MICROSOFT EXHIBIT 1041
Microsoft v. Qomplx
IPR2026-00183

EXHIBIT C
U.S. Patent No. 12,231,426

As used herein and with respect to the ’426 Patent, the term “Accused ’426 Products” means:

(a) Microsoft products that incorporate, rely upon, interact with, or otherwise utilize Microsoft Entra ID (“Entra ID”), including at least the Microsoft Entra product family;

(b) Any other systems, services, or products that utilize the libraries, applications, scripts, packages, or other modules that implement the functionality described below in a manner not materially different with respect to the claims charted below;

(c) any other products that infringe the asserted claims for analogous reasons to those described below; and,

(d) Microsoft products that practice one of more claims of the ’426 Patent.

This claim chart for the ’426 Patent covers all Accused ’426 Products. The theory of infringement described below in connection with the Asserted Claims is analogous to the theory of infringement for all the Accused ’426 Products.

I. Claim 1

A computer system configured to execute software instructions stored on nontransitory machine-readable storage media, wherein the software instructions comprise instructions that:	The '426 Accused Products include a computer system configured to execute software instructions stored on nontransitory machine-readable storage media. For example, Entra ID is a "cloud-based identity and access management service," which includes features to enforce and implement multifactor authentication such as Entra ID Protection:[1] **Microsoft Entra ID** Microsoft Entra ID is the foundational product of Microsoft Entra. It's a cloud-based identity and access management service that provides the essential identity, authentication, policy, and protection to secure users, devices, apps, and resources. Every new Microsoft Entra directory includes an initial domain name, like `contoso.onmicrosoft.com`. You can also add your organization's domain names. **Microsoft 365, Azure, or Dynamics CRM Online subscribers** already use Microsoft Entra ID as every Microsoft 365, Office 365, Azure, and Dynamics CRM Online tenant is automatically a Microsoft Entra tenant. You can immediately start managing access to your integrated cloud apps.
receive a request to authenticate a client, wherein	The software instructions of the '426 Accused Products receive a request to authenticate a client, wherein the request comprises a first identifier and a password.

[1] Microsoft, *What is Microsoft Entra?*, available at `https://learn.microsoft.com/en-us/entra/fundamentals/whatis` [hereinafter *What is Microsoft Entra?*].

the request comprises a first identifier and a password,	For example, Entra ID supports various forms of identifiers for users, including email addresses, bank account numbers, and IP addresses:[2] **Identity** A digital identity is a collection of unique identifiers or attributes that represent a person, software component, machine, asset, or resource in a system. An identifier can be: • An email address • Sign-in credentials (username/password) • A bank account number • A government issued ID • A MAC address or IP address As another example, Entra ID also receives and manages passwords on behalf of users and applications:[3]

[2] Microsoft, *Identity and access management fundamental concepts*, available at `https://learn.microsoft.com/en-us/entra/fundamentals/identity-fundamental-concepts` [hereinafter *Identity Fundamentals*].

[3] Microsoft, *How it works: Microsoft Entra self-service password reset*, available at `https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-howitworks` [hereinafter *Entra Password Reset*].

	Microsoft Entra self-service password reset (SSPR) gives users the ability to change or reset their password, with no administrator or help desk involvement. If a user's account is locked or they forget their password, they can follow prompts to unblock themselves and get back to work. This ability reduces help desk calls and loss of productivity when a user can't sign in to their device or an application. We recommend this video on how to enable and configure SSPR in Microsoft Entra ID. Based on Qomplx's analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.
store, in a multidimensional time-series database, information about the request, determine whether the password corresponds to a first user account identified by the first identifier,	The software instructions of the '426 Accused Products store, in a multidimensional time-series database, information about the request, and determine whether the password corresponds to a first user account identified by the first identifier. For example, Entra ID stores historical data about correct and incorrect password use, among other data, to determine risk profiles for the future.[4] Microsoft's current cloud-based systems rely on several platforms that store and manage multiple dimensions of time-series data. For example, modern versions of Microsoft Fabric, Azure Data Explorer, Azure Monitor, Microsoft Sentinel use the Kusto platform, described as "a powerful tool for exploring your data and discovering patterns, identifying anomalies and outliers, creating statistical

[4] Microsoft, *What are risk detections?*, available at `https://learn.microsoft.com/en-us/entra/id-protection/concept-identity-protection-risks` [hereinafter *What are risk detections?*].

	modeling, and more.[5] Microsoft's documentation explains that "KQL is optimal for querying telemetry, metrics, and logs with deep support for text search and parsing, time-series operators and functions, analytics and aggregation, geospatial, vector similarity searches, and many other language constructs that provide the most optimal language for data analysis":[6] KQL is a simple yet powerful language to query structured, semi-structured, and unstructured data. The language is expressive, easy to read and understand the query intent, and optimized for authoring experiences. KQL is optimal for querying telemetry, metrics, and logs with deep support for text search and parsing, time-series operators and functions, analytics and aggregation, geospatial, vector similarity searches, and many other language constructs that provide the most optimal language for data analysis. The query uses schema entities that are organized in a hierarchy similar to SQLs: databases, tables, and columns. On information about belief, Microsoft's use of a multi-dimensional time-series database significantly improves the bandwidth and latency of both storing and querying past user behavior, resulting in faster login times and the use of a larger volume of data than could be consulted in prior art systems.

[5] Microsoft, *Kusto Query Language overview*, available at `https://learn.microsoft.com/en-us/kusto/query/` [hereinafter *KQL Overview*].

[6] *Id*.

	Further, Entra ID "verifies identities, validates access conditions, checks permissions, . . . and monitors for compromise."[7] It also performs authentication,[8] including via passwords.[9] Based on Qomplx's analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.
determine whether an additional verification is required to grant access, wherein determining whether the additional verification is required to grant access comprises: retrieving, from the multidimensional time-series database, historical information about previous	The software instructions of the '426 Accused Products that determine whether an additional verification is required to grant access, wherein determining whether the additional verification is required to grant access comprises retrieving, from the multidimensional time-series database, historical information about previous access requests associated with the first user account, and 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. For example, Entra ID's Conditional Access uses data about the real-time and offline behavior of users to determine whether an access request is suspicious and thus whether to trigger MFA:[10]

[7] *What is Microsoft Entra?*.

[8] *Id*.

[9] Microsoft, *Reset a user's password*, available at `https://learn.microsoft.com/en-us/entra/fundamentals/users-reset-password-azure-portal` [hereinafter *Reset Password*].

[10] Microsoft, *Tutorial: Use risk detections for user sign-ins to trigger Microsoft Entra multifactor authentication or password changes*, available at `https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-risk-based-sspr-mfa` [hereinafter *Entra Risk Detections*].

access requests associated with the first user account, and 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,	To protect your users, you can configure risk-based Microsoft Entra Conditional Access policies that automatically respond to risky behaviors. These policies can automatically block a sign-in attempt or require extra action, such as require a secure password change or prompting for Microsoft Entra multifactor authentication. These policies work with existing Microsoft Entra Conditional Access policies as an extra layer of protection for your organization. Users might never trigger a risky behavior in one of these policies, but your organization is protected if an attempt to compromise your security is made. Entra ID's understanding of user behavior is based at least on historical information about previous access requests. For example, as explained in Microsoft's documentation:[11]

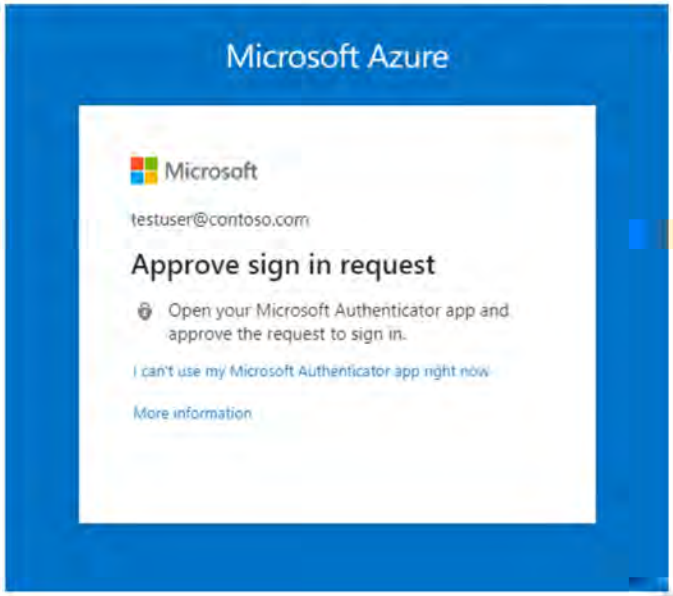
[11] Microsoft, *What is Microsoft Entra ID Protection?*, available at `https://learn.microsoft.com/en-us/entra/id-protection/overview-identity-protection` [hereinafter *What is Microsoft Entra ID Protection?*].

	Microsoft continually adds and updates detections in our catalog to protect organizations. These detections come from our learnings based on the analysis of trillions of signals each day from Active Directory, Microsoft Accounts, and in gaming with Xbox. This broad range of signals helps ID Protection detect risky behaviors like: • Anonymous IP address usage • Password spray attacks • Leaked credentials • and more... During each sign-in, ID Protection runs all real-time sign-in detections, generating a sign-in session risk level that indicates how likely the sign-in is compromised. Based on this risk level, policies are applied to protect the user and the organization. Session risk level can be based on, among other relevant factors, "a token played from an unfamiliar location," "user activity that is unusual for the user or consistent with known attack patterns," a "SAML token issuer for the associated SAML token [being] potentially compromised," "properties that are unfamiliar for the user," and "leaked credentials."[12] Based on Qomplx's analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.
based on the additional verification being required to grant access:	Based on the additional verification being required to grant access, the software instructions of the '426 Accused Products select an additional verification method from a plurality of verification methods.

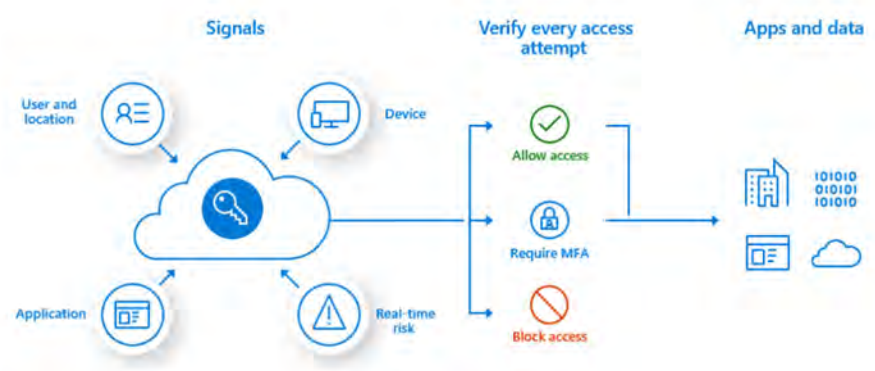
[12] *What are risk detections?*.

select an additional verification method from a plurality of verification methods,	For example, Entra ID supports multiple additional verification methods, including, but not limited to, Microsoft Authenticator, Windows Hello for Business, and voice calls:[13] The following additional forms of verification can be used with Microsoft Entra multifactor authentication: • Microsoft Authenticator • Authenticator Lite (in Outlook) • Windows Hello for Business • Passkey (FIDO2) • Passkey in Microsoft Authenticator • QR code • Certificate-based authentication (when configured for multifactor authentication) • External authentication methods (preview) • Temporary Access Pass (TAP) • OATH hardware token (preview) • OATH software token • SMS • Voice call Based on Qomplx's analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.
cause the client to be prompted to complete the	The software instructions of the '426 Accused Products cause the client to be prompted to complete the additional verification method.

[13] Microsoft, *How it works: Microsoft Entra multifactor authentication*, available at `https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mfa-howitworks` [hereinafter *Microsoft Entra Multifactor Authentication*].

additional verification method, and	For example, many of the additional verification methods supported by Entra ID cause the client to be prompted to complete verification, as shown in the following screenshot informing a user to complete verification using Microsoft Authenticator:[14] 5. Close the browser window, and sign in to the Microsoft Entra admin center again to test the authentication method that you configured. For example, if you configured a mobile app for authentication, you should see a prompt like the following.  Based on Qomplx's analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents.

[14] Microsoft, *Tutorial: Secure user sign-in events with Microsoft Entra multifactor authentication*, available at `https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-azure-mfa` [hereinafter *Secure User Sign-in*].

	For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.
determine whether the additional verification method has been completed correctly.	The software instructions of the '426 Accused Products determine whether the additional verification method has been completed correctly. For example, Microsoft documentation explains that Entra ID implements the entire MFA process for natively supported methods, meaning that Entra ID determines whether the additional verification method has been completed correctly, allowing Entra ID to determine whether to allow access, require further authentication, or block access:[15]  Based on Qomplx's analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.

[15] *Microsoft Entra Multifactor Authentication.*

II. Claim 3

The computer system of claim 1, wherein	See above for an analysis of Claim 1.
determining whether the additional verification is required to grant access further comprises processing an external threat intelligence feed.	Determining whether the additional verification is required of Claim 1 further comprises processing an external threat intelligence feed. For example, Microsoft Entra threat intelligence, which is "based on Microsoft's internal and external threat intelligence sources," "indicates user activity that is unusual for the user":[16] **Microsoft Entra threat intelligence (sign-in)** Microsoft Entra threat intelligence indicates user activity that is unusual for the user or consistent with known attack patterns. This detection is based on Microsoft's internal and external threat intelligence sources. These detections show up as "Microsoft Entra threat intelligence" in logs and ID Protection reports. As another example, Entra ID detects leaked credentials which have been "post[ed] publicly on the dark web, paste sites, or by trading and selling the credentials on the black market":[17]

[16] *What are risk detections?*.

[17] *Id*.

	Leaked credentials This risk detection type indicates that the user's valid credentials leaked. When cybercriminals compromise valid passwords of legitimate users, they often share these gathered credentials. This sharing is typically done by posting publicly on the dark web, paste sites, or by trading and selling the credentials on the black market. When the Microsoft leaked credentials service acquires user credentials from the dark web, paste sites, or other sources, they're checked against Microsoft Entra users' current valid credentials to find valid matches. For more information about leaked credentials, see FAQs. Based on Qomplx's analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.

III. Claim 5

The computer system of claim 1,	See above for an analysis 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, and	The software instructions of Claim 1 further comprise instructions that, based on the additional verification being requested to grant access, determine that a probable cyberattack is detected. For example, Microsoft Entra ID "detect[s] account[s] at risk":[18] **Users at risk detected email** In response to a detected account at risk, Microsoft Entra ID Protection generates an email alert with **Users at risk detected** as subject. The email includes a link to the Users flagged for risk report. As a best practice, you should immediately investigate the users at risk. Microsoft's documentation explains that "[a]s a best practice, you should immediately investigate the users at risk."[19] Based on Qomplx's analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents.

[18] Microsoft, *Microsoft Entra ID Protection notifications*, available at `https://learn.microsoft.com/en-us/entra/id-protection/howto-identity-protection-configure-notifications` [hereinafter *Protection Notifications*].

[19] *Id.*

	For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.
provide an alert, wherein the alert includes the first identifier and an indicator that a probable cyberattack is detected, and wherein the alert is designated to be provided to an administrator of the network.	The software instructions of Claim 1 further comprise instructions that provide an alert, wherein the alert includes the first identifier and an indicator that a probable cyberattack is detected, and wherein the alert is designated to be delivered to an administrator of the network. For example, Microsoft Entra generates "an email alert with Users at risk detected as subject":[20] **Users at risk detected email** In response to a detected account at risk, Microsoft Entra ID Protection generates an email alert with **Users at risk detected** as subject. The email includes a link to the Users flagged for risk report. As a best practice, you should immediately investigate the users at risk. The alert is designated to be delivered to an administrator of the network. For example, the administrator can "specify at what user risk level" the administrator "want[s] the alert to be generated."[21] Based on Qomplx's analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.

[20] *Id.*

[21] *Id.*

IV. Claim 9

A method implemented on a computer system connected to a network, the method comprising:	The '426 Accused Products perform a method implemented on a computer system connected to a network. For example, Entra ID is a "cloud-based identity and access management service," which includes features to enforce and implement multifactor authentication such as Entra ID Protection:[22] **Microsoft Entra ID** Microsoft Entra ID is the foundational product of Microsoft Entra. It's a cloud-based identity and access management service that provides the essential identity, authentication, policy, and protection to secure users, devices, apps, and resources. Every new Microsoft Entra directory includes an initial domain name, like `contoso.onmicrosoft.com`. You can also add your organization's domain names. **Microsoft 365, Azure, or Dynamics CRM Online subscribers** already use Microsoft Entra ID as every Microsoft 365, Office 365, Azure, and Dynamics CRM Online tenant is automatically a Microsoft Entra tenant. You can immediately start managing access to your integrated cloud apps.
receiving a request to authenticate a client, wherein the request comprises a first identifier and a password,	The '426 Accused Products receive a request to authenticate a client, wherein the request comprises a first identifier and a password. For example, Entra ID supports various forms of identifiers for users, including email addresses, bank account numbers, and IP addresses:[23]

[22] *What is Microsoft Entra?*.

[23] *Identity Fundamentals*.

	Identity A digital identity is a collection of unique identifiers or attributes that represent a person, software component, machine, asset, or resource in a system. An identifier can be: • An email address • Sign-in credentials (username/password) • A bank account number • A government issued ID • A MAC address or IP address As another example, Entra ID also receives and manages passwords on behalf of users and applications:[24] Microsoft Entra self-service password reset (SSPR) gives users the ability to change or reset their password, with no administrator or help desk involvement. If a user's account is locked or they forget their password, they can follow prompts to unblock themselves and get back to work. This ability reduces help desk calls and loss of productivity when a user can't sign in to their device or an application. We recommend this video on how to enable and configure SSPR in Microsoft Entra ID. Based on Qomplx's analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be

[24] *Entra Password Reset*.

	insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.
storing, in a multidimensional time-series database, information about the request, determining whether the password corresponds to a first user account identified by the first identifier,	The ’426 Accused Products perform a method comprising storing, in a multidimensional time-series database, information about the request, and determining whether the password corresponds to a first user account identified by the first identifier. For example, Entra ID stores historical data about correct and incorrect password use, among other data, to determine risk profiles for the future.[25] Microsoft’s current cloud-based systems rely on several platforms that store and manage multiple dimensions of time-series data. For example, modern versions of Microsoft Fabric, Azure Data Explorer, Azure Monitor, Microsoft Sentinel use the Kusto platform, described as “a powerful tool for exploring your data and discovering patterns, identifying anomalies and outliers, creating statistical modeling, and more.[26] Microsoft’s documentation explains that “KQL is optimal for querying telemetry, metrics, and logs with deep support for text search and parsing, time-series operators and functions, analytics and aggregation, geospatial, vector similarity searches, and many other language constructs that provide the most optimal language for data analysis”:[27]

[25] *What are risk detections?*.

[26] *KQL Overview*.

[27] *Id*.

	KQL is a simple yet powerful language to query structured, semi-structured, and unstructured data. The language is expressive, easy to read and understand the query intent, and optimized for authoring experiences. KQL is optimal for querying telemetry, metrics, and logs with deep support for text search and parsing, time-series operators and functions, analytics and aggregation, geospatial, vector similarity searches, and many other language constructs that provide the most optimal language for data analysis. The query uses schema entities that are organized in a hierarchy similar to SQLs: databases, tables, and columns. On information about belief, Microsoft's use of a multi-dimensional time-series database significantly improves the bandwidth and latency of both storing and querying past user behavior, resulting in faster login times and the use of a larger volume of data than could be consulted in prior art systems. Further, Entra ID "verifies identities, validates access conditions, checks permissions, . . . and monitors for compromise."[28] It also performs authentication,[29] including via passwords.[30] Based on Qomplx's analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.

[28] *What is Microsoft Entra?*.

[29] *Id*.

[30] *Reset Password*.

determining whether an additional verification is required to grant access, wherein determining whether the additional verification is required to grant access comprises: retrieving, from the multidimensional time-series database, historical information about previous access requests associated with the first user account, 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,	The '426 Accused Products determine whether an additional verification is required to grant access, wherein determining whether the additional verification is required to grant access comprises retrieving, from the multidimensional time-series database, historical information about previous access requests associated with the first user account, and 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. For example, Entra ID's Conditional Access uses data about the real-time and offline behavior of users to determine whether an access request is suspicious and thus whether to trigger MFA:[31] To protect your users, you can configure risk-based Microsoft Entra Conditional Access policies that automatically respond to risky behaviors. These policies can automatically block a sign-in attempt or require extra action, such as require a secure password change or prompting for Microsoft Entra multifactor authentication. These policies work with existing Microsoft Entra Conditional Access policies as an extra layer of protection for your organization. Users might never trigger a risky behavior in one of these policies, but your organization is protected if an attempt to compromise your security is made. Entra ID's understanding of user behavior is based at least on historical information about previous access requests. For example, as explained in Microsoft's documentation:[32]

[31] *Entra Risk Detections*.

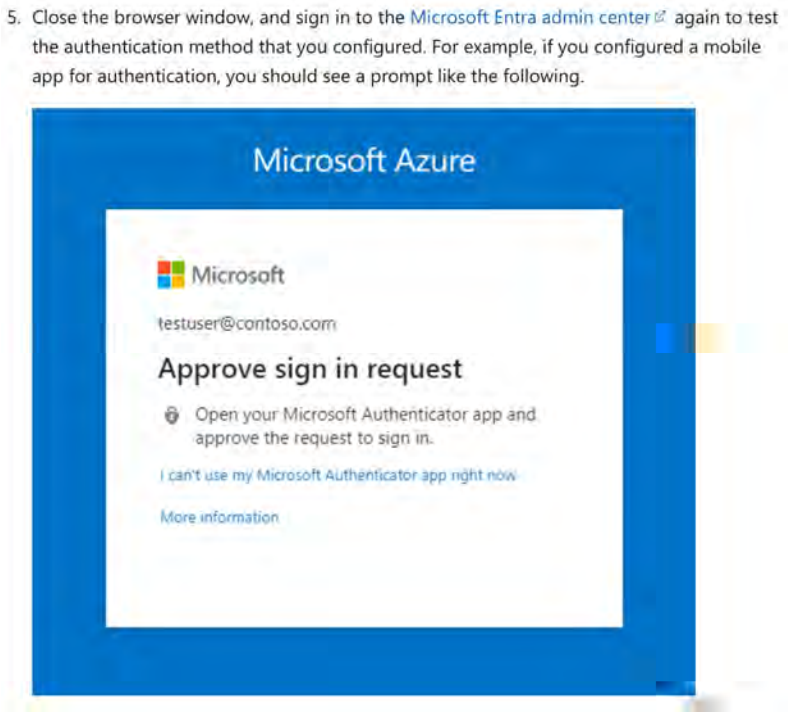
[32] *What is Microsoft Entra ID Protection?*.

	Microsoft continually adds and updates detections in our catalog to protect organizations. These detections come from our learnings based on the analysis of trillions of signals each day from Active Directory, Microsoft Accounts, and in gaming with Xbox. This broad range of signals helps ID Protection detect risky behaviors like: • Anonymous IP address usage • Password spray attacks • Leaked credentials • and more... During each sign-in, ID Protection runs all real-time sign-in detections, generating a sign-in session risk level that indicates how likely the sign-in is compromised. Based on this risk level, policies are applied to protect the user and the organization. Session risk level can be based on, among other relevant factors, "a token played from an unfamiliar location," "user activity that is unusual for the user or consistent with known attack patterns," a "SAML token issuer for the associated SAML token [being] potentially compromised," "properties that are unfamiliar for the user," and "leaked credentials."[33] Based on Qomplx's analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.
based on the additional verification being required to grant access:	Based on the additional verification being required to grant access, the '426 Accused Products select an additional verification method from a plurality of verification methods.

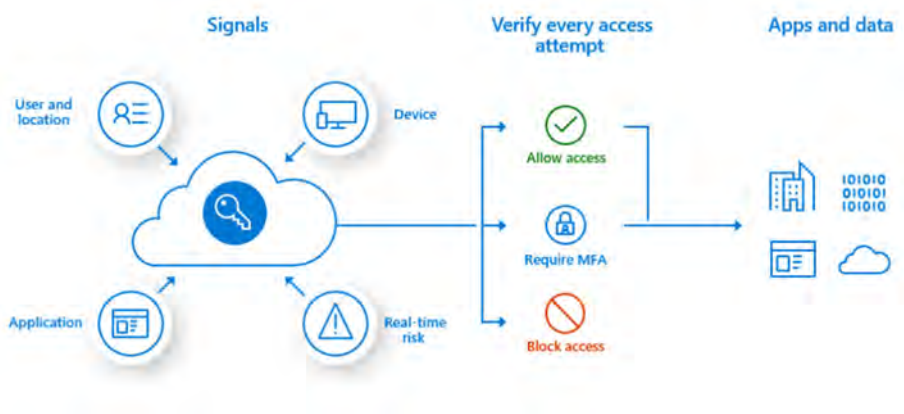
[33] *What are risk detections?*.

selecting an additional verification method from a plurality of verification methods,	For example, Entra ID supports multiple additional verification methods, including, but not limited to, Microsoft Authenticator, Windows Hello for Business, and voice calls:[34] The following additional forms of verification can be used with Microsoft Entra multifactor authentication: • Microsoft Authenticator • Authenticator Lite (in Outlook) • Windows Hello for Business • Passkey (FIDO2) • Passkey in Microsoft Authenticator • QR code • Certificate-based authentication (when configured for multifactor authentication) • External authentication methods (preview) • Temporary Access Pass (TAP) • OATH hardware token (preview) • OATH software token • SMS • Voice call Based on Qomplx’s analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.
causing the client to be prompted to complete the	The ’426 Accused Products perform a method comprising causing the client to be prompted to complete the additional verification method.

[34] *Microsoft Entra Multifactor Authentication.*

additional verification method, and	For example, many of the additional verification methods supported by Entra ID cause the client to be prompted to complete verification, as shown in the following screenshot informing a user to complete verification using Microsoft Authenticator:[35]  Based on Qomplx's analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents.

[35] *Secure User Sign-in.*

	For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.
determining whether the additional verification method has been completed correctly.	The '426 Accused Products determine whether the additional verification method has been completed correctly. For example, Microsoft documentation explains that Entra ID implements the entire MFA process for natively supported methods, meaning that Entra ID determines whether the additional verification method has been completed correctly, allowing Entra ID to determine whether to allow access, require further authentication, or block access:[36]  Based on Qomplx's analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.

[36] *Microsoft Entra Multifactor Authentication.*

V. Claim 11

The method of claim 9, wherein	See above for an analysis of Claim 9.
determining whether the additional verification is required to grant access further comprises processing an external threat intelligence feed.	Determining whether the additional verification is required of Claim 9 further comprises processing an external threat intelligence feed. For example, Microsoft Entra threat intelligence, which is "based on Microsoft's internal and external threat intelligence sources," "indicates user activity that is unusual for the user":[37] **Microsoft Entra threat intelligence (sign-in)** Microsoft Entra threat intelligence indicates user activity that is unusual for the user or consistent with known attack patterns. This detection is based on Microsoft's internal and external threat intelligence sources. These detections show up as "Microsoft Entra threat intelligence" in logs and ID Protection reports. As another example, Entra ID detects leaked credentials which have been "post[ed] publicly on the dark web, paste sites, or by trading and selling the credentials on the black market":[38]

[37] *What are risk detections?*.

[38] *Id*.

	Leaked credentials This risk detection type indicates that the user's valid credentials leaked. When cybercriminals compromise valid passwords of legitimate users, they often share these gathered credentials. This sharing is typically done by posting publicly on the dark web, paste sites, or by trading and selling the credentials on the black market. When the Microsoft leaked credentials service acquires user credentials from the dark web, paste sites, or other sources, they're checked against Microsoft Entra users' current valid credentials to find valid matches. For more information about leaked credentials, see FAQs. Based on Qomplx's analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.

VI. Claim 13

The method of claim 9, further comprising:	See above for an analysis of Claim 9.
based on the additional verification being required to grant access: determining that a probable cyberattack is detected, and	Based on the additional verification being required to grant access, Microsoft Entra determines that a probable cyberattack is detected. For example, Microsoft Entra ID "detect[s] account[s] at risk":[39] **Users at risk detected email** In response to a detected account at risk, Microsoft Entra ID Protection generates an email alert with **Users at risk detected** as subject. The email includes a link to the Users flagged for risk report. As a best practice, you should immediately investigate the users at risk. Microsoft's documentation explains that "[a]s a best practice, you should immediately investigate the users at risk."[40] Based on Qomplx's analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.

[39] *Protection Notifications*.

[40] *Id*.

delivering an alert, wherein the alert includes the first identifier and an indicator that a probable cyberattack is detected, and wherein the alert is designated to be delivered to an administrator of the network.	Microsoft Entra delivers an alert, wherein the alert includes the first identifier and an indicator that a probable cyberattack is detected, and wherein the alert is designated to be delivered to an administrator of the network. For example, Microsoft Entra generates "an email alert with Users at risk detected as subject":[41] **Users at risk detected email** In response to a detected account at risk, Microsoft Entra ID Protection generates an email alert with **Users at risk detected** as subject. The email includes a link to the Users flagged for risk report. As a best practice, you should immediately investigate the users at risk. The alert is designated to be delivered to an administrator of the network. For example, the administrator can "specify at what user risk level" the administrator "want[s] the alert to be generated."[42] Based on Qomplx's analysis to date, this element appears to be practiced literally, including as charted above. Any differences between the charted material and this claim element are expected to be insubstantial, in which case the element is expected to be practiced under the Doctrine of Equivalents. For example, the technology described above performs substantially the same function in substantially the same way to achieve substantially the same result as this claim element.

[41] *Id.*

[42] *Id.*