p>

U.S. Pat. No. 12,231,426	Exemplary citations to Azure AD																
	<p>Detection and Risk</p> <p>Risk events</p> <p>Risk events are events that were flagged as suspicious by Identity Protection, and indicate that an identity may have been compromised. For a complete list of risk events, see Types of risk events detected by Azure Active Directory Identity Protection.</p> <p>Some of these risk events have been available through the Azure AD Anomalous Activity reports in the Azure Management Portal. The table below lists the various risk event types and the corresponding Azure AD Anomalous Activity report. Microsoft is continuing to invest in this space, and plans to continuously improve the detection accuracy of existing risk events and add new risk event types on an ongoing basis.</p> <table border="1" data-bbox="613 532 1407 1003"> <thead> <tr> <th>Identity Protection Risk Event Type</th> <th>Corresponding Azure AD Anomalous Activity Report</th> </tr> </thead> <tbody> <tr> <td>Leaked credentials</td> <td>Users with leaked credentials</td> </tr> <tr> <td>Impossible travel to atypical locations</td> <td>Irregular sign-in activity</td> </tr> <tr> <td>Sign-ins from infected devices</td> <td>Sign-ins from possibly infected devices</td> </tr> <tr> <td>Sign-ins from anonymous IP addresses</td> <td>Sign-ins from unknown sources</td> </tr> <tr> <td>Sign-ins from IP addresses with suspicious activity</td> <td>Sign-ins from IP addresses with suspicious activity</td> </tr> <tr> <td>Signs in from unfamiliar locations</td> <td>-</td> </tr> <tr> <td>Lockout events (not in public preview)</td> <td>-</td> </tr> </tbody> </table> <p><i>Id.</i></p> <p>To the extent that Azure AD 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 Azure AD, 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.</p>	Identity Protection Risk Event Type	Corresponding Azure AD Anomalous Activity Report	Leaked credentials	Users with leaked credentials	Impossible travel to atypical locations	Irregular sign-in activity	Sign-ins from infected devices	Sign-ins from possibly infected devices	Sign-ins from anonymous IP addresses	Sign-ins from unknown sources	Sign-ins from IP addresses with suspicious activity	Sign-ins from IP addresses with suspicious activity	Signs in from unfamiliar locations	-	Lockout events (not in public preview)	-
Identity Protection Risk Event Type	Corresponding Azure AD Anomalous Activity Report																
Leaked credentials	Users with leaked credentials																
Impossible travel to atypical locations	Irregular sign-in activity																
Sign-ins from infected devices	Sign-ins from possibly infected devices																
Sign-ins from anonymous IP addresses	Sign-ins from unknown sources																
Sign-ins from IP addresses with suspicious activity	Sign-ins from IP addresses with suspicious activity																
Signs in from unfamiliar locations	-																
Lockout events (not in public preview)	-																
[1h] based on the additional verification being required to grant access:	Under Plaintiff’s contentions, Azure AD 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:																

U.S. Pat. No. 12,231,426	Exemplary citations to Azure AD
<p>[1i] select an additional verification method from a plurality of verification methods</p>	<p>Azure Multi-Factor Authentication helps safeguard access to data and applications while meeting user demand for a simple sign-in process. It provides additional security by requiring a second form of authentication and delivers strong authentication via a range of easy verification options:</p> <ul style="list-style-type: none"> • phone call • text message • mobile app notification—allowing users to choose the method they prefer • mobile app verification code • 3rd party OATH tokens <p>For additional information on how it works see the following video.</p> <p>Microsoft, <i>What is Azure Multi-Factor Authentication</i>.</p> <p>To the extent that Azure AD 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 Azure AD, 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.</p>
<p>[1j] cause the client to be prompted to complete the additional verification method, and</p>	<p>Under Plaintiff’s contentions, Azure AD 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:</p>

Methods available for multi-factor authentication

When a user signs in, an additional verification is sent to the user. The following are a list of methods that can be used for this second verification.

Verification Method	Description
Phone Call	A call is placed to a user's smart phone asking them to verify that they are signing in by pressing the # sign. This will complete the verification process. This option is configurable and can be changed to a code that you specify.
Text Message	A text message will be sent to a user's smart phone with a 6 digit code. Enter this code in to complete the verification process.
Mobile App Notification	A verification request will be sent to a user's smart phone asking them complete the verification by selecting Verify from the mobile app. This will occur if you selected app notification as your primary verification method. If they receive this when they are not signing in, they can choose to report it as fraud.
Verification code with Mobile App	A verification code will be sent to the mobile app that is running on a user's smart phone. This will occur if you selected a verification code as your primary verification method.

Microsoft, *What is Azure Multi-Factor Authentication.*

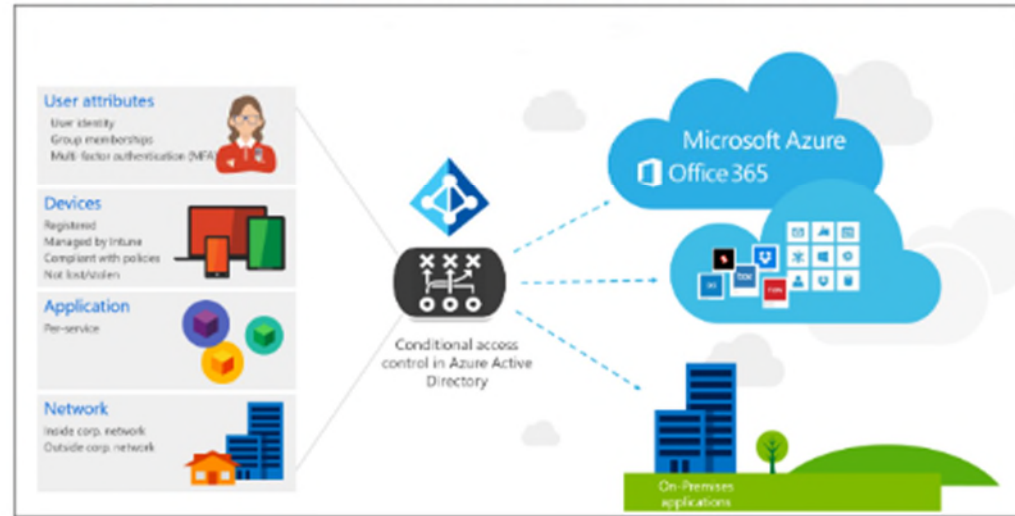
To the extent that Azure AD does not disclose any elements of this claim limitation, it would have been obvious to a person having ordinary skill in the art to combine, with the teachings of Azure AD, those elements, as known to them or as disclosed by other prior art identified herein, in the cover 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, Azure AD expressly or inherently discloses "determine whether the additional verification method has been completed correctly," as interpreted by Qomplx in its infringement contentions. For example:

How is conditional access control enforced?

With conditional access control, Azure Active Directory checks the specific conditions you choose when authenticating a user, before allowing access to an application. Once those conditions are met, the user is authenticated and allowed access to the application.



Microsoft, *Securing access to Office 365*.

To the extent that Azure AD 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 Azure AD, 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.

3. 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, Azure AD 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:

Getting Started

The vast majority of security breaches take place when attackers gain access to an environment by stealing a user's identity. Attackers have become increasingly effective at leveraging third party breaches, and using sophisticated phishing attacks. Once an attacker gains access to even a low privileged user account, it is relatively straightforward for them to gain access to important company resources through lateral movement. It is therefore essential to protect all identities and, when an identity is compromised, proactively prevent the compromised identity from being abused.

Discovering compromised identities is no easy task. Fortunately, Identity Protection can help: Identity Protection uses adaptive machine learning algorithms and heuristics to detect anomalies and risk events that may indicate that an identity has been compromised.

Using this data, Identity Protection generates reports and alerts that enables you to investigate these risk events and take appropriate remediation or mitigation action.

But Azure Active Directory Identity Protection more than a monitoring and reporting tool. Based on risk events, Identity Protection calculates a user risk level for each user, enabling you to configure risk-based policies to automatically protect the identities of your organization. These risk-based policies, in addition to other conditional access controls provided by Azure Active Directory and EMS, can automatically block or offer adaptive remediation actions that include password resets and multi-factor authentication enforcement.

Explore Identity Protection's capabilities

Detecting risk events and risky accounts:

- Detecting 6 risk event types using machine learning and heuristic rules
- Calculating user risk levels
- Providing custom recommendations to improve overall security posture by highlighting vulnerabilities

Microsoft, *Azure Active Directory Identity Protection.*

Detection and Risk

Risk events

Risk events are events that were flagged as suspicious by Identity Protection, and indicate that an identity may have been compromised. For a complete list of risk events, see [Types of risk events detected by Azure Active Directory Identity Protection](#).

Some of these risk events have been available through the Azure AD Anomalous Activity reports in the Azure Management Portal. The table below lists the various risk event types and the corresponding Azure AD Anomalous Activity report. Microsoft is continuing to invest in this space, and plans to continuously improve the detection accuracy of existing risk events and add new risk event types on an ongoing basis.


Identity Protection Risk Event Type	Corresponding Azure AD Anomalous Activity Report
Leaked credentials	Users with leaked credentials
Impossible travel to atypical locations	Irregular sign-in activity
Sign-ins from infected devices	Sign-ins from possibly infected devices
Sign-ins from anonymous IP addresses	Sign-ins from unknown sources
Sign-ins from IP addresses with suspicious activity	Sign-ins from IP addresses with suspicious activity
Signs in from unfamiliar locations	-
Lockout events (not in public preview)	-

The following Azure AD Anomalous Activity reports are not included as risk events in Azure AD Identity Protection, and will therefore not be available through Identity Protection. These reports are still available in the Azure Management Portal however they will be deprecated at some time in the future as they are being superseded by risk events in Identity Protection.

- Sign-ins after multiple failures
- Sign-ins from multiple geographies

Microsoft, *Azure Active Directory Identity Protection*.

To the extent that Azure AD 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 Azure AD, 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.

<p>U.S. Pat. No. 12,231,426</p>	<p>Exemplary citations to Azure AD</p>
<p>[5a] The computer system of claim 1, wherein the software instructions further comprise instructions that:</p> <p>based on the additional verification being required to grant access;</p> <p>determine that a probable cyberattack is detected, and</p>	<p>Under Plaintiff’s contentions, Azure AD expressly or inherently discloses “the 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. For example:</p> <p>Risk level</p> <p>The Risk level for a risk event is an indication (High, Medium, or Low) of the severity of the risk event. The risk level helps Identity Protection users prioritize the actions they must take to reduce the risk to their organization. The severity of the risk event represents the strength of the signal as a predictor of identity compromise, combined with the amount of noise that it typically introduces.</p> <ul style="list-style-type: none"> • High: High confidence and high severity risk event. These events are strong indicators that the user’s identity has been compromised, and any user accounts impacted should be remediated immediately. • Medium: High severity, but lower confidence risk event, or vice versa. These events are potentially risky, and any user accounts impacted should be remediated. • Low: Low confidence and low severity risk event. This event may not require an immediate action, but when combined with other risk events, may provide a strong indication that the identity is compromised.  <p>Microsoft, <i>Azure Active Directory Identity Protection</i>.</p> <p>To the extent that Azure AD 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 Azure AD, 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.</p>
<p>[5b] provide an alert,</p>	<p>Under Plaintiff’s contentions, Azure AD expressly or inherently discloses “provide an alert,” as interpreted by Qomplx in its infringement contentions.</p>

U.S. Pat. No. 12,231,426	Exemplary citations to Azure AD
	<p>For example: <i>See</i> [5c] and [5d]</p> <p>Investigating risk events:</p> <ul style="list-style-type: none">• Sending notifications for risk events• Investigating risk events using relevant and contextual information• Providing basic workflows to track investigations• Providing easy access to remediation actions such as password reset <p>Microsoft, <i>Azure Active Directory Identity Protection</i>.</p>

What is a user risk level?


A user risk level is an indication (High, Medium, or Low) of the likelihood that the user's identity has been compromised. It is calculated based on the user risk events that are associated with the user's identity.

The status of a risk event is either **Active** or **Closed**. Only risk events that are **Active** contribute to the user risk calculation.

The user risk level is calculated using the following inputs:

- Active risk events impacting the user
- Risk level of these events
- Whether any remediation actions have been taken

USER	PRIVILEGED	RISK LEVEL	RISK EVENTS	STATUS	DATE RANGE (UTC)
Nikolai Gogol		Medium	6 risk events	Policy: User passw...	2/26/2016 - 2/27/2016
			6 sign-ins from an...	Active	2/26/2016 - 2/27/2016
Harry Slate		Medium	3 risk events	Policy: User passw...	2/27/2016
			2 impossible trave...	Active	2/27/2016
			1 sign-in from infe...	Active	2/27/2016
Tom Newman		Medium	3 risk events	Policy: User passw...	2/27/2016
			2 impossible trave...	Active	2/27/2016
			1 sign-in from infe...	Active	2/27/2016

<p>U.S. Pat. No. 12,231,426</p>	<p>Exemplary citations to Azure AD</p>
	<p>Microsoft, <i>Azure Active Directory Identity Protection</i>.</p> <p>Investigation</p> <p>Your journey through Identity Protection typically starts with the Identity Protection dashboard.</p> <p> Remediation</p> <p>The dashboard gives you access to:</p> <ul style="list-style-type: none"> • Reports such as Users flagged for risk, Risk events and Vulnerabilities • Settings such as the configuration of your Security Policies, Notifications and multi-factor authentication registration <p>It is typically your starting point for investigation, which is the process of reviewing the activities, logs, and other relevant information related to a risk event to decide whether remediation or mitigation steps are necessary, and how the identity was compromised, and understand how the compromised identity was used.</p> <p>You can tie your investigation activities to the notifications Azure Active Directory Protection sends per email.</p> <p>The following sections provide you with more details and the steps that are related to an investigation.</p> <p>Microsoft, <i>Azure Active Directory Identity Protection</i>.</p> <p>To the extent that Azure AD 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 Azure AD, 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.</p>
<p>[5c] wherein the alert includes the first identifier and an indicator that a probable cyberattack is detected, and</p>	<p>Under Plaintiff’s contentions, Azure AD expressly or inherently discloses “wherein the alert includes the first identifier and an indicator that a probable cyberattack is detected,” as interpreted by Qomplx in its infringement contentions.</p> <p>For example:</p> <p><i>See</i> [5b]</p>

U.S. Pat. No. 12,231,426	Exemplary citations to Azure AD
	To the extent that Azure AD 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 Azure AD, 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.
[5d] wherein the alert is designated to be provided to an administrator of the network	Under Plaintiff’s contentions, Azure AD 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: <i>See</i> [5b] To the extent that Azure AD 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 Azure AD, 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[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, Azure AD 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:

<p>U.S. Pat. No. 12,231,426</p>	<p>Exemplary citations to Azure AD</p>
	<div data-bbox="583 175 1621 792" style="background-color: #333; color: white; padding: 10px;"> <h2 style="margin: 0;">Azure Active Directory</h2> <p style="margin: 0;">Azure Active Directory (Azure AD) provides an easy way for businesses to manage identity and access, both in the cloud and on-premises. Your users can use the same work or school account for single sign-on to any cloud and on-premises web application. Your users can use their favorite devices, including iOS, Mac OS X, Android, and Windows. Your organization can protect sensitive data and applications both on-premises and in the cloud with integrated multi-factor authentication ensuring secure local and remote access. Azure AD extends your on-premises directories so that information workers can use a single organizational account to securely and consistently access their corporate resources. Azure AD also offers comprehensive reports, analytics, and self-service capabilities to reduce costs and enhance security. The Azure AD SLA ensures that your business runs smoothly at all times and can be scaled to enterprise levels.</p> </div> <p>Microsoft, <i>Azure Active Directory</i>.</p> <p>To the extent that Azure AD 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 Azure AD, 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.</p>
<p>[9a] receiving a request to authenticate a client, wherein the request comprises a first identifier and a password,</p>	<p>Under Plaintiff’s contentions, Azure AD expressly or inherently discloses “receiving a request to authenticate a client, wherein the request comprises a first identifier and a password,” as interpreted by Qomplx in its infringement contentions. For example:</p> <p><i>See</i> above at claim [1a].</p> <p>To the extent that Azure AD 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 Azure AD, those elements, as known to them or as disclosed by other prior art identified herein, in the cover pleading, in</p>

U.S. Pat. No. 12,231,426	Exemplary citations to Azure AD
	Microsoft’s other claim charts, and/or in combination with the general knowledge of a person having ordinary skill in the art.
[9b] storing, in a multidimensional time-series database, information about the request,	<p>Under Plaintiff’s contentions, Azure AD 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:</p> <p><i>See</i> above at claim [1b].</p> <p>To the extent that Azure AD 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 Azure AD, 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.</p>
[9c] determining whether the password corresponds to a first user account identified by the first identifier,	<p>Under Plaintiff’s contentions, Azure AD expressly or inherently discloses “determining whether the password corresponds to a first user account identified by the first identifier,” as interpreted by Qomplx in its infringement contentions. For example:</p> <p><i>See</i> above at claim [1c].</p> <p>To the extent that Azure AD 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 Azure AD, 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.</p>
[9d] determining whether an additional verification is required to grant access,	<p>Under Plaintiff’s contentions, Azure AD expressly or inherently discloses “determining whether an additional verification is required to grant access,” as interpreted by Qomplx in its infringement contentions. For example:</p> <p><i>See</i> above at claim [1d].</p> <p>To the extent that Azure AD 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 Azure AD, 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.</p>

U.S. Pat. No. 12,231,426	Exemplary citations to Azure AD
<p>[9e] wherein determining whether the additional verification is required to grant access comprises:</p>	<p>Under Plaintiff’s contentions, Azure AD 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:</p> <p><i>See</i> above at claim [1e].</p> <p>To the extent that Azure AD 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 Azure AD, 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.</p>
<p>[9f] retrieving, from the multidimensional time-series database, historical information about previous access requests associated with the first user account,</p>	<p>Under Plaintiff’s contentions, Azure AD expressly or inherently discloses “retrieving, from the multidimensional time-series database, historical information about previous access requests associated with the first user account,” as interpreted by Qomplx in its infringement contentions. For example:</p> <p><i>See</i> above at claim [1f].</p> <p>To the extent that Azure AD 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 Azure AD, 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.</p>
<p>[9g] determining, based at least on the historical information, whether the first user account is associated with a previous request to authenticate, wherein the previous request to authenticate comprised a second identifier not associated with the first user account; and,</p>	<p>Under Plaintiff’s contentions, Azure AD expressly or inherently discloses “determining, based at least on the historical information, whether the first user account is associated with a previous request to authenticate, wherein the previous request to authenticate comprised a second identifier not associated with the first user account,” as interpreted by Qomplx in its infringement contentions. For example:</p> <p><i>See</i> above at claim [1g].</p> <p>To the extent that Azure AD 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 Azure AD, 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.</p>

U.S. Pat. No. 12,231,426	Exemplary citations to Azure AD
<p>[9h] based on the additional verification being required to grant access:</p>	<p>Under Plaintiff’s contentions, Azure AD expressly or inherently discloses “based on the additional verification being required to grant access,” as interpreted by Qomplx in its infringement contentions. For example:</p> <p><i>See</i> above at claim [1h].</p> <p>To the extent that Azure AD 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 Azure AD, 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.</p>
<p>[9i] selecting an additional verification method from a plurality of verification methods,</p>	<p>Under Plaintiff’s contentions, Azure AD 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:</p> <p><i>See</i> above at claim [1i].</p> <p>To the extent that Azure AD 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 Azure AD, 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.</p>
<p>[9j] causing the client to be prompted to complete the additional verification method, and</p>	<p>Under Plaintiff’s contentions, Azure AD 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:</p> <p><i>See</i> above at claim [1j].</p> <p>To the extent that Azure AD 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 Azure AD, 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.</p>

U.S. Pat. No. 12,231,426	Exemplary citations to Azure AD
<p>[9k] determining whether the additional verification method has been completed correctly.</p>	<p>Under Plaintiff’s contentions, Azure AD expressly or inherently discloses “determining whether the additional verification method has been completed correctly,” as interpreted by Qomplx in its infringement contentions. For example:</p> <p><i>See</i> above at claim [1k].</p> <p>To the extent that Azure AD 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 Azure AD, 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.</p>
<p>11. The method of claim 9, wherein determining whether the additional verification is required to grant access further comprises processing an external threat intelligence feed.</p>	<p>Under Plaintiff’s contentions, Azure AD expressly or inherently discloses “[t]he method of claim 9, 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:</p> <p><i>See</i> above at claim 3.</p> <p>To the extent that Azure AD 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 Azure AD, 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.</p>
<p>[13a] The method of claim 9, further comprising: based on the additional verification being required to grant access: determining that a probable cyberattack is detected, and</p>	<p>Under Plaintiff’s contentions, Azure AD expressly or inherently discloses “the method of claim 9, 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.</p> <p>For example:</p> <p><i>See</i> above at claim [5a].</p> <p>To the extent that Azure AD 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 Azure AD, 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.</p>

U.S. Pat. No. 12,231,426	Exemplary citations to Azure AD
[13b] delivering an alert,	<p>Under Plaintiff’s contentions, Azure AD expressly or inherently discloses “delivering an alert,” as interpreted by Qomplx in its infringement contentions. For example:</p> <p><i>See</i> above at claim [5b].</p> <p>To the extent that Azure AD 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 Azure AD, 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.</p>
[13c] wherein the alert includes the first identifier and an indicator that a probable cyberattack is detected, and	<p>Under Plaintiff’s contentions, Azure AD expressly or inherently discloses “wherein the alert includes the first identifier and an indicator that a probable cyberattack is detected,” as interpreted by Qomplx in its infringement contentions. For example:</p> <p><i>See</i> above at claim [5c].</p> <p>To the extent that Azure AD 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 Azure AD, 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.</p>
[13d] wherein the alert is designated to be delivered to an administrator of the network.	<p>Under Plaintiff’s contentions, Azure AD 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:</p> <p><i>See</i> above at claim [5d].</p> <p>To the extent that Azure AD 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 Azure AD, 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.</p>