

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

MICROSOFT CORPORATION,  
Petitioner,

v.

QOMPLX LLC,  
Patent Owner.

IPR2026-00184  
Patent: USP 12,231,426  
Issued: February 18, 2025  
Application No. 18/885,510  
Filed: September 13, 2024

Title: CONTEXTUAL AND RISK-BASED  
MULTI-FACTOR AUTHENTICATION

---

**PETITION FOR**  
**INTER PARTES REVIEW OF U.S. PATENT NO. 12,231,426**

**TABLE OF CONTENTS**

|   | Page |
|---|------|
| LIST OF EXHIBITS .....  | v    |
| MANDATORY NOTICES UNDER 37 C.F.R. § 42.8 .....  | ix   |
| 1. Real Party-In-Interest.....  | ix   |
| 2. Related Matters .....  | ix   |
| 3. Lead And Back-Up Counsel, And Service Information.....   | ix   |
| I. INTRODUCTION .....   | 1    |
| II. GROUNDS FOR STANDING PER 37 C.F.R. § 42.104(A).....   | 2    |
| III. IDENTIFICATION OF CHALLENGE .....  | 3    |
| A. Statement Of The Precise Relief Requested / Statutory Grounds.....   | 3    |
| IV. LEVEL OF SKILL IN THE ART, AND STATE OF THE ART .....   | 3    |
| A. Person Of Ordinary Skill In The Art.....   | 3    |
| B. State Of The Art .....   | 4    |
| 1. Authentication With Username And<br>Password Was Long-Known And Regularly Used .....                           | 4    |
| 2. Additional (i.e., Multi-Factor) Authentication<br>Was Known And Regularly Used For Added Security .....        | 7    |
| 3. It Was Well Known To Implement Systems To Detect<br>Anomalous Log-In Attempts, E.g., Brute Force Attacks ..... | 9    |
| V. THE '426 PATENT.....   | 10   |
| A. The Claims' Earliest Effective Filing Date Is October 19, 2017.....  | 11   |
| B. The '426 Patent's Specification .....  | 11   |
| C. The Prosecution History.....   | 14   |

- VI. CLAIM CONSTRUCTION .....15
- VII. GROUNDS 1-2: CLAIMS 1-21, 23-28, AND 30 ARE OBVIOUS OVER KIRTI (EX1004) ALONE OR COMBINED WITH COFFIN (EX1005)....15
  - A. Kirti (EX1004) .....16
  - B. Coffin (EX1005).....18
  - C. Combining Kirti And Coffin.....20
    - 1. Claim 1 .....24
      - a) Element [1.1] .....24
      - b) Elements [1.2], [1.4] .....25
      - c) Element [1.3] .....30
      - d) Element [1.5] .....34
      - e) Elements [1.6]-[1.7].....38
      - f) Element [1.8]-[1.11] .....49
    - 2. Claim 2 .....54
    - 3. Claim 3 .....56
    - 4. Claim 4 .....57
    - 5. Claim 5 .....58
    - 6. Claim 6 .....64
    - 7. Claim 7 .....66
    - 8. Claim 8 .....68
    - 9. Claims 9-16 .....71
    - 10. Claims 17-18 .....71
    - 11. Claims 19-21 And 23-25 .....71

12. Claims 26-28 And 30 .....72

VIII. NO OBJECTIVE INDICIA OF NON-OBVIOUSNESS.....72

IX. CONCLUSION .....72

CERTIFICATE OF COMPLIANCE.....73

CERTIFICATE OF SERVICE .....74

**TABLE OF AUTHORITIES**

Page

**Cases**

*KEYnetik, Inc. v. Samsung Elecs. Co., LTD.*,  
No. 2022-1127, 2023 WL 2003932 (Fed. Cir. Feb. 15, 2023).....22

*VidStream LLC v. Twitter, Inc.*,  
981 F.3d 1060 (Fed. Cir. 2020).....19

**Board Decisions**

*Nearmap US, Inc. v. Eagle View Tech., Inc.*,  
IPR2022-01009 Paper 28 at 31 (PTAB Dec. 14, 2023).....18

**Statutes**

35 U.S.C. § 103 .....3

**Rules**

37 C.F.R. § 42.24 .....73

37 C.F.R. § 42.6 .....74

**LIST OF EXHIBITS**

| <b>No.</b> | <b>Description</b>  |
|------------|---|
| 1001       | U.S. Patent No. 12,231,426 (“ <b>426 patent</b> ”)  |
| 1002       | File History of U.S. Patent No. 12,231,426  |
| 1003       | Declaration of Dr. John Black, dated December 29, 2025  |
| 1004       | U.S. Patent No. 10,063,654 (“Kirti”)  |
| 1005       | David Coffin, <i>Expert Oracle and Java Security: Programming Secure Oracle Database Applications with Java</i> , Apress (2011) (“Coffin”)                |
| 1006       | U.S. Patent No. 8,572,391 (“Golan”)   |
| 1007       | U.S. Patent No. 7,979,899 (“Guo”)   |
| 1008       | International Publication No. WO 2015/109947 (“Zhang”)  |
| 1009       | U.S. Patent No. 8,312,540 (“Kahn”)  |
| 1010       | U.S. Patent No. 10,021,108 (“Mankovskii”)   |
| 1011       | U.S. Patent No. 7,908,645 (“Varghese”)  |
| 1012       | U.S. Patent Application Pub. No. 2007/0079135 (“Saito”)   |
| 1013       | N/A   |
| 1014       | U.S. Patent No. 9,237,143 (“Dotan”)   |
| 1015       | U.S. Patent No. 9,148,424 (“Yang”)  |
| 1016       | U.S. Patent No. 9,319,419 (“Sprague”)   |
| 1017       | U.S. Patent Application Pub. No. 2008/0249947 (“Potter”)  |
| 1018       | International Pub. No. WO 2015/158874 (“Enqvist”)   |
| 1019       | U.S. Patent No. 5,774,525 (“Kanevsky”)  |
| 1020       | Olli Jarva, <i>Intelligent Two-Factor Authentication: Deciding Authentication Requirements Using Historical Context Data</i> , Aalto Univ. (May 13, 2014) |

| No.  | Description   |
|------|---|
| 1021 | U.S. Patent No. 9,298,890 (“Bajenov”)   |
| 1022 | Affidavit of Mina Ching dated October 14, 2025 (“Azure Wayback”)  |
| 1023 | U.S. Patent No. 9,955,349 (“McClintock”)  |
| 1024 | U.S. Patent No. 11,184,766 (“Lord”)   |
| 1025 | U.S. Patent No. 11,184,392 (“Thomas”)   |
| 1026 | U.S. Patent No. 9,160,726 (“Kaufman”)   |
| 1027 | U.S. Patent No. 9,122,866 (“Kolman”)  |
| 1028 | U.S. Patent Application Pub. No. 2003/0115142 (“Brickell”)  |
| 1029 | U.S. Patent Application Pub. No. 2014/0208419 (“Chang”)   |
| 1030 | U.S. Patent Application Pub. No. 2018/0189470 (“Kim”)   |
| 1031 | U.S. Patent Application Pub. No. 2014/0289833 (“Briceno”)   |
| 1032 | U.S. Patent Application Pub. No. 2016/0191512 (“Tatourian”)   |
| 1033 | U.S. Patent Application Pub. No. 2015/0150090 (“Carroll”)   |
| 1034 | U.S. Patent Application Pub. No. 2017/0063896 (“Muddu”)   |
| 1035 | U.S. Patent No. 10,432,605 (“Lester”)   |
| 1036 | U.S. Patent Application Pub. No. 2010/0211996 (“McGeehan”)  |
| 1037 | U.S. Patent No. 9,779,236 (“Abrams”)  |
| 1038 | U.S. Patent No. 9,639,678 (“Moore”)   |
| 1039 | U.S. Patent No. 9,648,034 (“Bailey”)  |
| 1040 | U.S. Patent Application Pub. No. 2018/0027006 (“Zimmermann”)  |
| 1041 | Shammi Ishara Hewamadduma, <i>Detection and Prevention of Possible Unauthorized Login Attempts Through Stolen Credentials from a Phishing Attack in an Online Banking System</i> , IEEE Int’l Conf. on Rsch. and Innovation in Info. Sys., at 13-18 (ICRIIS 2017) (“Hewamadduma”) |

| No.  | Description   |
|------|---|
| 1042 | U.S. Patent No. 8,266,682 (“Lee”)   |
| 1043 | U.S. Patent No. 9,397,996 (“Roskind”)   |
| 1044 | Affidavit of Mina Ching dated November 14, 2025 (“Phone Factor + Oracle Wayback”)   |
| 1045 | N/A   |
| 1046 | N/A   |
| 1047 | N/A   |
| 1048 | Declaration of Ingrid Hsieh-Yee dated December 16, 2025   |
| 1049 | Affidavit of Mina Ching dated November 14, 2025 (“Coffin Wayback”)  |
| 1050 | <p>Lucas Jellema, <i>Just Launched: The Oracle Identity Cloud Service –for Authentication and Authorization Across the Cloud and on Premises</i>, AMIS Tech. Blog (Nov. 2, 2016), available at: <a href="https://technology.amis.nl/platform/just-launched-the-oracle-identity-cloud-service-for-authentication-and-authorization-across-the-cloud-and-on-premises/">https://technology.amis.nl/platform/just-launched-the-oracle-identity-cloud-service-for-authentication-and-authorization-across-the-cloud-and-on-premises/</a></p> |
| 1051 | <p>John Ribeiro, <i>Oracle Will Acquire Cloud Security Vendor Palerra</i>, FoundryCo, Inc. (Sep. 18, 2016), available at: <a href="https://www.networkworld.com/article/955458/oracle-will-acquire-cloud-security-vendor-palerra-2.html">https://www.networkworld.com/article/955458/oracle-will-acquire-cloud-security-vendor-palerra-2.html</a></p>   |
| 1052 | <p>Sarah Kuranda, <i>Oracle Acquires Cloud Access Security Brokerage Startup Palerra</i>, The Channel Co. (Sep. 19, 2016), available at: <a href="https://www.crn.com/news/security/300082128/oracle-acquires-cloud-access-security-brokerage-startup-palerra">https://www.crn.com/news/security/300082128/oracle-acquires-cloud-access-security-brokerage-startup-palerra</a></p>  |
| 1053 | <p><i>Hiding in Plain Sight: How a Cloud Access Security Broker With Built-In User Behavior Analytics Unmasks Insider Threats in the Cloud</i>, Oracle (Jan. 2017)</p>  |

| No.  | Description  |
|------|--|
| 1054 | <p>Ganesh Kirti, <i>Dealing With Dropbox: Unmasking Hackers With User Behavior Analytics</i>, Cloud Sec. Alliance (Sep. 7, 2016), available at:<br/> <a href="https://cloudsecurityalliance.org/blog/2016/09/07/dealing-dropbox-unmasking-hackers-user-behavior-analytics">https://cloudsecurityalliance.org/blog/2016/09/07/dealing-dropbox-unmasking-hackers-user-behavior-analytics</a></p> |
| 1055 | <p>Mitch Wagner, <i>Oracle Buys Palerra to Boost Cloud Security</i>, Informa TechTarget (Sep. 18, 2016), available at:<br/> <a href="https://www.lightreading.com/security/oracle-buys-palerra-to-boost-cloud-security">https://www.lightreading.com/security/oracle-buys-palerra-to-boost-cloud-security</a></p>  |
| 1056 | N/A  |
| 1057 | Complaint, <i>Qomplx LLC v. Microsoft Corp.</i> , Case No. 1:25-cv-01383-ADA (W.D. Tex.) (Aug. 8, 2025)  |
| 1058 | Affidavit of Mina Ching dated December 12, 2025 (“2016 White Paper”)   |
| 1059 | U.S. Patent No. 10,742,647 (“Crabtree 647”)  |
| 1060 | Guohui Wang and T.S. Eugene Ng, <i>The Impact of Virtualization on Network Performance of Amazon EC2 Data Center</i> , IEEE INFOCOM 2010, at 1163-1171 (Mar. 2010) (“Wang NPL”)  |
| 1061 | U.S. Patent Application Pub. No. 2011/0314558 (“Song”)   |
| 1062 | U.S. Patent No. 11,218,474 (“Crabtree 474”)  |
| 1063 | U.S. Patent Application Pub. No. 2015/0319185 (“Kirti App.”)   |
| 1064 | N/A  |
| 1065 | Patent Comparison Chart  |
| 1066 | Affidavit of Mina Ching dated December 24, 2025 (“APress-Coffin”)  |

**MANDATORY NOTICES UNDER 37 C.F.R. § 42.8**

**1. Real Party-In-Interest**

Microsoft Corporation is the sole real party-in-interest.

**2. Related Matters**

The '426 patent (EX1001) has been asserted against Microsoft in the following district court litigation: *Qomplx LLC v. Microsoft Corporation*, Case No. 1-25-cv-01383 (W.D. Tex.), filed August 28, 2025.

**3. Lead And Back-Up Counsel, And Service Information**

| <b>Lead Counsel</b>  | <b>Back-up Counsel</b>  |
|--|---|
| Andrew M. Mason, Reg. No. 64,034<br>andrew.mason@klarquist.com   | Frank Morton-Park, Reg. No. 80,750<br>frank.morton-park@klarquist.com<br><br>Todd M. Siegel, Reg. No. 73,232<br>todd.siegel@klarquist.com<br><br>Samuel B. Thacker, Reg. No. 78,633<br>samuel.thacker@klarquist.com |
| KLARQUIST SPARKMAN, LLP<br>121 SW Salmon Street, Suite 1600<br>Portland, Oregon, 97204<br>503-595-5300 (phone)<br>503-595-5301 (fax) |   |

Petitioner consents to service via email at the above email addresses and the email address of Msft-Qomplx@klarquist.com.

Pursuant to 37 C.F.R. § 42.10(b), concurrently filed with this Petition is a Power of Attorney executed by Petitioner and appointing the above counsel.

Petitioner authorizes Account No. 02-4550 to be charged for any fees,  
including those enumerated in 37 C.F.R. § 42.15.

## **I. INTRODUCTION**

Microsoft Corporation (“Petitioner”) respectfully requests *inter partes* review (“IPR”) of claims 1-21, 23-28, and 30 of U.S. Patent No. 12,231,426 (“the ’426 patent”) (EX1001), allegedly assigned to QOMPLX LLC (“Patent Owner”).

The ’426 patent issued February 18, 2025, and relates to multi-factor authentication (MFA), a concept that the patent itself admits was “widely used” before the patent’s earliest possible effective filing date (October 2017). EX1001, 2:20. As was well known, MFA typically involves a traditional username/password login and an additional form of verification, such as a one-time password (OTP) sent to a mobile device, a fingerprint scan, etc.

The challenged claims are directed to performing multi-factor authentication (“additional verification”) upon determining that a previous login attempt (“access request”) comprised an identifier not associated with the user account.

Prior art patent Kirti (EX1004), however, teaches analyzing historical login data to identify threats based on previous anomalous login requests, and teaches flagging a previous access request that originated from an IP address, geolocation, device and/or connection type that is not associated with the user account (e.g., a suspicious or blacklisted IP address). Kirti also teaches requiring “additional steps for authentication” when a threat is identified (e.g., when a previous request

originated from a suspicious or blacklisted IP address). Kirti alone renders the challenged claims obvious (Ground 1).

While Kirti teaches performing long-known multi-factor techniques, it lacks certain implementation details for basic aspects of these techniques (such as prompting the user to complete the additional authentication and checking that it was completed correctly). To the extent these well-known basics were not known to a POSITA, they are expressly taught by prior art Coffin. A POSITA implementing Kirti's system for threat detection and remediation would have naturally turned to Coffin for any needed implementation details, further rendering all challenged claims obvious (Ground 2).

The Examiner erred in failing to uncover Kirti and in issuing the challenged claims without a single prior art rejection. For these and other reasons presented more fully below, the Board should institute IPR based on the Grounds presented herein.

## **II. GROUNDS FOR STANDING PER 37 C.F.R. § 42.104(a)**

Petitioner certifies that the '426 patent is available for IPR and that Petitioner is not barred or estopped from requesting an IPR challenging the patent claims on the grounds identified in this petition.

### III. IDENTIFICATION OF CHALLENGE

#### A. Statement Of The Precise Relief Requested / Statutory Grounds

Petitioner requests *inter partes* review of claims 1-21, 23-28, and 30 (the “Challenged Claims”) of the ’426 patent, on the following statutory grounds:

|                 | Reference(s)                  | Basis           | Claims          |
|-----------------|-------------------------------|-----------------|-----------------|
| <b>Ground 1</b> | Kirti <sup>1</sup>            | 35 U.S.C. § 103 | 1-21, 23-28, 30 |
| <b>Ground 2</b> | Kirti and Coffin <sup>2</sup> | 35 U.S.C. § 103 | 1-21, 23-28, 30 |

### IV. LEVEL OF SKILL IN THE ART, AND STATE OF THE ART

#### A. Person Of Ordinary Skill In The Art

The person of ordinary skill in the art for the purposes of the ’426 patent in October 2017 (“POSITA”) would have had a bachelor’s degree in computer science, or equivalent, with two to four years’ experience designing, implementing, or otherwise working with cybersecurity technologies. More education, e.g., a Master’s or Ph.D., would compensate for less work experience and vice versa. EX1003, ¶35.

A POSITA would have been familiar with common, then-existing technologies for securing networks, applications, databases, and other digital systems, including the following state of the art:

---

<sup>1</sup> EX1004, U.S. Patent No. 10,063,654, filed June 24, 2015.

<sup>2</sup> EX1005, *Expert Oracle and Java Security*, published 2011.

- Authentication techniques based on an identifier (e.g., username) and password (*infra* Section IV.B.1);
- Additional or “multi-factor” authentication techniques used for added security (e.g., a one-time passcode or “OTP” sent to a mobile phone) (*infra* Section IV.B.2); and
- Tracking login attempts to determine standard behaviors and detect anomalous login attempts, in order to remediate security threats, such as a hacker cracking a user’s password) (*infra* Section IV.B.3).

EX1003, ¶36; *see also infra* Section IV.B.

## **B. State Of The Art**

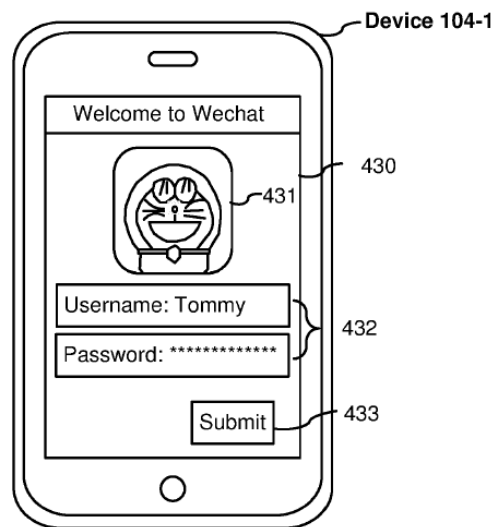
The knowledge and skill of a POSITA included the following claim-recited features, as reflected in the ’426 patent itself, background references, and the Kirti and Coffin prior art. These features were well-known, widely deployed (including in commercial systems), discussed in numerous patents, and often combined with one another. EX1003, ¶37.

### **1. Authentication With Username And Password Was Long-Known And Regularly Used**

It was well known to require a user to enter a username (or other unique identifier) and a password to gain access to their account. The ’426 patent acknowledges that a “login and password” was a “traditional” way to authenticate a

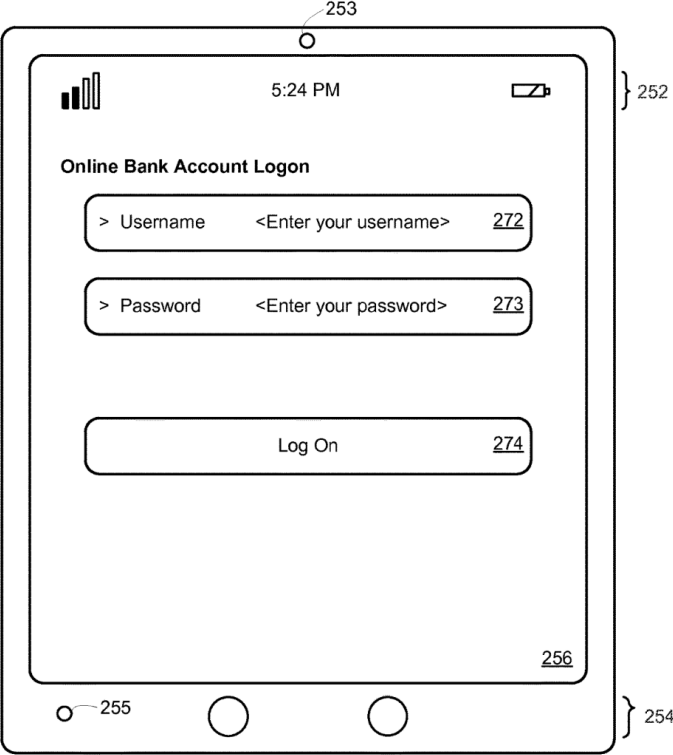
user. EX1001, 2:22. Indeed, this authentication method was commonly employed by at least 2004. *See* EX1003, ¶38 (citing EXS1006-1012, 1014, 1015, 1044).

Zhang, Varghese, and Mankovskii, for example, illustrate exemplary user interfaces requiring a user to enter their username and password to access their account.



**Figure 4B**

EX1008, FIG. 4B.



Mobile Device 141

FIG. 2

EX1010, FIG. 2

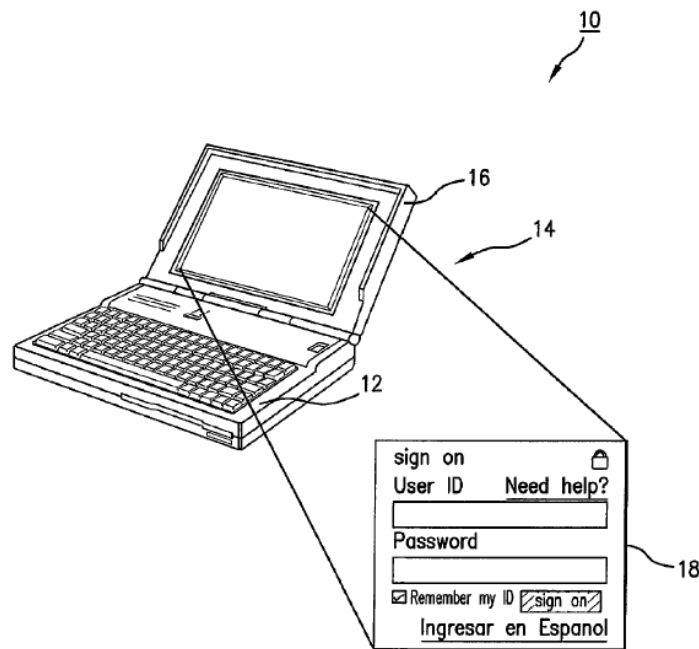


FIG. 1  
PRIOR ART

EX1011, FIG. 1. EX1003, ¶39.

## 2. Additional (i.e., Multi-Factor) Authentication Was Known And Regularly Used For Added Security

It was also well known to require additional forms of authentication in combination with a username and password. This technique, often called “multi-factor authentication,” increased security and reduced access risks posed by stolen or compromised usernames and passwords. *See* EX1003, ¶40 (citing EXS1005-1008, 1010-1012, 1014, 1016-1025, 1044, EX1058).

Indeed, the patent itself acknowledges that “[m]ulti-factor authentication (MFA) is widely used today as an additional verification step often used in

conjunction with a traditional login and password as a way to further secure a user's online accounts.” EX1001, 2:20-23. EX1003, ¶41.

Some of these known verification methods included “a second password or PIN code ... a CAPTCHA ... personal questions ... a biometric scan[], like fingerprint, retina, or facial recognition ... [and] pass codes sent to [] e-mail, pager, or cell phone.” EX1005, 177. Users could also “respon[d] to an email sent to a registered email address” (EX1011, 12:49-50), “answer[] the phone and ... enter[] an optional PIN” (EX1044, 9/34), and/or scan an encoded image such as a QR code (e.g., EX1016, 17:2-10; EX1008, [0040], [0103]-[0104], FIGS. 4C, 4F). *See also*, EX1001, 2:23-27 (describing “one-time use codes,” “uniquely generated link,” “authenticator devices and apps”). EX1003, ¶42.

Indeed, challenge questions were known by at least 1997 (*see* EX1019), one-time passwords were commonly employed by at least 2007 (*see* EX1017), and biometric scans were commonly employed by at least 2006 (*see* EX1011). *E.g.*, EX1019, Abstract, 2:5-23, 5:46-65, 10:17-11:3, 11:10-36 (claims 1-3); EX1017, [0003]; EX1011, 11:34-45; *see also* EX1003, ¶43 (citing EXS1005-1007, 1010-1011, 1017, 1019, 1020, 1044).

Further, it was known for a single system to offer several multi-factor verification options, each of which prompts a user to complete the additional verification method (e.g., enter the one-time password) and checks to ensure the user

completed the additional verification method correctly (e.g., the user-entered passcode matches the passcode sent to the user). *See* EX1003, ¶44 (citing EXS1005-1008, 1010, 1016-1020, 1022-1023).

Further, it was known to select a particular authentication method, including an additional authentication method from a plurality of authentication methods, such as based on the risk level of the access request, which authentication methods are available, cost, user preferences, etc. EX1003, ¶45 (citing EXS 1006, 1011, 1016, 1026-1033, 1061).

Indeed, more than 13 years before the '426 patent's alleged priority date, Golan disclosed "selecting the optimal [additional authentication] method" (EX1006, 12:18-19) based on, e.g., a risk assessment, available authentication methods, and deployment constraints. EX1006, 4:50-53, 6:25-29, 11:51-12:19, 19:11-22 ("[D]etermining which additional authentication options are available, wherein the one or more additional authentication details are selected from among the determined available authentication options"). EX1003, ¶46.

### **3. It Was Well Known To Implement Systems To Detect Anomalous Log-In Attempts, E.g., Brute Force Attacks**

It was well known for systems to detect anomalous activities (including anomalous login requests) to, for example, prevent, report, and/or remediate security

breaches (e.g., by requiring multi-factor authentication). EX1003, ¶47 (citing EXS1004, 1009-1011, 1018, 1021, 1023-1025, 1034-1041).

The '426 patent lists several types of cyberattack profiles as examples of anomalous activities, including a brute force attack in which a hacker tries different username/password combinations (EX1001, 8:35-46), and admits these cyberattack profiles were “just . . . a very small sample of the cyberattack profiles known to those skilled in the field.” EX1001, 8:45-46. Indeed, brute force attacks were well known. EX1003, ¶48 (citing EXS1004, 1015, 1042, 1043).

Another type of well-known anomaly is impossible travel (e.g., a user logs in from Portland, Oregon at 10:00 AM and minutes later logs in from Frankfurt, Germany), which can indicate credential theft and/or VPN abuse or proxy masking techniques typically employed by hackers. EX1003, ¶49 (citing EXS1004, 1011, 1022, 1036, 1037, 1040).

## V. THE '426 PATENT

The '426 patent, titled “Contextual and Risk-Based Multi-Factor Authentication,” issued February 18, 2025, from an application filed September 13, 2024. EX1001. It alleges priority via several continuation applications to a CIP application filed on October 23, 2017, which in turn claims priority to an October

19, 2017, provisional application and two strings of CIP applications going back to October 28, 2015.

**A. The Claims' Earliest Effective Filing Date Is October 19, 2017**

In district court, Patent Owner asserts an effective filing date of October 19, 2017, the filing date of the provisional application. EX1057, ¶92. This is the earliest possible effective filing date for the challenged claims at least because the earlier applications in the priority chain lack Section 112 support for the claims' additional verification steps (e.g., elements [1.8]-[1.11]).

The applications prior to October 19, 2017—each of them a continuation-in-part—describe systems for monitoring network traffic but do not disclose requiring additional verification steps. For example, the pre-October 19, 2017 applications lack FIGS. 4-7 of the '426 patent and the corresponding description related to multi-factor authentication.

**B. The '426 Patent's Specification**

The '426 patent purports to relate to “multi-factor [] authentication” (e.g., EX1001, 2:15-16) and its claims are directed to this concept, e.g., requiring additional verification after verifying the user's identifier and password (e.g., *id.*, 18:34-41). EX1003, ¶51.

Yet the '426 patent also admits that “[m]ulti-factor authentication (MFA) [was] widely used [] as an additional verification step ... in conjunction with a

traditional login and password,” (*id.*, 2:20-22) yet faults existing systems for their “over-reliance on a single method of deliver[ing]” the additional verification. *Id.*, 2:28-29. EX1003, ¶52.

The ’426 patent alleges that “[w]hat is needed is a system that uses a combination of verification methods.” *Id.*, 2:35-36. It purports to solve this problem by “requiring a user to use a plurality of verification methods to ... gain access to the network resource.” *Id.*, 3:38-40; *see also id.*, 2:53-55, 3:7-9, 11:40-51. For example, after the user performs “some initial form of authentication, such as a login and password,” “the server may request that the user use a plurality of verification methods to reach the verification score needed before access is granted.” *Id.*, 11:41-47. These additional verification methods include biometric scans (e.g., fingerprint), badge scans (e.g., RFID, NFC), one-time-use codes, and passive information such as IP address and device ID. *Id.*, 10:16-11:27, 11:44-48, FIG. 4. EX1003, ¶53.

Consistent with this emphasis, two earlier patents in the post-October 19, 2017 string of continuations have claims that require a *plurality* of additional verification methods. EX1062, 19:11-20:14 (claim 1) (“select a plurality of verification methods”); EX1059, 17:49-18:25 (claim 1) (“select a plurality of verification methods”). EX1003, ¶54.

The claims of the '426 patent, however, require only “an additional verification method” selected from the plurality of verification methods, as shown in Element 1.9 of claim 1, which recites:

| <b>Claim Element</b> | <b>Claim Language</b>  |
|----------------------|--|
| [1.1]                | A computer system configured to execute software instructions stored on nontransitory machine-readable storage media, wherein the software instructions comprise instructions that:  |
| [1.2]                | receive a request to authenticate a client, wherein the request comprises a first identifier and a password,   |
| [1.3]                | store, in a multidimensional time-series database, information about the request,  |
| [1.4]                | determine whether the password corresponds to a first user account identified by the first identifier,   |
| [1.5]                | determine whether an additional verification is required to grant access, wherein determining whether the additional verification is required to grant access comprises:   |
| [1.6]                | retrieving, from the multidimensional time-series database, historical information about previous access requests associated with the first user account, and  |
| [1.7]                | 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, |
| [1.8]                | based on the additional verification being required to grant access:   |
| [1.9]                | select an additional verification method from a plurality of verification methods,   |
| [1.10]               | cause the client to be prompted to complete the additional verification method, and  |
| [1.11]               | determine whether the additional verification method has been completed correctly.   |

EX1003, ¶55.

Independent claims 9, 19, and 26 are substantively identical to claim 1. EX1003, ¶56.

**C. The Prosecution History**

Prosecution was brief, with the Examiner allowing the claims just over three months after the application was filed. EX1002, 2-76, 272. The Examiner issued no prior art rejections. The sole Office action rejected claims 11-17 as indefinite because of a conditional “if” in independent claim 11 and rejected claims 1-30 based on nonstatutory double patenting over then-pending application no. 18/885,474<sup>3</sup>. EX1002, 149-153. Applicant filed a terminal disclaimer and amended the claims to remove the conditional “if,” and the Examiner subsequently allowed the claims. *Id.*, 155-158, 165-175, 272-281.

The Examiner did not search for “two-factor authentication.” *Id.* 187-271. Nor did the Examiner search PE2E for “multi-factor authentication.”<sup>4</sup> *Id.* 187-267.

---

<sup>3</sup> This application led to the '934 patent, which Petitioner concurrently challenges in IPR2026-00182.

<sup>4</sup> The Examiner appears to have searched the entire title of the patent (“contextual and risk-based multi-factor authentication”) in Google Patents without limiting the priority date. EX1002, 270-271. The file history shows only the first page of results, many of which do not appear to qualify as prior art. *Id.*

Neither Kirti nor Coffin, the two prior art references relied on in the Grounds herein, were cited or discussed on the record during prosecution.

## **VI. CLAIM CONSTRUCTION**

Unless otherwise noted below, Petitioner applies the plain and ordinary meaning of each claim term.<sup>5</sup> EX1003, ¶57.

## **VII. GROUNDS 1-2: CLAIMS 1-21, 23-28, AND 30 ARE OBVIOUS OVER KIRTI (EX1004) ALONE OR COMBINED WITH COFFIN (EX1005)**

As explained below, claims 1-21, 23-28, and 30 are obvious over Kirti alone (Ground 1) or Kirti and Coffin (Ground 2), as Coffin teaches implementation details for multi-factor authentication and other additional verification processes. EX1003, ¶58.

For the independent claims, Kirti teaches all claim elements but lacks express implementation details for certain well-known features. For example, while it teaches performing additional steps for authenticating a user, Kirti does not expressly state that this involves prompting the user to complete the additional authentication or confirming correct completion of the additional authentication. These details were at least obvious based on the knowledge and skill of a POSITA

---

<sup>5</sup> In any litigation, Petitioner reserves the right to raise additional issues of claim construction and/or argue that claim terms are indefinite or otherwise invalid and will apprise the Board of any briefing or orders that reflect such positions.

(see e.g., *supra* Section IV.B.2). Given the knowledge and skills of a POSITA, Kirti alone renders all challenged claims obvious under Ground 1. EX1003, ¶59.

To the extent Patent Owner argues otherwise, Coffin expressly teaches the basic implementation details for the techniques disclosed by Kirti. As explained in greater detail below (*infra* Section VII.C), a POSITA implementing Kirti would have been motivated with a reasonable expectation of success to incorporate Coffin’s more detailed teachings on multi-factor authentication, rendering all claims further obvious under Ground 2. EX1003, ¶60.

**A. Kirti (EX1004)**

Kirti issued as U.S. Patent No. 10,063,654 on August 28, 2018, from an application filed June 24, 2015 (EX1004, Cover; EX1063, Cover), and is prior art under Section 102(a)(2). In December 2016, original assignee Palerra, Inc. assigned Kirti to Oracle International Corporation, the named assignee. EX1004, Cover.

Kirti relates generally to a cloud-based system in which users log in to various cloud-based applications and other services. The Kirti system analyzes user login activity over time, to detect and remediate security threats such as brute force hacking attempts. *E.g.*, EX1004, 15:49-59, Abstract, claim 1. The “remedial measures” in Kirti include “additional steps to authentication.” *Id.*, 5:27-35; *see also*, *e.g.*, *id.*, 6:6-27, 28:21-36. EX1003, ¶¶61-62.

Kirti explains how a given user “may have user accounts with various cloud applications” (*e.g.*, EX1004, 5:9-14) and the “[c]loud applications connect a user’s device to remote services” (*id.*, 1:31-32). Much like the ’426 patent would later do, Kirti depicts a system in which various clients connect with other aspects of the system via a network (“Internet”), as shown in Kirti FIG. 1:

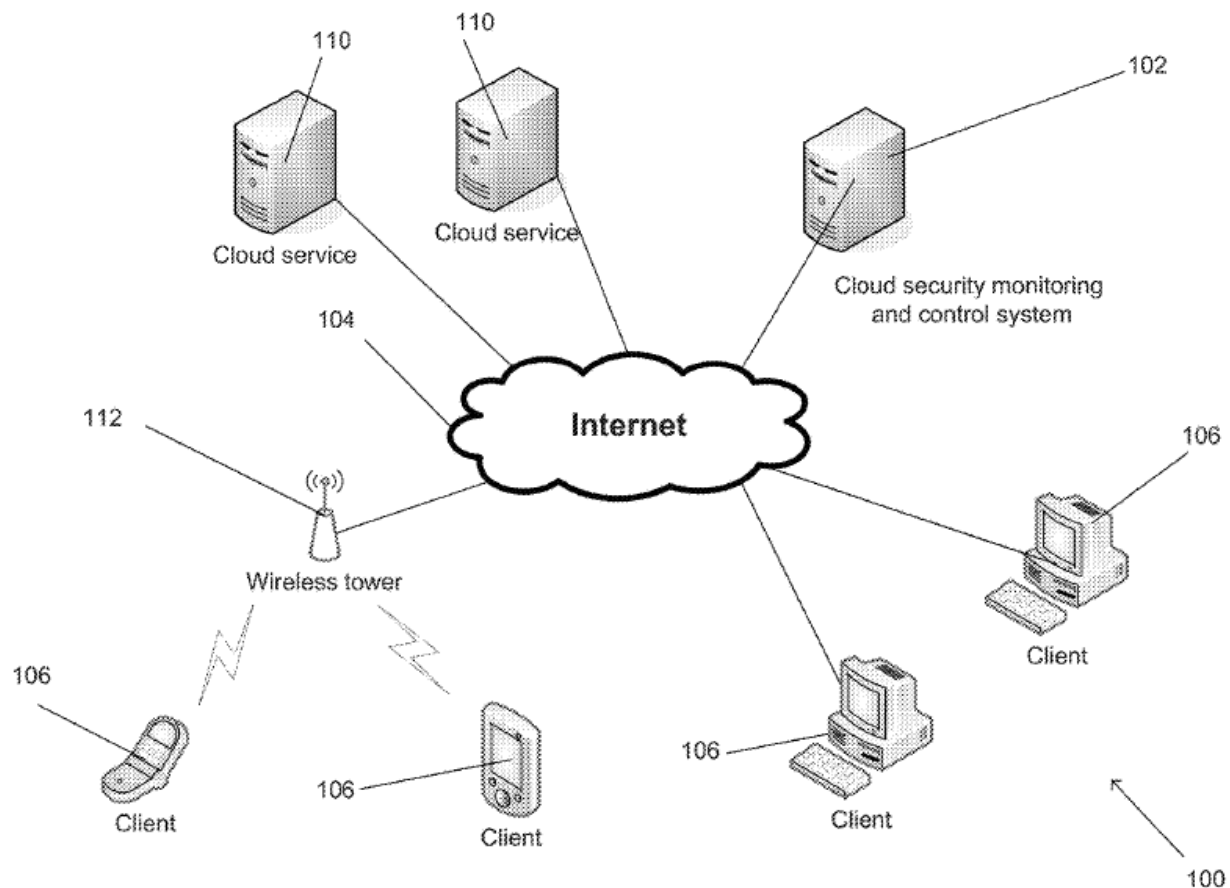


FIG. 1

EX1004, FIG. 1. EX1003, ¶63.

Based on a user’s login activity over time, Kirti creates a “baseline user profile” and then identifies “anomalous activity using the baseline user profile.”

EX1004, 1:47-59, 2:8-16, 29:37-46; 28:66-67; *see also id.*, 5:25-37, 10:9-59, 14:5-7, 18:14-42, 24:9-32. Login activity data includes the time of the login attempt (*e.g.*, *id.*, 12:28-57, 14:46-67, 16:53-17:8, 18:9-26); whether the login was successful, *e.g.*, correct username and password (*see e.g., id.*, 10:33-36, 18:38-41); the device and/or IP address from which the attempt was made (*e.g., id.*, 10:33-38, 12:5-13:2, 13:52-59, 16:28-32, 16:53-17:19, 17:44-46, 18:14-25, 18:38-41); and the resources accessed (*e.g., id.*, 10:33-44, 12:5-18, 16:53-61, 18:14-27). EX1003, ¶64.

In response to detecting anomalous activity or threats, the Kirti system may require “a higher level of security controls” (EX1004, 28:32) such as requiring “elevated authentication or OTP validation” (*id.*, 28:33). *See also id.*, 5:34 (“adding additional steps to authentication”); EX1003, ¶65.

**B. Coffin (EX1005)**

Coffin is a book that explains how to increase security for Oracle database applications. EX1005, 1. Coffin was published in 2011, by an established publisher (Springer), and thus qualifies as prior art under 102(a)(1) (AIA). EX1005, ii; EX1048 (expert librarian declaration confirming public accessibility of Coffin); EX1049, 5-9; *Nearmap US, Inc. v. Eagle View Tech., Inc.*, IPR2022-01009 Paper 28 at 31 (PTAB Dec. 14, 2023) (finding “presumption of public accessibility” for “textbook published by established publisher Springer”); *see also VidStream LLC v.*

*Twitter, Inc.*, 981 F.3d 1060, 1065 (Fed. Cir. 2020) (“When there is an established publisher there is a presumption of public accessibility as of the publication date.”).

Coffin teaches how to implement several types of additional verification methods, beyond username/password, in an Oracle database system. These additional verification methods include: a “second password or PIN,” “a CAPTCHA,” an “answer [to] personal questions,” a “biometric scan[], like fingerprint, retina, or facial recognition,” and “pass codes sent to [] e-mail, pager, or cell phone.” EX1005, 177. Coffin also explains that this additional verification beneficially provides an added layer of security by “assur[ing] [] that the person sitting at the keyboard is who they claim to be.” *Id.* EX1003, ¶66.

Coffin provides detailed step-by-step instructions explaining how to implement several types of one-time passcodes in Oracle database applications, such as an SMS to a phone, a URL to a pager, and an email to supporting devices. EX1005, 178-208. EX1003, ¶67. Coffin expressly teaches details for selecting one or more of the plurality of verification methods (*e.g.*, EX1005, 183, 185, 200, 201), prompting the user to complete the additional verification method (*e.g.*, *id.*, 183, 190, 193, 194, 201, 207), and determining whether the user correctly completed the additional verification method (*e.g.*, *id.*, 194, 201, 206). For example, “[b]y preference, [the system] will send the two-factor code to the user’s pager and cell phone. If neither of those is available, [the system] will send the code to the user’s

e-mail.”). *Id.*, 200. “Once the user receives the two-factor pass code” (*id.*, 183), “[they] will have to enter those 2-factor codes in order to get access” (*id.*, 207). The computer system then “test[s] the two-factor code to see if it passes muster.” *Id.*, 194. EX1003, ¶67.

### **C. Combining Kirti And Coffin**

The Kirti+Coffin combination combines Kirti’s threat detection and remediation system with Coffin’s implementation details on how to select and perform an additional verification process, such as 2-factor authentication. As noted above, Kirti provides less implementation detail, however, on selecting and performing its additional steps for authentication, and does not expressly disclose some of the more basic steps recited in Elements [1.8]-[1.11] of the challenged claims. Yet POSITAs knew that implementing an additional authentication requires these common steps: “select[ing] an additional verification method from a plurality of verification methods, caus[ing] the client to be prompted to complete the additional verification method, and determin[ing] whether the additional verification method has been completed correctly” (EX1001, 18:36-41 (claim 1)). *Supra* Section IV.B.2. EX1003, ¶68.

To the extent a POSITA implementing Kirti (an Oracle patent) did not already know these details, she would have naturally looked to Coffin (a book on improving security in Oracle systems) for its detailed teachings on well-known types of

additional verification methods and step-by-step instructions for how to implement these additional verification methods. EX1003, ¶69.

A POSITA would have been motivated with a reasonable expectation of success to incorporate Coffin’s additional verification teachings in Kirti’s system for at least several reasons:

1. Kirti teaches requiring and performing well-known techniques for additional verification but provides few implementation details;

2. Coffin provides details on how to implement these additional verification techniques, with step-by-step instructions;

3. Kirti and Coffin both offer the same motivation for including this additional verification (added security), as was well known in the art (*supra* Section IV.B.2); *see also* EX1005, 177 (Two-factor authentication “assure[s] [] that the person sitting at the keyboard is who they claim to be.”);

4. Coffin’s additional verification teachings would have been easily implemented in Kirti’s system—requiring only minimal software modifications that were well within the skill of a POSITA; and

5. Both Kirti and Coffin relate to Oracle cloud applications, making them a natural pairing (Kirti is an Oracle patent and Coffin a textbook on how to program secure Oracle database applications).

EX1003, ¶70.

Kirti already teaches requiring additional verification. *E.g.*, EX1004, 28:33 (“elevated authentication or OTP validation”) and 5:34 (“adding additional steps to authentication”). Coffin provides step-by-step instructions explaining how to implement at least some of these additional verification methods. *E.g.*, EX1005, 177-178, 183, 207 (“[W]e developed a process to send 2-factor authentication codes to our application users on their cell phones, pagers and e-mail accounts.”); *see generally id.*, 177-208 (Chapter 9). Moreover, implementing these additional verification teachings in Kirti’s system would have required simple, predictable, and straightforward software modifications. *E.g.*, EX1005, xxv (explaining Coffin purpose to “provide you tools and knowledge that you can put to immediate use ... [and] get you thinking about how you can write bulletproof applications of your own”), xxvi (explaining how book provides “a template that we can provide to other application programmers so that they can implement the same security structures”); EX1003, ¶71; *KEYnetik, Inc. v. Samsung Elecs. Co., LTD.*, No. 2022-1127, 2023 WL 2003932, at \*\*1-2 (Fed. Cir. Feb. 15, 2023) (expert testimony that “the software modifications needed to combine the prior art references would be ‘straightforward’ and ‘simple’ for a skilled artisan” “sufficient to establish a reasonable expectation of success”).

Further, Kirti is a patent assigned to Oracle and Coffin provides teachings on how to improve security in Oracle systems. Indeed, Kirti includes what appears to

be a screen shot from Palerra's LORIC product (EX1004, FIG. 5D), which Oracle integrated into its CASB Cloud Service after acquiring Palerra in September 2016 (EX1053, 3 n.1; EX1050; EX1051; EX1052; EX1054; EX1055). This further establishes both motivation and reasonable expectation of success in applying Coffin's Oracle-centered teachings to the threat detection systems of Kirti. Moreover, Coffin provides "a foundation for secure programming in Java and Oracle, and their common ground, Java Stored Procedures (JSP)." EX1005, xxv; *see also id.*, 1 ("[M]uch of what we will do here can be acquired through commercial products from Oracle corporation and elsewhere."), 2 (explaining that Coffin provides a foundation for achieving "application security using the basic Oracle Database and Java services"), 27 (noting that Oracle provides the Java Development Kit), 193 (describing Oracle "Java stored procedure" used "to send two-factor codes to a user"). EX1003, ¶72.

The narrative claim mappings below provide additional explanation, as pertinent, on why and how a POSITA would have incorporated Coffin's teachings into a system like that taught by Kirti. EX1003, ¶73.

1. Claim 1

a) Element [1.1]<sup>6</sup>

[1.1] A computer system configured to execute software instructions stored on nontransitory machine-readable storage media, wherein the software instructions comprise instructions that:

If the preamble is limiting, Kirti satisfies it. Kirti teaches a system, such as “system 100 including a cloud security monitoring and control system 102, client devices 106 ... and cloud services 110.” *E.g.*, EX1004, 4:14-19, FIG. 1. The system includes “software modules” and a processor, and Kirti teaches storing the software modules “in volatile or non-volatile memory and,” that these modules “configure the processor 201 to perform certain functions or processes.” *Id.*, 5:38-44. The software modules include Kirti’s threat detection and prediction analytics and other applications. *Id.*, 5:44-6:35. *See also id.*, 2:37-51 (discussing memory containing applications), 29:66-30:39 (claim 15) which recites *inter alia* “memory including one or more instructions that, when executed by the processor, cause the processor to” carry out various steps such as determine anomalous activity using a user profile and send instructions to change security controls), 4:5-13 (describing system components including “software applications and/or modules that configure a server

---

<sup>6</sup> Reference numbers in the format of [claim#.limitation#] are added throughout for ease of reference.

or other computing device to perform processes”), 4:29-45. These software modules include instructions that cause the system to carry out the steps recited in the body of the claim, as explained in the following sections. EX1003, ¶74.

**b) Elements [1.2], [1.4]**

[1.2] receive a request to authenticate a client, wherein the request comprises a first identifier and a password,

[1.4] determine whether the password corresponds to a first user account identified by the first identifier,

Kirti teaches these claim elements at least because it teaches tracking whether requests to authenticate (“login attempts”) are successful and that “login attempts” include an identifier (e.g., “identifier,” “username”) and “password.” *E.g.*, EX1004, 10:9-46, 22:3-10. A POSITA would have understood or at least found it obvious that, as part of tracking whether the requests are successful, the Kirti system receives each such request and determine whether the password is correct (i.e., corresponds to the user account identified by the identifier). EX1003, ¶75.

Kirti discloses users logging in to cloud applications from various “client devices,” as shown in FIG. 1:

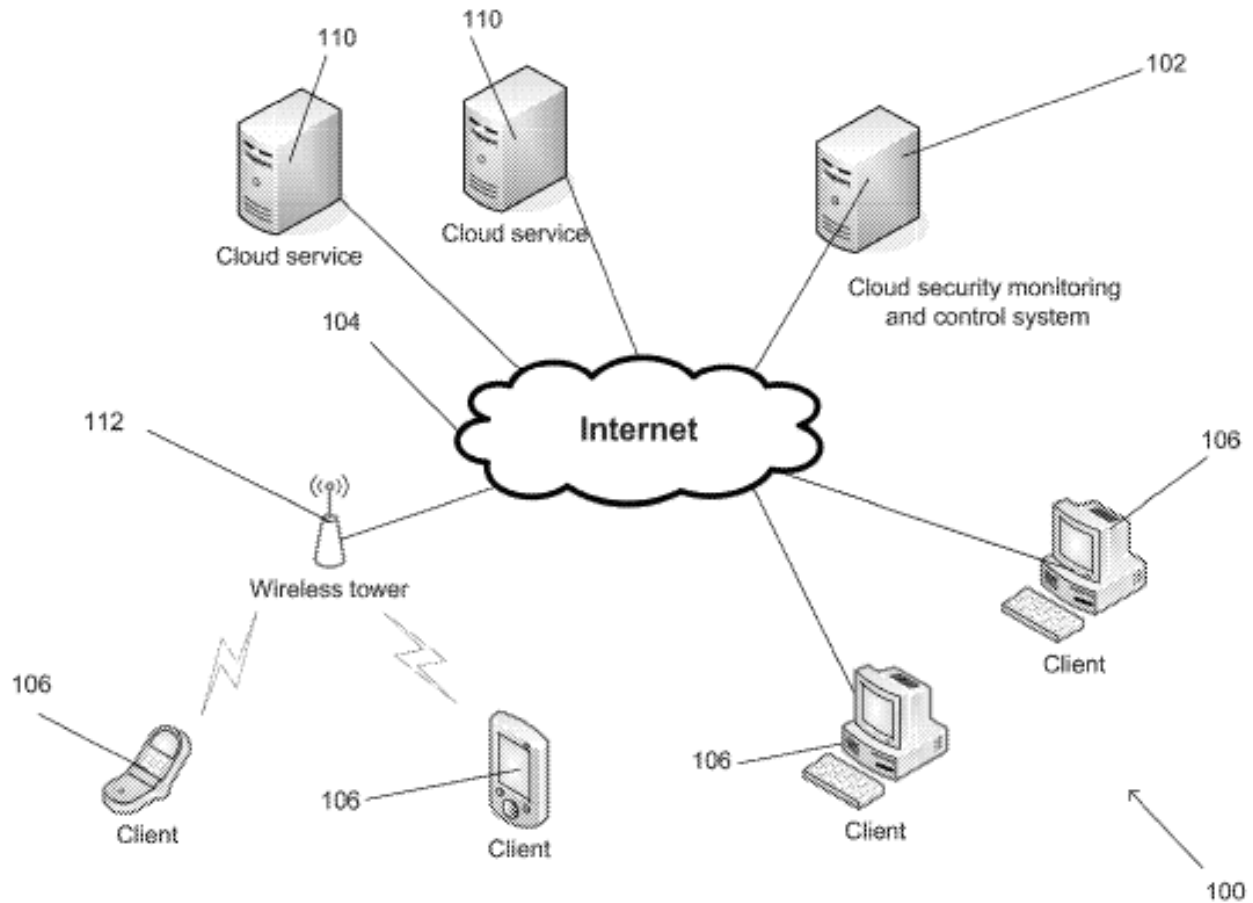


FIG. 1

EX1004, FIG. 1; *id.*, 4:15-20 (“client devices 106 that can be used to access the cloud security system 102”), 1:31-34 (“Cloud applications connect a user’s device to remote services that provide an additional functionality.”), 9:38 (“user login[] attempts”), 15:36-37, 16:31-32 (“how a user does or is expected to log in or access a cloud application”), 17:4-5, 18:40-41, 28:4 (“user logs”). EX1003, ¶76.

Kirti discloses login attempts that include a username or other identifier.<sup>7</sup> *E.g.*, EX1004, 15:55-59 (describing “login attempts with invalid or terminal/suspended usernames”), 13:47-51 (“A single user can be identified across multiple clouds using one or more attributes or identification factors, such as a primary user identifier (ID).”), 22:3-12 (tracking distance between “login attempts, successful logins, and/or failed logins,” accounting for a user’s “different usernames” for “different cloud applications”), 18:17-23 (“events such as ... logging in to the cloud application ... [include] event details such as ... user name”); *see also id.*, 10:30-46 (“types of activity data can include ... login and logout statistics ... [and] can include the user account or other user identifier for the user associated with the events or statistics”), 7:30-67 (Tables 1-2) (“Credentials and Identifiers”)’ 13:62-67 (describing “the user identifier associated with” a user’s different cloud application accounts and providing example identifiers “jdoe, john.doe, etc.”). EX1003, ¶77

Kirti also teaches that its login attempts include a password and discloses that the system determines whether a given login attempts succeeds or fails. EX1004, 10:35-36 (tracking “login and logout statistics (including attempts and successes)”); 2:23-25 (tracking failures); *see also id.*, 12:9, 12:19-20, 12:65-13:17, 13:52-59, 15:4-

---

<sup>7</sup> The ’426 patent does not use the term “identifier” outside the claims.

7, 15:14-16, 15:47-59, 18:38-41, 19:25-59 (Table 4), 21:19-52, 22:8, 29:53-55, FIGS. 8C (“Failed logins”), 8D (“failed logins”). EX1003, ¶78.

For example, Kirti discloses detecting a threat if a user has several failed login attempts because such activity “indicate[s] a concerted effort to crack the user’s password.” EX1004, 13:14-16; *see also id.*, 13:56-57 (identifying “users who have several failed login attempts and then change their password”), 15:49-59 (“A brute force attack scenario may refer to an attacker's attempts to try many passwords in order to discover a correct password and compromise a user account.”). Kirti also discloses changing and/or resetting the user’s password (*id.*, 5:35, 12:13, 13:57, 24:45, 25:34-40, 25:48) and password policies (*id.*, 7:30-67 (Tables 1-2), 14:40-45, 19:25-59 (Table 4), 26:33-38, 27:23-26, 27:31-35, 27:39-42, FIG. 8E (illustrating different password options for a given user account)). Kirti (EX1004) FIG. 8E shows a user interface with “Password Controls” that include example “password requirements for a user account.” EX1004, FIG. 8E, 26:29-38; *id.*, 6:32-38.

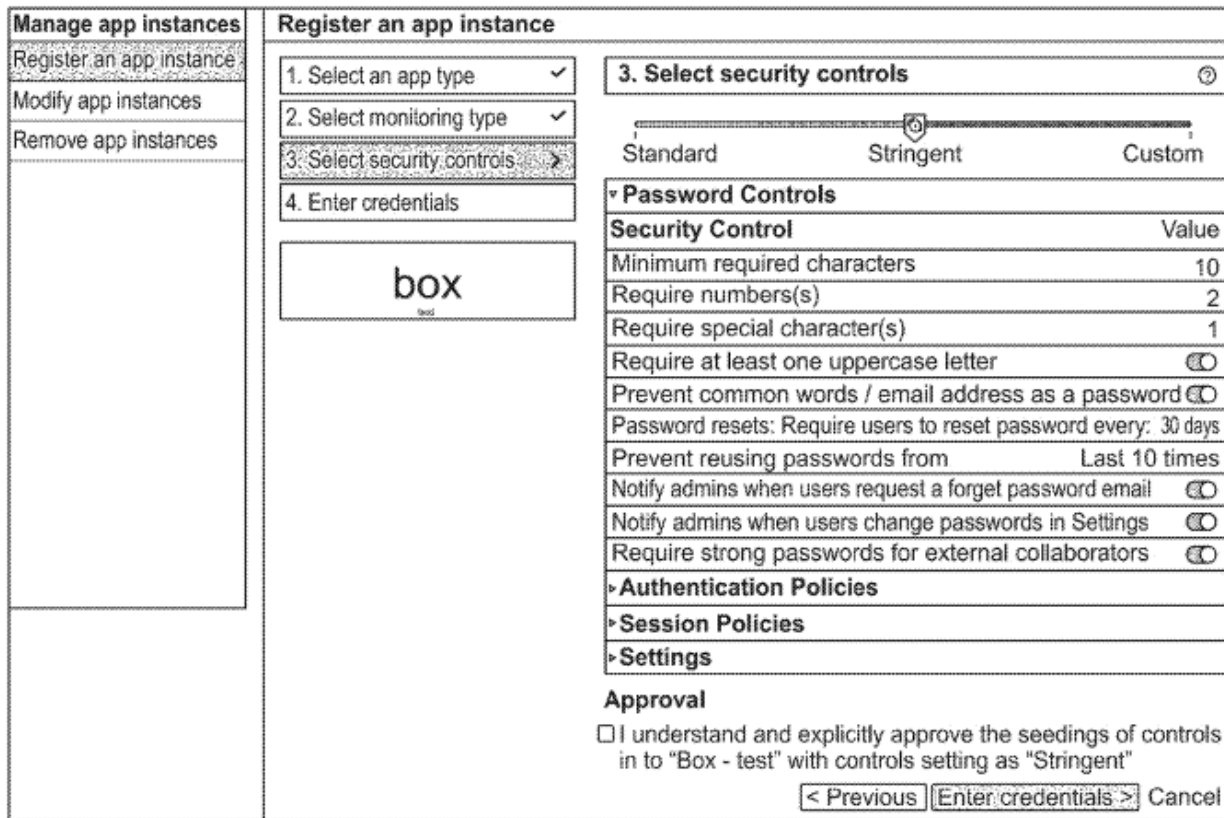


FIG. 8E

EX1004, FIG. 8E; EX1003, ¶79.

POSITAs understood that the success or failure of a given login attempt in Kirti resulted from the system determining whether the received password corresponded to a user account identified by the received username or other identifier, consistent with known login conventions. *Supra* Section IV.B.1. The '426 patent confirms that this was conventional by noting “traditional login and password” in its “State of the Art” section without providing any detail on how to implement this “traditional” functionality. EX1001, 2:18-23. EX1003, ¶80.

A POSITA also would have understood that a user enters a username and password when connecting to the cloud application(s) at least because this is what an administrator does when connecting to the cloud. EX1004, 5:20-24, 6:60-65, 10:9-15, 26:49-54. EX1003, ¶81.

Thus, Kirti teaches that a client (“user”) submits a request to authenticate (“login attempt[]”), which includes an identifier (e.g., “identifier,” “username”) and “password,” and that the system receives this request and determines whether the password corresponds to a user account identified by the identifier (i.e., determines, based on the received username and password, whether the login succeeds or fails). Further supporting that it was obvious to implement Kirti’s system to receive and check the user’s username and password, this was a well-known, standard, and conventional technique for authenticating a user. *Supra* Section IV.B.1. EX1003, ¶82.

**c) Element [1.3]**

[1.3] store, in a multidimensional time-series database, information about the request,

Kirti teaches this claim element at least because it discloses that its system stores, in a multidimensional time-series database (e.g., “analytics and threat intelligence repository database”), information about requests for authentication (e.g., “activity data,” for “login and logout statistics (including attempts and

successes)”). *E.g.*, EX1004, 10:33-36, 10:60-61. The information includes timestamp (*e.g.*, *id.*, 12:35-54, 14:48-54, 16:49-60, 18:9-23), whether the request was successful (*e.g.*, *id.*, 10:34-44, 18:38-41), the device and/or IP address of the request (*e.g.*, *id.*, 10:34-44, 12:1-18, 12:35-13:29, 13:44-59, 16:28-40, 16:55-67, 17:9-55, 18:17-23, 18:38-41), and what resources were accessed (*e.g.*, *id.*, 10:34-44, 12:7-18, 16:49-60, 18:17-23). *Id.*, 10:35-39 (“activity data can include ... login and logout statistics (including attempts and successes), IP addresses used to access the application, devices used to access the application, and cloud resources that were accessed”). EX1003, ¶83.

Kirti’s analytics and threat intelligence repository database is a multidimensional time-series database. It is multidimensional because each time point includes activity data for multiple parameters/attributes (*e.g.*, IP address, login attempt result (success or failure), identifier (*e.g.*, username), resources accessed, etc.). EX1004, 4:46-5:3, 10:25-50, 10:60-11:4, 12:1-18, 12:35-13:29, 13:44-59, 14:48-54, 16:28-40, 16:55-67, 17:9-55, 18:9-23, 18:38-41). And it is a time-series database at least because it includes the same activity data (*i.e.*, values for the same parameters/attributes) for multiple time points. *E.g.*, EX1004, 13:27-30 (“[D]ata collected over time is used to build models of normal behavior (*e.g.*, patterns of events and activity) and flag behavior that deviates from normal as abnormal behavior.”).

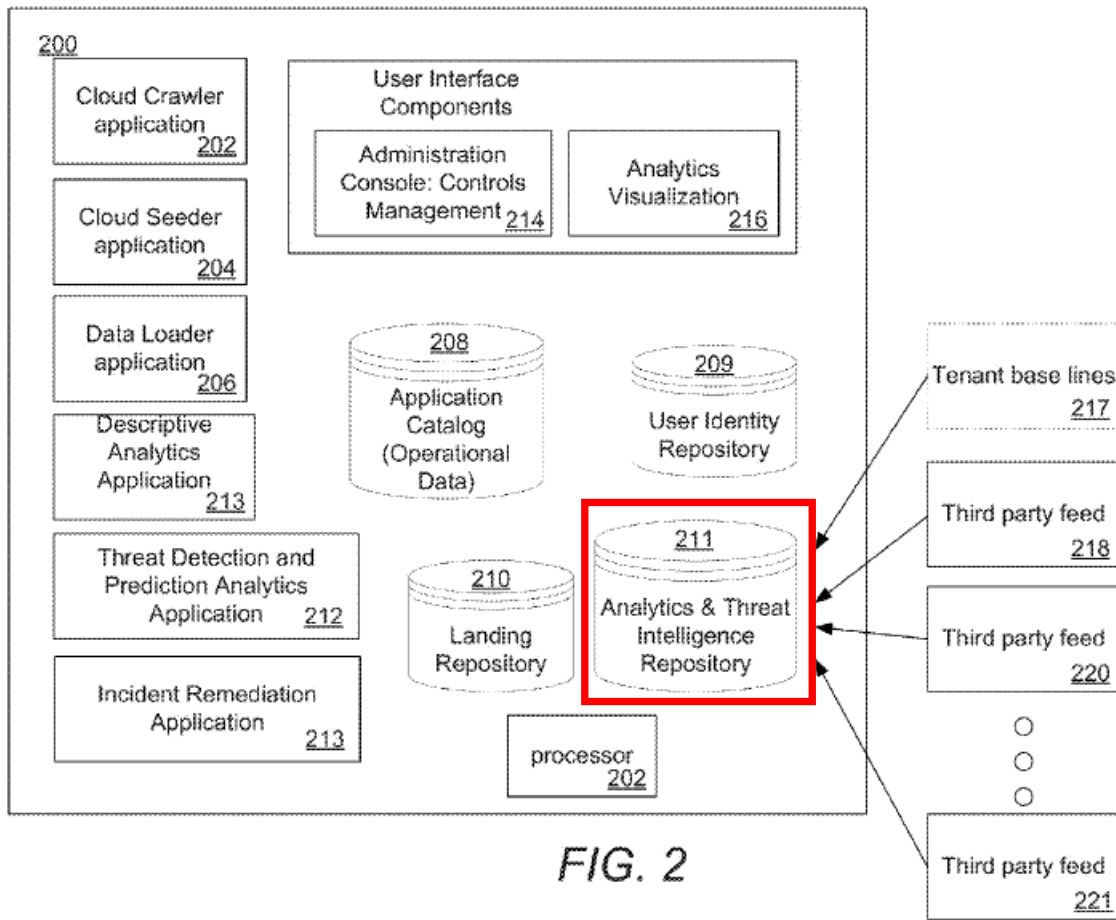


FIG. 2

EX1004, FIG. 2 (red annotations added). EX1003, ¶84.

Consistent with its time-series nature, Kirti’s database stores weeks’ worth of activity data that “can be utilized to generate reports that may be presented visually.” EX1004, 4:54-59; *see also id.*, 6:35-44, 11:15-58, 12:5-35, 12:50-57, 14:46-15:16, FIGS. 8B-8D. For example, FIG. 8C “displays a count of events by date in each of the color coded categories such as activities at an unusual time, after-hours downloads, failed logins, etc.,” for prior four-week and twelve-week periods, thus

confirming that Kirti's multidimensional time-series database stores timestamped data for multiple attributes/parameters over a period of time. *Id.*, 15:5-7.

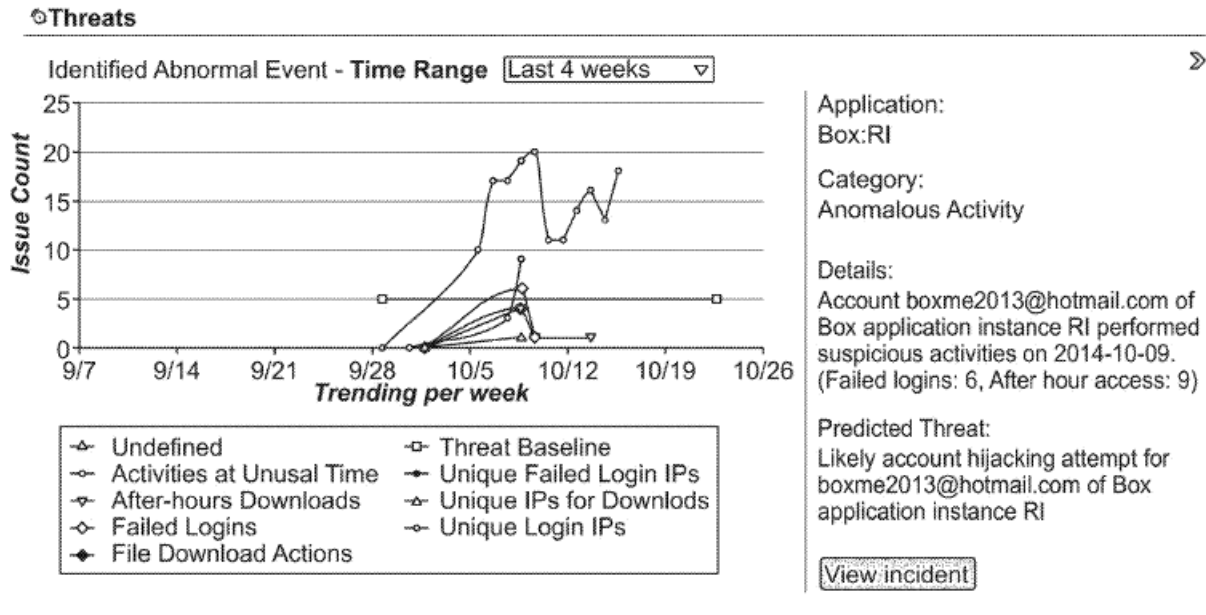


FIG. 8C

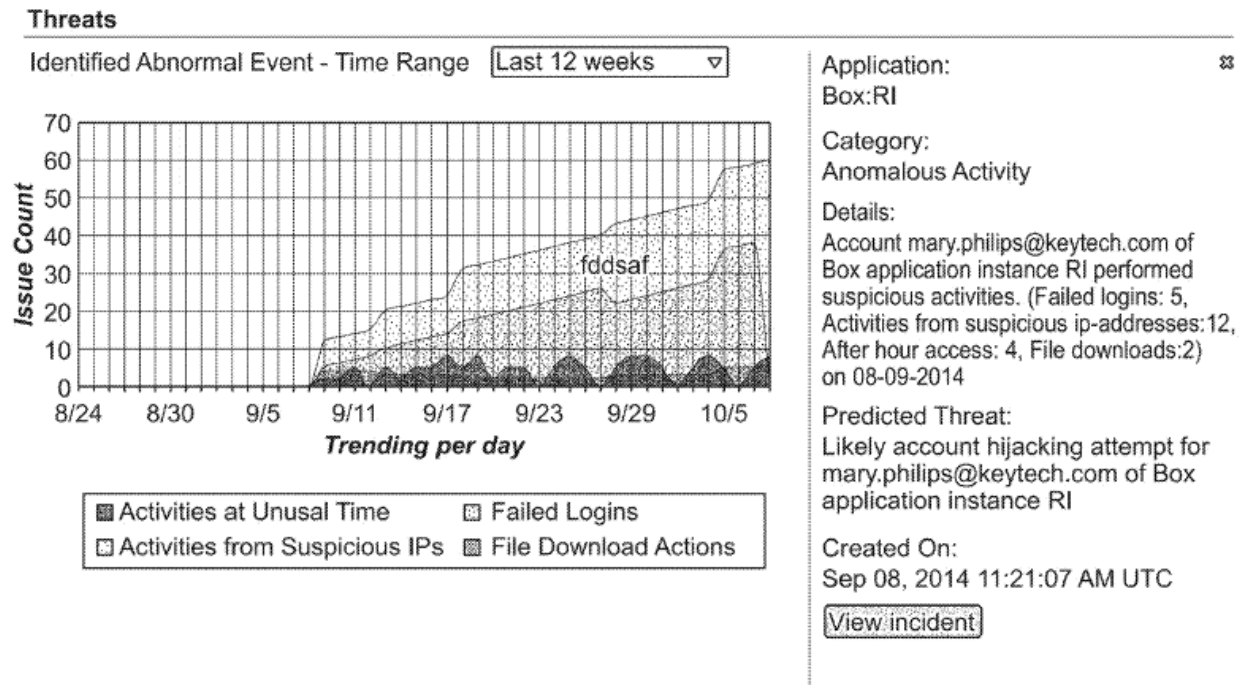


FIG. 8C (Cont.)

EX1004, FIG. 8C. EX1003, ¶85.

d) **Element [1.5]**

[1.5] determine whether an additional verification is required to grant access,

Kirti teaches this claim element. The Kirti system analyzes a user’s historic login activity to identify potential threats and determine whether to apply “remedial measures, such as **adding additional steps to authentication.**” *E.g.*, EX1004, 5:25-37 (emphasis added); *see also id.*, 3:53-58 (system performs “threat detection” and recommends “appropriate responses to different categories of threat”), 3:58-4:3 (system determines “models of normal and/or abnormal behavior in user activity,” detects “patterns of suspicious activity,” and then recommends “remedial

measures”). Kirti teaches carrying out this remediation “automatically.” 25:49-52. EX1003, ¶86

Kirti explains that “[a]ny of a variety of security measures may be taken to address an identified threat such as, but not limited to ... setting stronger security controls.” EX1004 25:46-49 (within section titled “Remediation”); *see also id.*, 25:16-20 (describing alert with recommended “remediation action(s), such as implementing stronger security controls”). Example stronger security controls include requiring “elevated authentication or OTP validation.” *Id.*, 28:31-33. POSITAs knew that “OTP validation” in Kirti referred to “one-time passwords,” a commonly-used secondary authentication technique. *E.g.*, EX1020, 2 (2014 thesis, stating “the most commonly used second factor is one-time passwords”); *see also* EX1001, 2:23-25 (“MFA methods commonly used today includes one-time use codes sent to a user’s mobile device or email”); EX1014, 4:17-18 (“some users may be required to engage in a token-based one-time password (OTP) process”); EX1016, 1:58-59 (“Another authentication approach is for a service provider to equip the user with a One Time Password (OTP) device.”); EX1018, 3:3-4 (“One solution to avoid attacks with replaying captured reusable passwords is to use one-time passwords (OTP).”). EX1003, ¶87.

POSITAs would have understood that Kirti’s “additional steps to authentication” and other “stronger security controls” are additional verification

beyond the traditional username/identifier and password authentication used by Kirti client devices. EX1003, ¶88. Kirti describes logins as involving username and password (*supra* Section VII.C.1.b) and POSITAs would have understood that the “stronger security controls” are in addition to that baseline username/password requirement. EX1003, ¶88.

Thus, Kirti’s recommended “additional steps to authentication”—such as elevated authentication or OTP validation—satisfy the claimed “additional verification [] required to grant access.” EX1003, ¶89. The ’426 patent itself characterizes types of additional authentication as additional verification: “Multi-factor authentication (MFA) is widely used today as an additional verification step often used in conjunction with a traditional login and password ....” EX1001, 2:20-23. EX1003, ¶89.

Thus, Kirti determines that additional verification is required to grant a client access to a cloud application or other network resource. That Kirti makes this determination is further shown by the fact that Kirti discloses performing the additional steps to authentication (additional verification). *Infra* Section VII.C.1.f) (mapping Element [1.8]-[1.11]). EX1003, ¶90.

**Coffin’s teachings**

To the extent Kirti’s remedial measures alone do not satisfy the claimed “additional verification,” a POSITA would have found it obvious to implement

Kirti's system with the specific types of measures taught by Coffin, thus satisfying these claim elements. EX1003, ¶91.

Coffin expressly discloses several types of additional verification for an Oracle system, including: a "second password or PIN," "a CAPTCHA," an "answer [to] personal questions," a "biometric scan[], like fingerprint, retina, or facial recognition," and "pass codes sent to [] e-mail, pager, or cell phone." EX1005, 177; *see also id.*, 178-208 (explaining how to implement some of these additional verification methods). Coffin also explains the benefits of this additional verification: it "assure[s] us that the person sitting at the keyboard is who they claim to be." *Id.*, 177. EX1003, ¶92.

Thus, to the extent Kirti does not render obvious implementing its system to require this additional authentication, a POSITA would have been motivated to do so in view of Coffin, which teaches use of this authentication to provide an added layer of security. *Supra* Section VII.C. A POSITA would have reasonably expected to succeed in implementing Coffin's additional verification teachings in Kirti's disclosed system for at least three reasons: (1) Kirti already discloses performing remedial actions and expressly mentions additional verification steps including one-time passwords (OTPs) (*e.g.*, EX1004, 3:53-4:1, 5:27-37, 5:55-6:34, 14:48-54, 14:61-67, 24:43-47, 24:66-67, 25:16-20, 25:34-52, 25:61-26:5, 28:22-36, FIGS. 5B, 6), (2) Coffin expressly teaches a POSITA how to implement at least some of the

additional verification methods (EX1005, 178-208), and (3) implementing this additional verification functionality in Kirti's disclosed system requires only minor software changes that were well within the skill of a POSITA. *E.g.*, *KEYnetik*, 2023 WL 2003932, at \*2; *see also supra* Section IV.B.2 (explaining that additional authentication was well known in the art). EX1003, ¶93.

e) **Elements [1.6]-[1.7]**

[1.6] 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

[1.7] 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,

Kirti teaches these claim elements. For example, Kirti teaches determining whether to require additional authentication steps using “analytics and security intelligence processes.” *E.g.*, EX1004, 24:67-25:5 (“process for remediating threats” “includes identifying (602) a threat”); *see also id.*, FIG. 6. These processes involve retrieving historic user login data from Kirti's analytics and threat repository database and using that information to detect “anomalous behavior” relative to “baseline user profiles over various periods of time.” *Id.*, 14:5-7, 24:33-50; *see also id.*, FIG. 5B (exemplary process for “detecting threats”), 3:53-4:1 (“detecting

patterns of suspicious activity” and “recommending remedial measures”), 14:5-14 (system “tracks user activity for anomalous behavior to detect attacks and unknown threats” and provides “recommendations for remediation”); *id.*, 28:22-36. EX1003, ¶94.

As explained above for element [1.3] (*supra* Section VII.C.1.c), the activity data stored in Kirti’s analytics and threat intelligence repository database (a multidimensional, time-series database) is historical at least because the database stores data collected over a relatively long time period (e.g., several weeks) and receives new data in batches (e.g., from the most recent 24-hour period). *E.g.*, EX1004, 4:54-59, 6:35-44, 11:15-58, 12:5-35, 12:50-57, 13:27-30, 14:46-15:16, FIGS. 8B-8D. Thus, even the most recent data in the database is historical. EX1003, ¶95.

And, as also explained above for element [1.3] (*supra* Section VII.C.1.c), the historical activity data stored in Kirti’s analytics and threat intelligence repository database includes information about previous access requests, such as “login and logout statistics (including attempts and successes)” (EX1004, 10:35-40), a timestamp (*e.g.*, EX1004, 12:35-54, 14:48-54, 16:49-60, 18:9-23), whether the request was successful (*e.g.*, *id.*, 10:34-44, 18:38-41), the device and/or IP address of the request (*e.g.*, *id.*, 10:34-44, 12:1-18, 12:35-13:29, 13:44-59, 16:28-40, 16:55-

67, 17:9-55, 18:17-23, 18:38-41), and what resources were accessed (*e.g.*, *id.*, 10:34-44, 12:7-18, 16:49-60, 18:17-23). *E.g.*, EX1004, FIG. 4 (step 406). EX1003, ¶96.

Kirti teaches its “Threat Detection and Prediction Analytics Application 212,” retrieves this past activity data from Kirti’s “Analytics & Threat Intelligence Repository 211” to detect threats. *E.g.*, EX1004, 18:10-14. Indeed, Kirti describes how its analytics tool (*e.g.*, threat detection and prediction analytics application 212) builds a baseline user profile based on data collected over time and stored in the analytics and threat intelligence repository, and uses this profile to detect anomalous login attempts (*e.g.*, in the most recent batch of data). For example, Kirti describes how “data collected over time is used to build models of normal behavior (*e.g.*, patterns of events and activity) and flag behavior that deviates from normal as abnormal behavior” (EX1004, 13:27-30), including behaviors related to “failed logins” (*id.*, 13:10-17). *See also id.*, 1:47-59 (“determining the likelihood of anomalous activity using the baseline user profile”), 1:66-2:18 (“the baseline profile is derived from activity data collected over a time period”), 2:37-51, 4:46-5:3 (“The aggregation of activity information in the analytics repository 211 concerning access patterns and other event statistics enables the system to establish baselines of user behavior.”), 5:46-54 (“The threat detection and prediction analytics application 212 can generate analytics .... Analytics may be performed using data stored in the analytics and threat intelligence repository 211.”), 14:5-14 (“a recommendation

engine tracks user activity for anomalous behavior to detect attacks and unknown threats” and provides “recommendations for remediation”); 14:27-31 (“[T]echniques such as outlier detection establish a baseline that is useful for detecting anomalous activities. Such anomalous activities along with contextual threat intelligence can provide more accurate prediction of threats with low prediction errors.”), 15:24-16:18 (describing detecting specific types of threats, including brute force attacks and describing how “[d]etection processes may track a user’s normal behavior and generate alerts when events or activities associated with the user’s account(s) deviate from the norm”), 19:61-24:47 (describing various “behavior analytics algorithms” for detecting “anomalous activity” in the user’s activity data to “determine the likelihood of various threats”), 29:23-27.

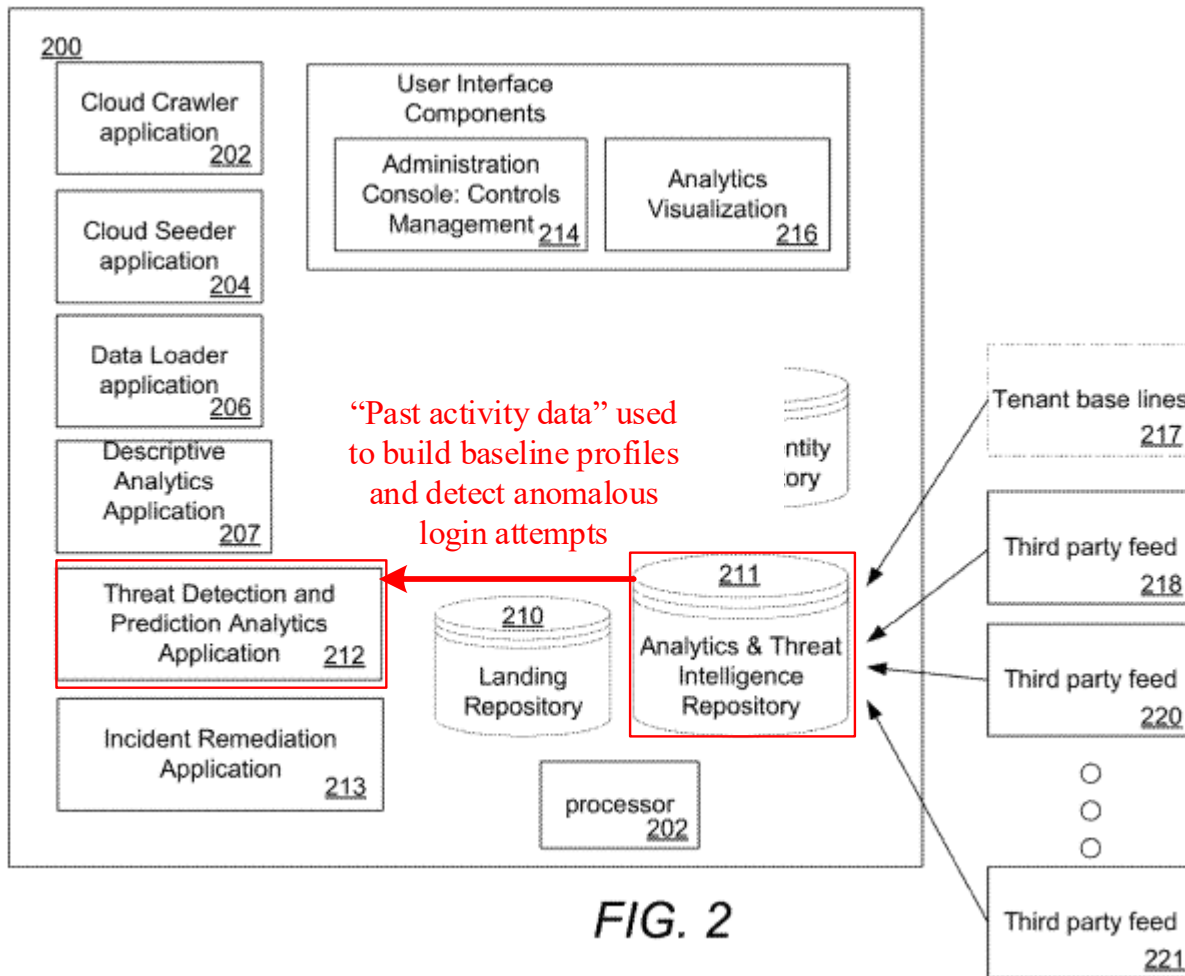
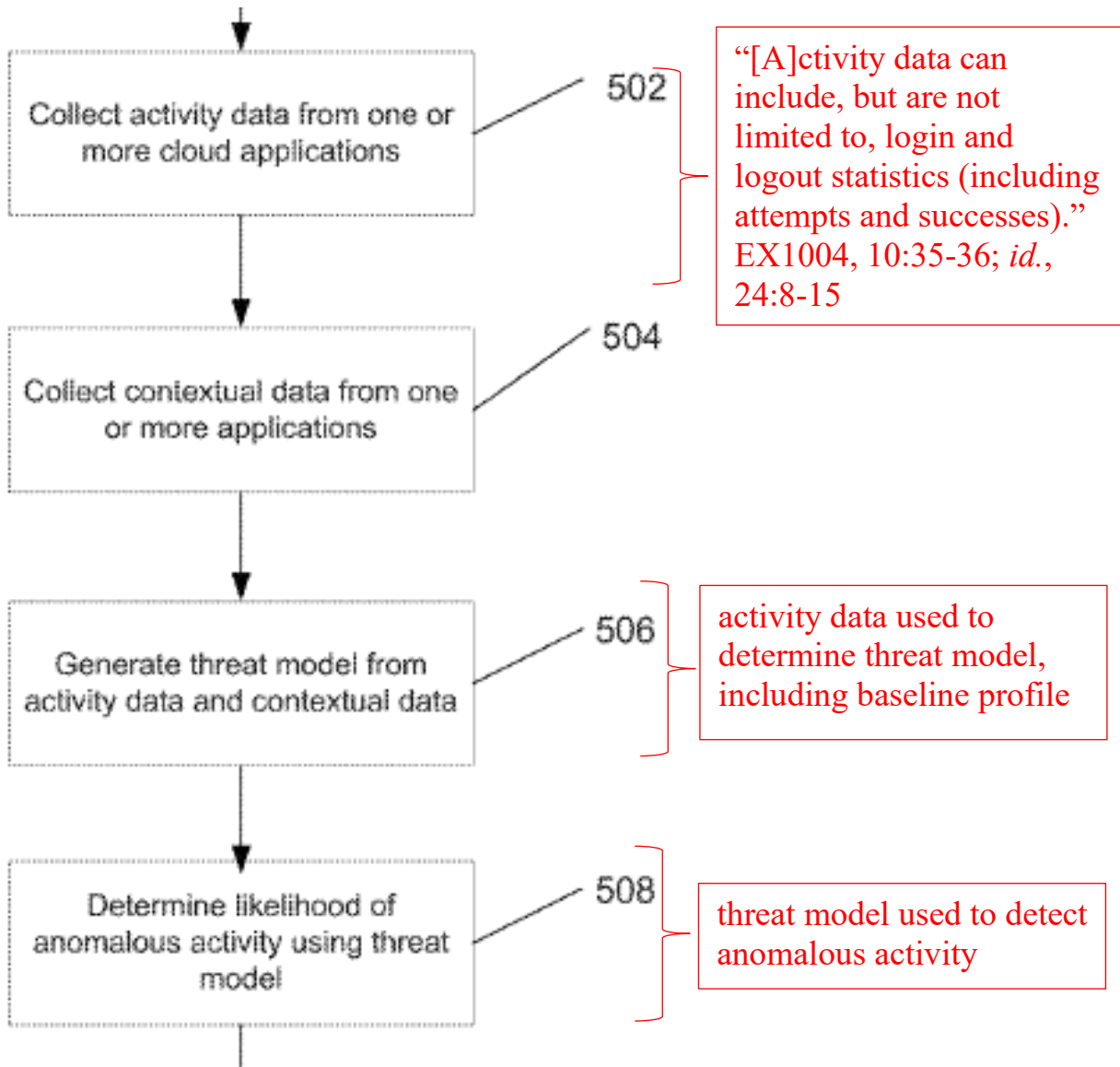


FIG. 2

EX1004, FIG. 2 (red annotations added). EX1003, ¶97.

Kirti (EX1004) FIG. 5B shows an exemplary process in which activity data is retrieved and used to generate threat models (step 506) that “include baseline user profiles over various periods of time.” EX1004, 24:33-38. These threat models are

then “used to determine (508) the likelihood of anomalous activity that may warrant additional verification.” *Id.*, 24:39-42.



EX1004, FIG. 5B (cropped and annotated in red); *see also id.*, FIG. 4 (showing process with step 406, “[s]tore activity data in analytics database,” and 410, “[g]enerate system reports and/or threat intelligence”); *id.*, 10:60-61 (“retrieved activity data is stored (406) in an analytics and threat intelligence repository database

211”); *id.*, 10:35-36 (“activity data can include, but are not limited to, login and logout statistics (including attempts and successes)”). EX1003, ¶98.

As shown in (EX1004) FIG. 5, Kirti teaches that its analyzer (e.g., threat detection and prediction analytics application 212) retrieves historic activity data from the Analytics and Threat Intelligence Repository 211, to “[d]iscover threats and risks.”

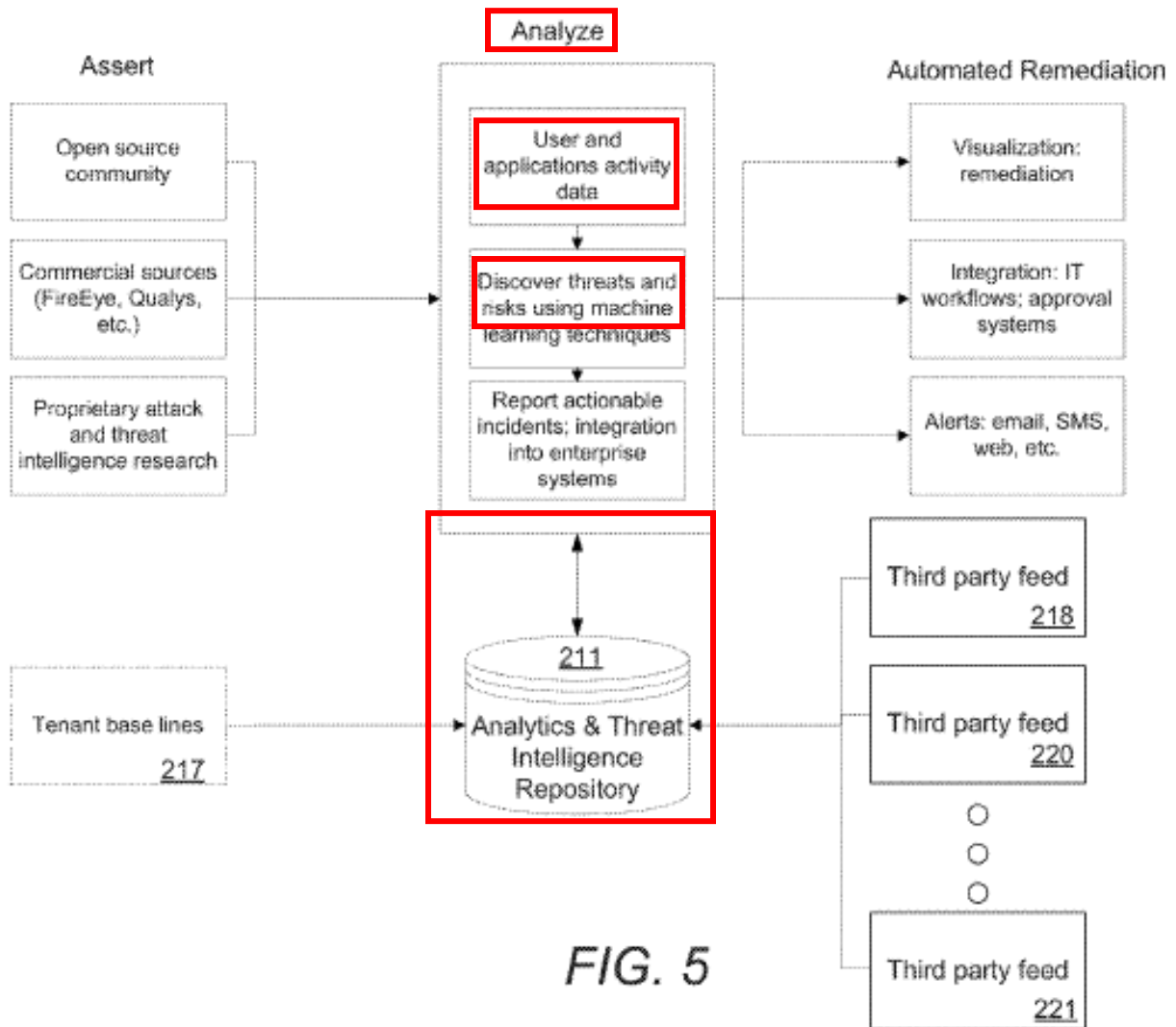


FIG. 5

EX1004, FIG. 5 (red annotations added); *see also id.*, Abstract, 1:44-59, 2:37-51, 3:53-4:3, 4:60-66 (“The aggregation of activity information in the analytics repository 211 concerning access patterns and other event statistics enables the system to establish baselines of user behavior. Machine learning techniques can then be applied to detect threats and provide recommendations concerning how to respond to threats.”), 5:25-37, 5:53-54, 5:55-6:5, 12:1-57. EX1003, ¶99.

The Kirti system thus satisfies the claimed **“retrieving ... historical information about previous access requests”** at least by its analytics and threat detection processes that retrieve a user’s historic login activity over time and then analyze that historical information to determine a baseline profile. *E.g.*, EX1004, 1:47-59, 2:37-51, 4:46-5:3, 5:46-54 (“The threat detection and prediction analytics application 212 can generate analytics .... Analytics may be performed using data stored in the analytics and threat intelligence repository 211.”), 29:23-27. EX1003, ¶100.

Kirti also teaches displaying anomalous access request in a historical report (e.g., to an administrator), further confirming that the anomalous access requests are *previous* access requests. *E.g.*, EX1004, 4:46-59, 6:35-44, 9:34-66, 11:15-58, 12:5-35, 12:50-57, 14:46-15:16, FIGS. 8B-8D. For example, FIG. 8C illustrates a report from October 26 that shows previous anomalous access requests (six failed logins and nine after hours accesses) on October 9.

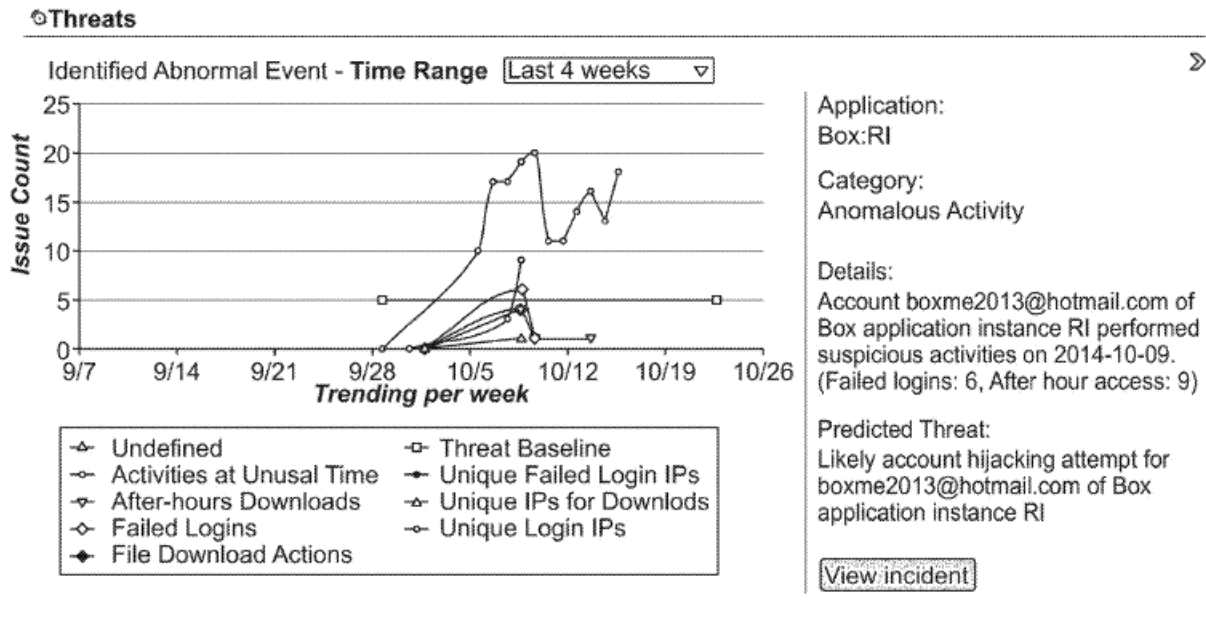


FIG. 8C

EX1004, FIG. 8C. EX1003, ¶101.

FIG. 8C (Cont.) also illustrates a report from October that indicates previous anomalous access requests (five failed logins, 12 suspicious IP addresses, four after hour accesses) on September 8. EX1004, FIG. 8C.

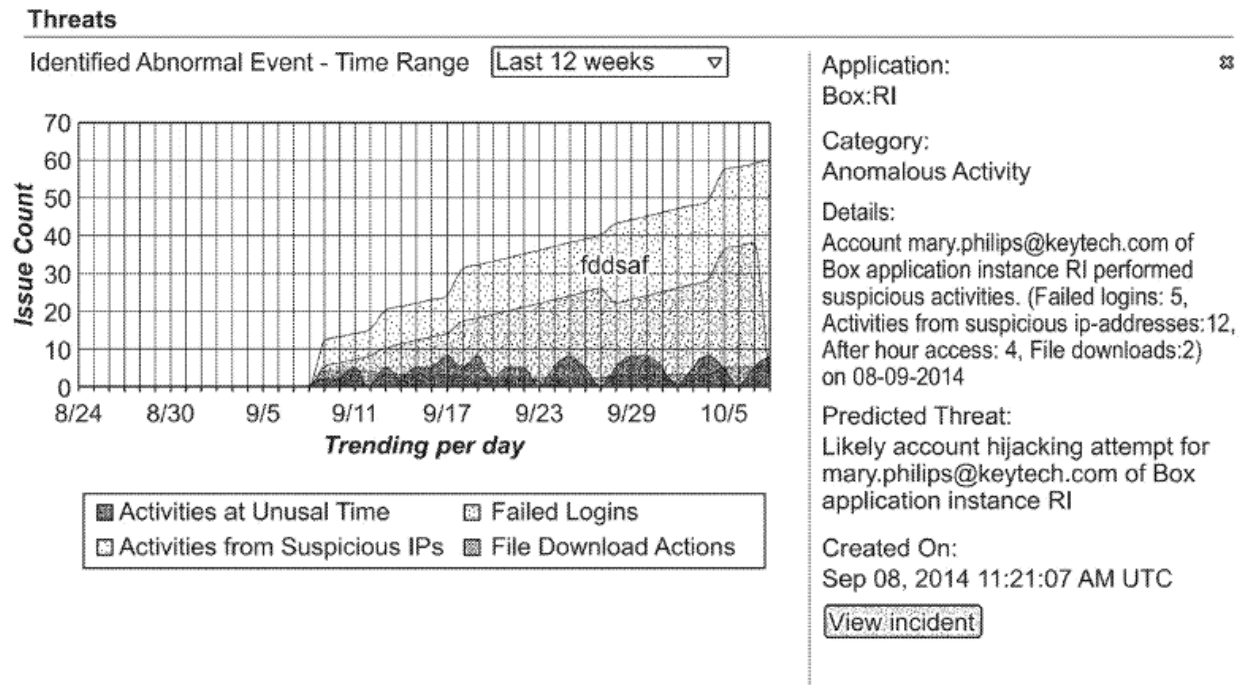


FIG. 8C (Cont.)

EX1004, FIG. 8C. EX1003, ¶102.

The Kirti system also satisfies the claimed “**determining ... whether the first user account is associated with a previous request to authenticate ... [that] comprised a second identifier not associated with the first user account**” at least because Kirti teaches determining whether a previous request originated from an IP address, geolocation, device and/or connection type that is not associated with the user account (e.g., a suspicious or blacklisted IP address) and requiring additional authentication if it did. EX1004, 1:66-2:7, 7:30-67 (Tables 1, 2), 9:60-65, 10:34-46, 12:7-57, 15:23-17:55, FIGS. 8A, 8C. EX1003, ¶103.

For example, the analytics application learns to identify, and account for, “where a user is or is expected to be, or how a user does or is expected to log in or access a cloud application (e.g., what type of device or connectivity)” based on the user’s historical activity data and contextual information, and develops a “baseline profile” for each user account that “includes a list of IP addresses” associated with the user account. *Id.*, 2:3-4, 16:28-32; *see also, e.g., id.*, 12:28-13:42, 14:20-31, 16:25-52. In turn, Kirti’s threat detection determines whether such identifiers for a given login request are not associated with the corresponding user account, as Kirti considers “IP address reputation data,” such as whether a request’s IP address is “suspicious,” “belongs to known anonymizer network,” and/or is on a “black-list.” *Id.*, 16:60-17:8. Thus, when these identifiers (e.g., IP address, geolocation, device type) deviate from what is expected or are associated with known security threats, the system may identify a potential threat. *Id.*, 3:58-4:3, 4:63-5:3, 5:25-37, 5:65-6:27, 12:28-13:42, 15:31-66, 16:53-18:7, 28:22-36. EX1003, ¶104.

For example, Kirti describes “an IP (Internet Protocol) hopping scenario,” which is detected by “geographic resolution (identifying or looking up a geographic location associated with an IP address)” and then “detect[ing] anomalous characteristics in the spatial data to predict threats.” *Id.*, 15:31-38. As another example, “[a]n unusual geolocation scenario may refer to activities being originated

in locations that are unexpected or outside of an established pattern.” *Id.*, 15:44-46.  
EX1003, ¶105.

Thus, Kirti teaches associating one or more IP addresses, geolocations, devices, and/or connectivity types with each user account. Within these associations, the user’s known IP addresses, geolocation, devices, and/or connectivity types serve as identifiers for the user’s account. Conversely, new, unknown, or suspicious IP addresses, geolocations, devices, and/or connectivity types are all identifiers not associated with the user account that may trigger additional authentication. EX1003, ¶106.

**f) Element [1.8]-[1.11]**

[1.8] based on the additional verification being required to grant access:

[1.9] select an additional verification method from a plurality of verification methods,

[1.10] cause the client to be prompted to complete the additional verification method, and

[1.11] determine whether the additional verification method has been completed correctly.

Kirti alone or in combination with Coffin teaches these claim elements. As explained above for elements [1.5]-[1.7] (*supra* Sections VII.C.1.d-VII.C.1.e), Kirti teaches recommending and performing a remedial action when a threat is detected and mentions that one such remedial action is “adding additional steps to

authentication,” i.e., requiring completion of an additional verification step (e.g., enter a one-time password). *E.g.*, EX1004, 5:27-37, 28:24-36. EX1003, ¶107.

Kirti discloses manually or automatically selecting which one of a plurality of remedial actions to use. *E.g.*, EX1004, 5:27-37, 5:55-57 (“embodiments of the invention may include remediation functions that provide manual and/or automated processes in response to threats.”), 6:10-14, 14:64-67, 25:15-20, 25:45-52, 27:10-12. EX1003, ¶108.

And Kirti further specifies that the selected remedial action is “performed.” *E.g.*, *id.*, 25:40-44 (“Remediation action(s) to address a threat may be performed automatically, if a response to such threats is predetermined, or may be instructed [] by a user selecting a remediation option from the alert that was presented.”). In the cases where the remedial action involved “additional steps to authentication,” such as a one-time password, performing that authentication would necessarily involve prompting the client to complete the additional authentication and then determining whether it was corrected completely. At the very least, this would have been obvious, as the most obvious way to perform such additional authentication would be to present the additional authentication steps for completion (i.e., “prompt”) and then confirm correct completion before allowing the login to complete. It was well known that these were necessary steps in any user-performed additional verification method

(e.g., biometric (face or fingerprint) scan, one-time passcode entry, answer to secret question, etc.). *Supra* Section IV.B.2. EX1003, ¶109.

**Coffin's teachings**

While Kirti teaches selecting and performing additional verification (e.g., “additional steps for authentication,” such as “elevated authentication or OTP validation”), it provides little implementation detail for these steps. To the extent a POSITA did not find these details obvious based on Kirti alone, they were obvious further in view of Coffin, which expressly teaches details for selecting one of a plurality of verification methods, prompting the user to complete the additional verification method, and determining whether the user correctly completed the additional verification method. EX1005, 177-208. Coffin provides these teachings in the context of an Oracle system, whereas Kirti is a patent assigned to Oracle, and reflects technology ultimately deployed as part of Oracle systems. EX1005, i, 1, 178; EX1004, Cover. EX1003, ¶110.

Coffin includes an entire chapter on implementing “Two-Factor Authentication.” EX1005, 177-208. Therein, Coffin teaches additional verification/authentication methods such as: a “second password or PIN,” “a CAPTCHA,” an “answer [to] personal questions,” a “biometric scan[], like fingerprint, retina, or facial recognition,” and “pass codes sent to [] e-mail, pager, or cell phone”). EX1005, 177. Coffin also explains how to implement additional

verification methods that include a passcode, such as an SMS to a phone, a URL to a pager, and an email to supporting devices. *Id.*, 178-208. EX1003, ¶111.

Coffin also teaches a heuristic for selecting an additional verification method from the plurality of passcode verification methods: select the user's pager and/or cell phone if these devices are available, otherwise select email. *E.g.*, EX1005, 183, 185, 200 (“By preference, [the system] will send the two-factor code to the user's pager and cell phone. If neither of those is available, [the system] will send the code to the user's e-mail.”), 201. It also was well known in the art to select an additional verification method from a plurality of verification method, for example, to ensure successful delivery of the additional verification based on the availability of the verification methods, cost, user preferences, etc. *Supra* Section IV.B.2. EX1003, ¶112.

Once the additional verification method is selected, Coffin teaches sending the passcode to the device(s), which then prompts the user to enter the provided passcode to complete the additional verification method. EX1005, 183 (“Once the user receives the two-factor pass code, they will submit that along with their request for data....”), 190, 193-194, 201, 207 (“Users will have to enter those 2-factor codes in order to get access to our application data.”). EX1003, ¶113.

The computer system then checks to ensure the user entered the correct code. EX1005, 194 (“[W]e test the two-factor code to see if it passes muster by calling the

f is cur cached cd function. If the two-factor code is good, we set the secure application role; however, if not we let them know by raising a NO DATA FOUND exception: they entered the wrong code, or perhaps just an old (older than 10 minutes) code.”), 201 (“[W]e want to cache [the code] for comparison to any code the user enters.”), 206 (“One definite potential error is the possibility that the user has entered a wrong or old code....”). EX1003, ¶114.

As explained above in Section VII.C, a POSITA implementing Kirti, which teaches additional authentication methods but without much detail, would have been motivated to incorporate Coffin’s detailed teachings on how to implement additional authentication methods. Given Kirti’s lack of detail on these aspects, a POSITA would have been motivated to look for implementation details elsewhere, naturally leading them to Coffin and its teachings on how to implement specific types of remedial measures in an Oracle database system. Coffin also expressly provides motivation for implementing the additional authentication: it ensures the user is who they say they are. EX1005, 177. EX1003, ¶115.

A POSITA would have reasonably expected success in implementing Coffin’s additional verification teachings in Kirti’s disclosed system at least because it would require only minor software changes that were well within the skill of a POSITA. *E.g.*, *KEYnetik*, 2023 WL 2003932, at \*2; *see also supra* Section IV.B.2 (explaining that additional authentication was well known in the art). The reasonable expectation

of success is further supported by the fact that both Kirti and Coffin relate to the same type of Oracle systems. EX1003, ¶116.

**2. Claim 2<sup>8</sup>**

[2.1] The computer system of claim 1, wherein determining whether the additional verification is required to grant access further comprises processing endpoint data from entities connected to the network.

Claim 2 is obvious at least because Kirti teaches the additional features recited by this dependent claim. As explained above for claims elements [1.5]-[1.7], Kirti teaches determining whether additional verification is required based on whether a threat (e.g., an anomalous access request) is detected in the past activity data. *Supra* Sections VII.C.1.d-VII.C.1.e. This involves processing endpoint data (e.g., “IP addresses,” “infected node points” and login information) from entities connected to the network (endpoints within the network). *E.g.*, *supra* Section VII.C.1.b; EX1004, FIGS. 4, 5B; *id.*, FIG. 1 (showing different endpoints). EX1003, ¶117.

For example, Kirti discloses that activity from suspicious IP addresses is a type of threat, and discloses identifying and including these suspicious IP addresses in a threat report to a system administrator. EX1004, 5:55-6:5, 10:34-46, 12:18-27, 12:35-57, 12:65-13:4, 15:38-59, 28:22-36, FIG. 8C. Kirti processes the “IP

---

<sup>8</sup> For each dependent claim mapped herein, Petitioner incorporates its analysis for any claim from which that dependent claim depends.

addresses ... [and] devices used to access the application” (*id.*, 10:36-38), and identifies suspicious nodes/IP addresses based on external intelligence feeds and/or login activity, such as a number of failed login attempts, login velocity, etc. *Id.*, 5:55-6:5, 12:18-27, 12:35-57 (“external information ... relating to potential security threats such as .... identification of infected node points ....”), 12:65-13:4, 15:38-59 (“Metrics used for detection can include ... a count of the number of unique IP addresses used by a user per day and/or a velocity ... [and] unusually high number of login failures for existing valid accounts ....”), 28:22-36. Further, Kirti discloses that “[a]ctivities from suspicious ip-addresses” is a type of threat that is reported to a system administrator. *Id.*, FIG. 8C.

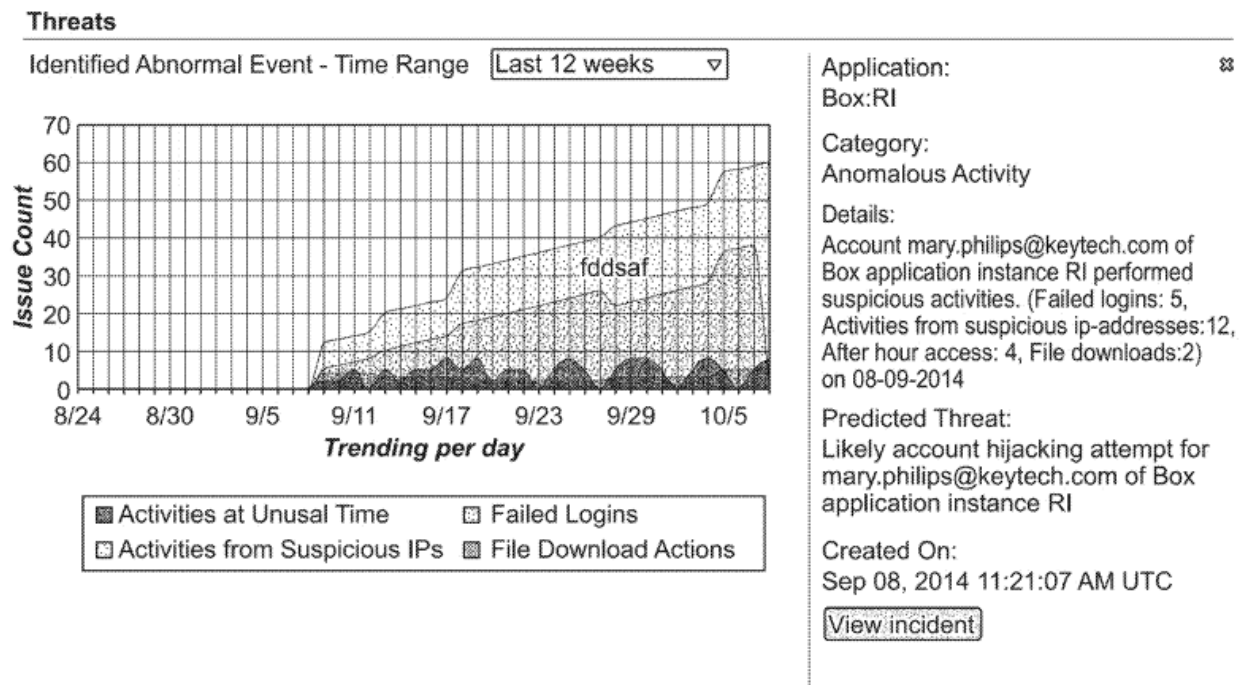


FIG. 8C (Cont.)

EX1004, FIG. 8C. EX1003, ¶118.

Thus, a POSITA would have understood or at least found it obvious that Kirti's system processes endpoint data from entities connected to the network at least because Kirti identifies endpoints ("nodes" / "IP addresses") that are suspicious. Further a POSITA would have understood or at least found it obvious that Kirti's system performs this processing of endpoint data when determining whether to require additional verification to grant access at least because Kirti teaches treating activity from suspicious endpoints as a threat, which, as explained above for elements [1.5]-[1.7] (*supra* Sections VII.C.1.d-VII.C.1.e), trigger the additional verification requirement. EX1003, ¶119.

### 3. Claim 3

[3.1] 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.

Claim 3 is obvious at least because Kirti teaches the additional features recited by this dependent claim. As explained above for claims elements [1.5]-[1.7], Kirti teaches determining whether additional verification is required based on whether a threat (e.g., an anomalous access request) is detected in the past activity data. *Supra* Sections VII.C.1.d-VII.C.1.e. Kirti further teaches that this threat detection involves processing an external threat intelligence feed: "Threats can also be identified by comparing activity data with external threat intelligence information, such as

information provided by third-party providers ....” EX1004, 4:67-5:3; *see also id.*, 5:55-6:5 (“[A]nalytics can utilize information received from external third party feeds ... to augment the threat intelligence by providing external information of security threats such as, but not limited to, identification of infected node points, malicious activity from a particular source IP address, malware infected email messages, vulnerable web browser versions, and known attacks on clouds.”), 11:51-58, 12:35-57, 12:65-13:4, 17:8-13. Thus, Kirti teaches processing information from an external threat intelligence feed (e.g., information indicating that the request came from an infected node), as part of determining whether to require additional verification. EX1003, ¶120.

#### 4. Claim 4

[4.1] The computer system of claim 1, wherein the second identifier is associated with a second user account, and wherein the second user account is different from the first user account.

Kirti teaches the additional features recited by this dependent claim. As described above for claim 1, the second identifier not associated with the first user account can be an unusual IP address, geolocation, and/or device. *Supra* Section VII.C.1.e. A POSITA would have understood or at least found it obvious that this second identifier is associated with a second user account in certain situations, such as where a second employee with lower-level permissions uses their normal computer to attempt to log in to a first employee’s account requiring higher-level

permissions (e.g., administrator's account) to download unauthorized content. Indeed, Kirti expressly discloses an “[i]nsider threat[.]” situation, such as one involving “a disgruntled internal employee.” EX1004, 15:60-16:11. In this situation, even if the disgruntled employee successfully guesses the administrator's credentials, a POSITA would have understood or at least found it obvious based on Kirti's teachings to flag the login as anomalous because the device, IP address, and/or geolocation is associated with the disgruntled employee's account (the second user account) not the administrator's account (the first user account). EX1003, ¶121.

## 5. Claim 5

[5.1] The computer system of claim 1, wherein the software instructions further comprise instructions that:

[5.2] based on the additional verification being required to grant access;

[5.3] determine that a probable cyberattack is detected, and

[5.4] provide an alert,

[5.5] wherein the alert includes the first identifier and an indicator that a probable cyberattack is detected, and

[5.6] wherein the alert is designated to be provided to an administrator of the network.

Claim 5 is obvious at least because Kirti teaches the additional features recited by this dependent claim. EX1004, 3:53-4:1, 4:54-59, 5:27-36, 13:12-17, 14:5-16:5, 25:3-44, 25:55-26:5, 28:22-37, FIGS. 6, 8B-8D. EX1003, ¶122.

Kirti teaches that based on the additional verification being required to grant access (e.g., due to a series of failed login attempts, a login attempt from an unknown/suspicious IP address, etc.), determining that a probable cyberattack (e.g.,

a brute force attack) is detected. *E.g.*, EX1004, 13:12-17, 14:5-7 (“detect[ing] attacks and unknown threats”), 15:31-48, 15:49-59 (“Detection [of a brute force attack] may involve evaluating the velocity of failed login attempts ...”). EX1003, ¶123.

Because Kirti discloses to “update statistics” “on various user behavioral activities” (EX1004, 18:28-31), a POSITA would have understood or at least found it obvious that if Kirti’s system determined that a user needs to supply additional verification information due to an anomalous login attempt in the most recent batch of activity data, such as an attempt from an unknown/suspicious IP address (*see supra* Sections VII.C.1.d-VII.C.1.e; EX1004, 1:66-2:7, 5:57-6:5, 12:28-57, 15:31-48, 16:6-11, 16:60-17:8, 28:26-31, 29:31-36, FIG. 8C), the system would also determine that a probable cyberattack is detected if that same user account is associated with other anomalies, such as repeated failed login attempts, especially since Kirti teaches to identify certain types of cyberattacks, including brute force attacks (*e.g.*, EX1004, 15:23-16:24). Thus, a POSITA would have understood or at least found it obvious based on Kirti’s teachings to determine, for example, that a probable brute force cyberattack is detected from a suspicious IP address based on that IP address being required to provide additional verification (because it is unknown/suspicious) and having failed multiple login attempts. EX1003, ¶124.

Kirti further discloses providing an alert to an administrator that includes the identifier (*e.g.*, username) and an indicator that a probable cyberattack is detected,

such as a category or description of the probable cyberattack. EX1004, 3:53-4:1, 4:54-59, 5:27-36, 13:12-17, 14:38-15:16, 15:63-65, 25:3-44, 25:55-26:5, 28:22-37, FIGS. 6, 8B-8D. For example, Kirti discloses to “preemptively alert a system administrator with respect to threats” (*id.*, 5:31-32; *see also id.*, 14:39-40, 25:25-30, 25:55-56) and describes and illustrates a system administrator user interface that displays alerts that include the user identifier (e.g., email) and an indicator that a probable cyberattack is detected. *Id.*, 6:35-44, 9:52-65, 14:46-15:16, FIGS. 2, 8B-8D. EX1003, ¶125.

For example, FIG. 8B illustrates an example of a list of alerts for several different user accounts (e.g., `boxme2013@hotmail.com`, `ralomari, ellen.schwab@keytech.com`) that include the alert category and the alert details.

| Incidents   |             |                                      |                    |                      |              |            |  |                  |        | Create New Incident  |
|---|-------------|--------------------------------------|--------------------|----------------------|--------------|------------|--|------------------|--------|--|
| Search Filter                                       |             |                                      |                    |                      |              |            |  |                  |        |  |
| ID  | Cloud App   | Category                             | Assigned to        | Created on           | Priority     | Status     |  |                  |        |  |
| <input type="text"/>                                | All         | All                                  | All                | <input type="text"/> | All          | Open       |  |                  |        |  |
| <input type="button" value="Search"/>               |             | <input type="button" value="Reset"/> |                    |                      |              |            |  |                  |        |  |
| ID  | Application | App Instance                         | Category           | Priority             | Assigned To  | Created On | Details  | Remediation Type | Status | Action   |
| 1020226   | Box         | RI                                   | Security Control   | High                 | i4qhckkju3fa | 2014-10-23 | Security level lower than recommended  | Manual           | Open   | <input type="button" value="edit"/> <input type="button" value="refresh"/> <input type="button" value="delete"/> |
| 1020200   | Box         | RI                                   | Security Control   | High                 | i4qhckkju3fa | 2014-10-23 | Security level lower than recommended  | Manual           | Open   | <input type="button" value="edit"/> <input type="button" value="refresh"/> <input type="button" value="delete"/> |
| 1020250   | Box         | RI                                   | Anomalous Activity | Medium               |              | 2014-10-23 | User Behavior Risk Related to Login Activity: Observed for boxme2013@hotmail.com of Box Application and Instance RI on 2014-10-24          | Manual           | Open   | <input type="button" value="edit"/> <input type="button" value="refresh"/> <input type="button" value="delete"/> |
| 1020275   | Box         | RI                                   | Anomalous Activity | High                 | i4qhckkju3fa | 2014-10-20 | Account boxme2013@hotmail.com of Box application instance RI performed suspicious activities   | Manual           | Open   | <input type="button" value="edit"/> <input type="button" value="refresh"/> <input type="button" value="delete"/> |
| 1020300   | Box         | RI                                   | Anomalous Activity | High                 | i4qhckkju3fa | 2014-10-20 | Account boxme2014@hotmail.com of Box application instance RI performed suspicious activities   | Manual           | Open   | <input type="button" value="edit"/> <input type="button" value="refresh"/> <input type="button" value="delete"/> |
| 2840001   | AWS         | aws_inst                             | Anomalous Activity | High                 | i4qhckkju3fa | 2014-10-20 | Account ralomari of AWS application instance aws_inst performed suspicious activities  | Manual           | Open   | <input type="button" value="edit"/> <input type="button" value="refresh"/> <input type="button" value="delete"/> |
| 1020105   | SFDC        | RI                                   | Anomalous Activity | High                 | Support      | 2014-10-09 | Account ellen.schwab@keytech.com of SFDC application instance RI performed suspicious activities   | Manual           | Open   | <input type="button" value="edit"/> <input type="button" value="refresh"/> <input type="button" value="delete"/> |
| 12830108  | SFDC        | RI                                   | Anomalous Activity | High                 | Admin        | 2014-10-09 | User Behavior Risk Related to Mass Delete, Transfer, or Export: Observed for edward.murali@keytech.com of SFDC Application and Instance RI | Manual           | Open   | <input type="button" value="edit"/> <input type="button" value="refresh"/> <input type="button" value="delete"/> |
| User Behavior Risk Related to Manage Users Changes: |             |                                      |                    |                      |              |            |  |                  |        |  |

FIG. 8B

EX1004, FIG. 8B. EX1003, ¶126.

FIG. 8C illustrates “[I]ikely account hijacking attempt[s]” for two users: boxme2013@hotmail.com and mary.philips@keytech.com.

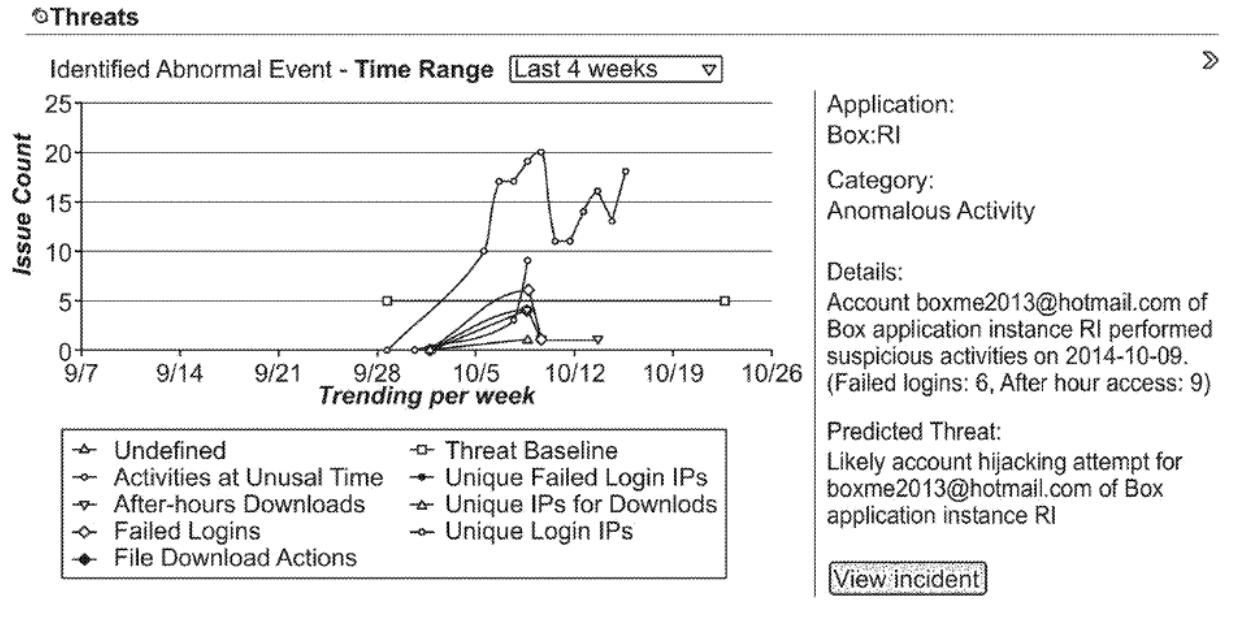


FIG. 8C

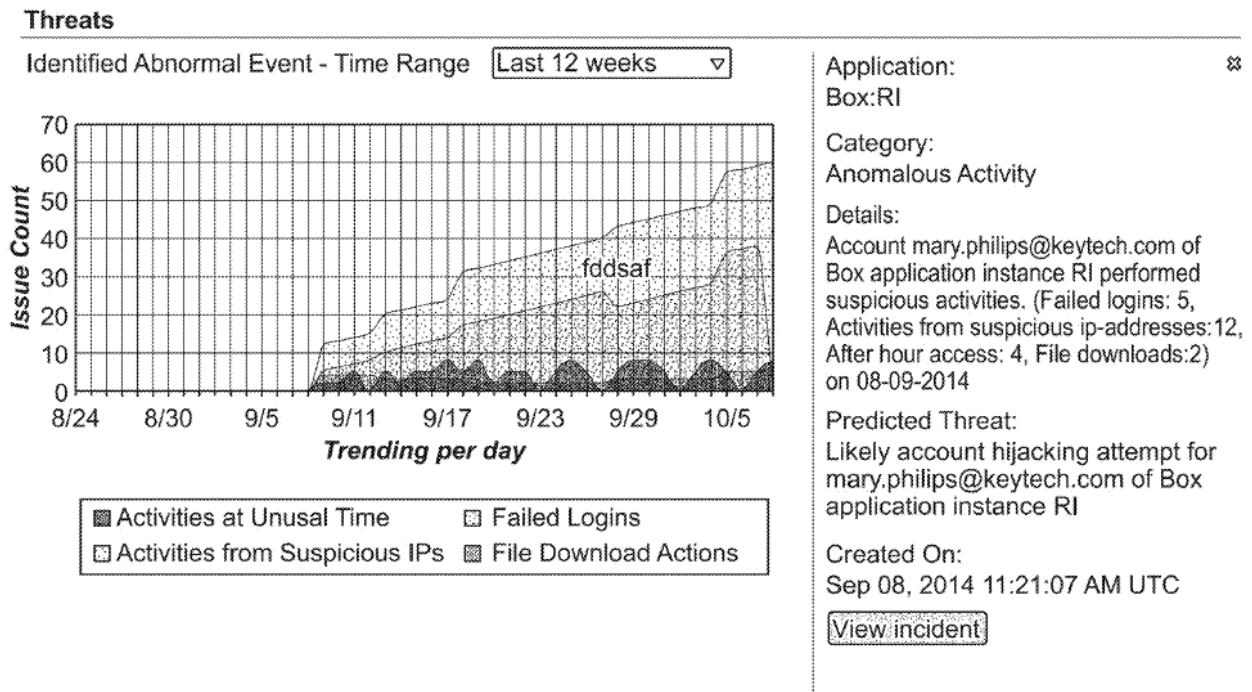


FIG. 8C (Cont.)

EX1004, FIG. 8C. EX1003, ¶127.

Similarly, FIG. 8D illustrates a list of alerts that each include the associated username and a description of the alert. For example, for user boxme2014@hotmail.com the alert is for suspicious activities—six failed login attempts.

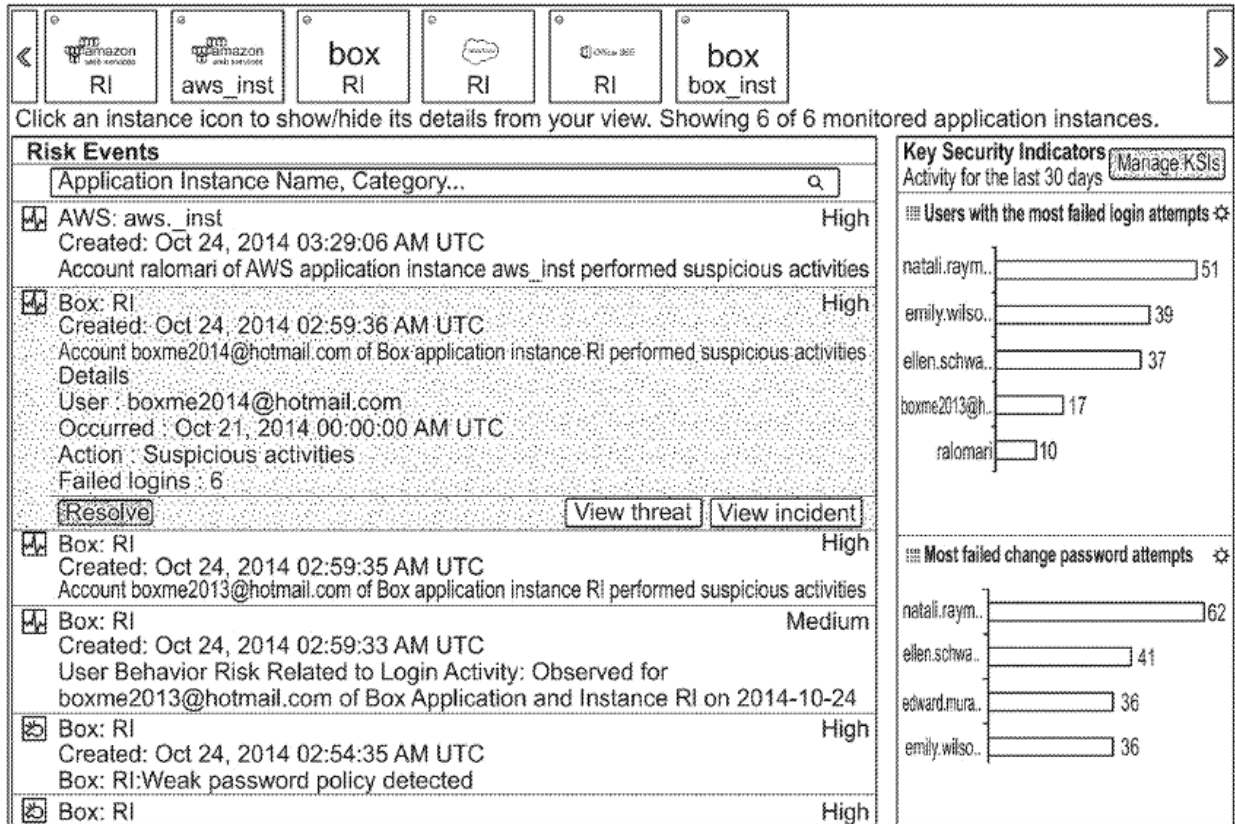


FIG. 8D

EX1004, FIG. 8D. EX1003, ¶128.

Kirti’s detailed description further explains that the alerts “can include information about the detected event such as, but not limited to an event identifier, date, time, risk level, event category, user account and/or security controls associated with the event, cloud application associated with the event, description of the event,

remediation type (e.g., manual or automatic), and/or event status (e.g., open, closed).” EX1004, 14:48-54. EX1003, ¶129.

**6. Claim 6**

[6.1] The computer system of claim 5, wherein the alert further includes an indication of where the probable cyberattack may have originated.

Claim 6 is obvious at least because Kirti teaches the additional features recited by this dependent claim. Specifically, Kirti teaches that the alert further includes an indication of where the probable cyberattack may have originated at least because Kirti discloses recording the IP address from which each access request was received, checking the IP addresses’ reputation (e.g., whether it is on a watch list), and recommending a remedial action if an anomaly is detected from that IP address (e.g., the IP address matches a blocked IP address or an IP address on a watch list, the IP address has suspicious activity such as a high volume of failed logins, etc.). EX1004, 3:58-4:1, 7:3-67, 9:60-65, 10:34-44, 12:7-18, 12:35-57, 12:64-13:2, 13:40-59, 15:31-43, 16:6-11, 16:55-17:55, 18:19-23, 18:38-42, 28:22-36, FIG. 8C (“Activities from suspicious ip-addresses”). EX1003, ¶130.

The system tracks the IP addresses associated with the requests at least because the activity data includes this information. “Activity data can include ... [the] IP addresses used to access the application.” EX1004, 10:33-37; *see also id.*, 18:38-42. Indeed, Kirti teaches “display[ing] high-level information such as a map

of IP addresses of user accounts associated with the tenant's account that have accessed cloud applications." *Id.*, 9:61-63; *see also id.*, FIG. 8A (suggesting a list of "Regular, Suspicious & Unknown Verified IPs"). EX1003, ¶131.

At least some of the threats (e.g., cyberattacks) that Kirti teaches detecting include an indication of where the detected threat originated (e.g., the IP address, geolocation). For example, "a threat can be identified based on an account accessing one or more files or failing a series of login attempts from an IP address that is flagged (by a third party feed or otherwise) as malicious." EX1004, 12:66-13:2; *see also, e.g., id.*, 6:3-4 ("identification of infected node points, malicious activity from a particular source IP address"), 12:41, 28:26-31. In these examples, POSITAs would have understood the account or IP address as the origination of the cyberattack. EX1003, ¶132. As another example, an application misuse threat is detected if the user logs in and performs suspicious activity from an unusual IP address or geolocation. EX1004, 16:6-11 ("Application misuse is a scenario that may include ... a malware-infected device performing an unusual number of file downloads/uploads using valid credentials but an unusual geolocation or IP address."). EX1003, ¶132.

Further, Kirti expressly discloses that the external intelligence feeds inform the system of the "source of attacks" (EX1004, 12:49), and the reports displayed to administrators include "login statistics (e.g., users with the most failed logins, IP

address based login history including consideration of IP reputation, geolocation, and other factors).” *Id.*, 12:7-11. EX1003, ¶133. Given this, POSITAs would have naturally implemented Kirti to provide this helpful and readily available information in the alert to beneficially allow the individuals or systems receiving the alert to better carry out any needed responsive action. EX1003, ¶133.

Thus, a POSITA would have understood or at least found it obvious that the alert includes an indication of where the probable cyberattack may have originated at least because Kirti tracks the IP addresses, detects IP address-based threats, and provides an administrator with information about specific IP addresses. EX1003, ¶134.

7. **Claim 7**

[7.1] The computer system of claim 5, wherein the alert further includes an indication of what enterprise information may be at risk in the probable cyberattack.

Claim 7 is obvious at least because Kirti teaches the additional features recited by this dependent claim. Specifically, Kirti teaches that the alert further includes an indication of what enterprise information may be at risk in the probable cyberattack at least because Kirti teaches tracking the resources the user accesses and generating an alert when the user accesses or downloads certain information, such as credit card numbers. EX1004, 10:34-44, 14:5-14, 15:60-16:5. EX1003, ¶135.

For example, the activity data includes the “cloud resources that were accessed (including, but not limited to, files and folders in a file management cloud application ... employees and contractors in a human resource cloud application ... and contacts and accounts in a customer relationship management cloud application ...).” EX1004, 10:38-44. EX1003, ¶136.

Further an alert is generated for certain high-risk operations, such as “downloading a file containing credit card numbers, copying encryption keys, elevating privileges of a normal user.” EX1004, 14:11-13. Other activities that Kirti teaches tracking include “an unusually high use of corporate resources such as a high number of downloads and/or an employee with a low rating downloading or sharing an unusually high number of files/folders, deleting code from a source code control system, or downloading, deleting, or modifying customer information/contracts.” *Id.*, 15:66-6:5. EX1003, ¶137.

Thus, a POSITA would have understood or at least found it obvious that the alert includes an indication of what enterprise information may be at risk in the probably cyberattack at least because Kirti teaches tracking the enterprise information accessed by the user and flagging suspicious activity, such as downloads. EX1003, ¶138.

8. Claim 8

[8.1] The computer system of claim 5, wherein the alert further includes predictive information.

Kirti teaches that the alerts include predictive information at least because Kirti expressly discloses displaying predicted threats, including as part of an alert, such as a likely account hijacking. EX1004, 1:44-47, 4:54-59, 5:44-50, 12:28-35, 12:58-13:42, 14:29-31, 17:8-43, 18:10-13, 21:59-61, 24:25-29, FIGS. 8A, 8C. Specifically, Kirti discloses that “[t]he data concerning activity information in the analytics repository 211 can be utilized to generate reports that may be presented visually to a system administrator via a user interface and to generate analytics for determining threat level, detecting specific threats, and *predicting potential threats*.” EX1004, 4:54-59 (emphases added). As shown in FIG. 8A, for example, “the dashboard view can display high-level information such as a map of IP addresses of user accounts associated with the tenant's account that have accessed cloud applications, number of risk alerts and *predicted threats*, number of inactive and active users, number of open and closed incidents, etc.” EX1004, 9:60-65 (emphases added).

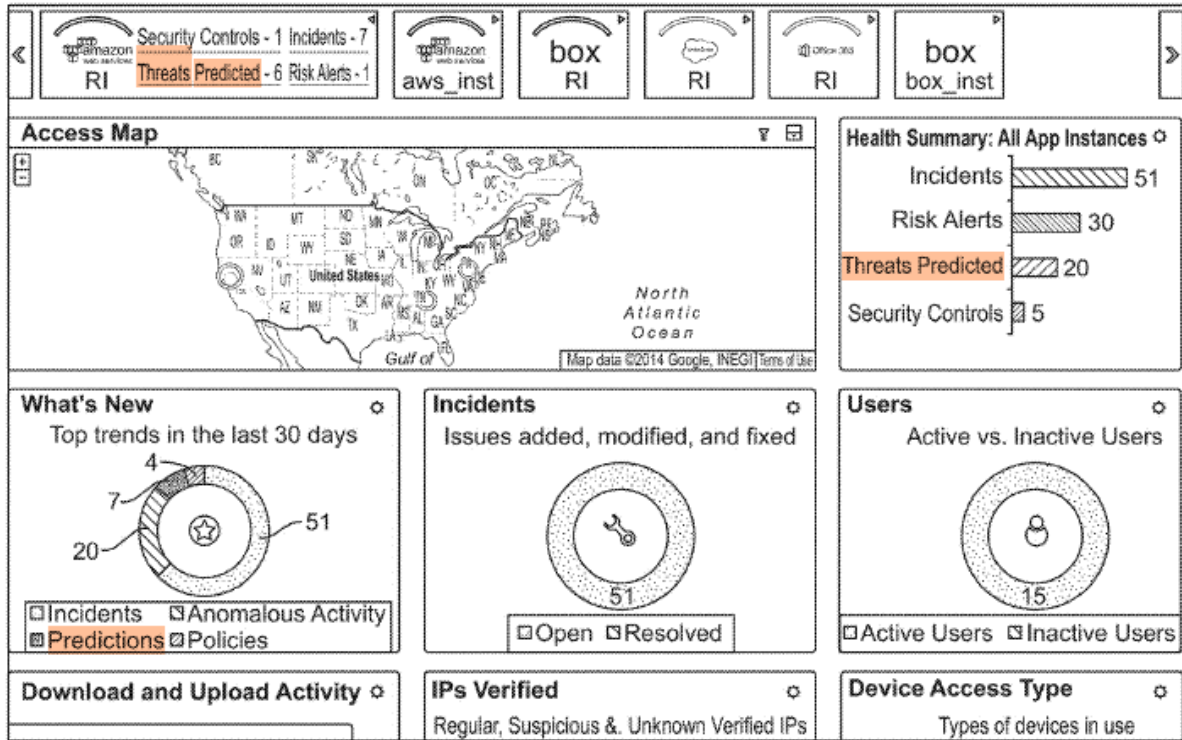


FIG. 8A

EX1004, FIG. 8A (orange annotations added). EX1003, ¶139. FIG. 8C shows an example alert that includes a predicted threat comprising a “[l]ikely account hijacking attempt.” *Id.*, FIG. 8C.

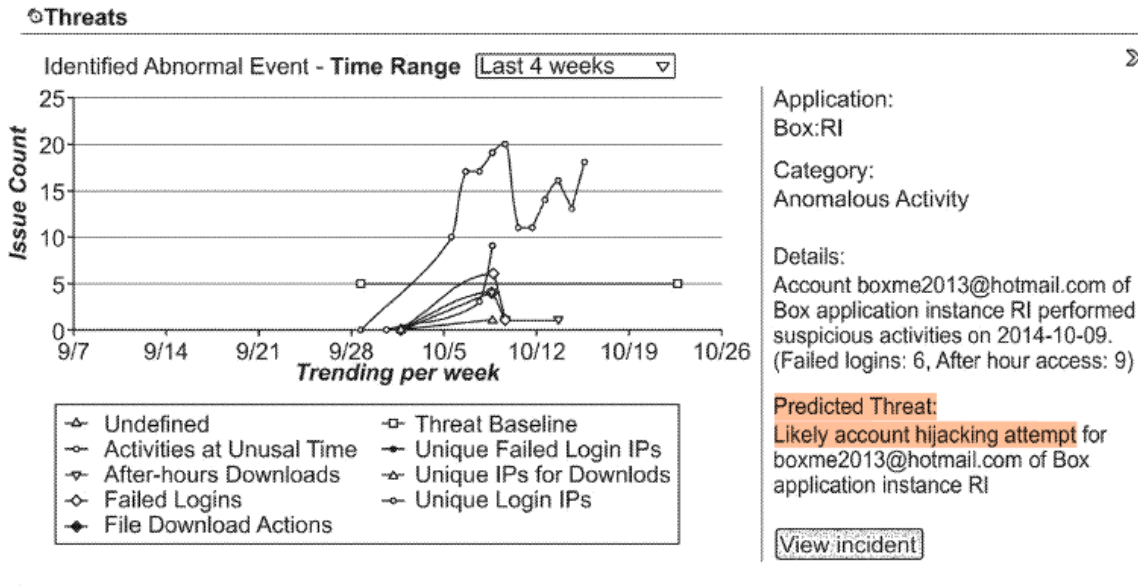


FIG. 8C

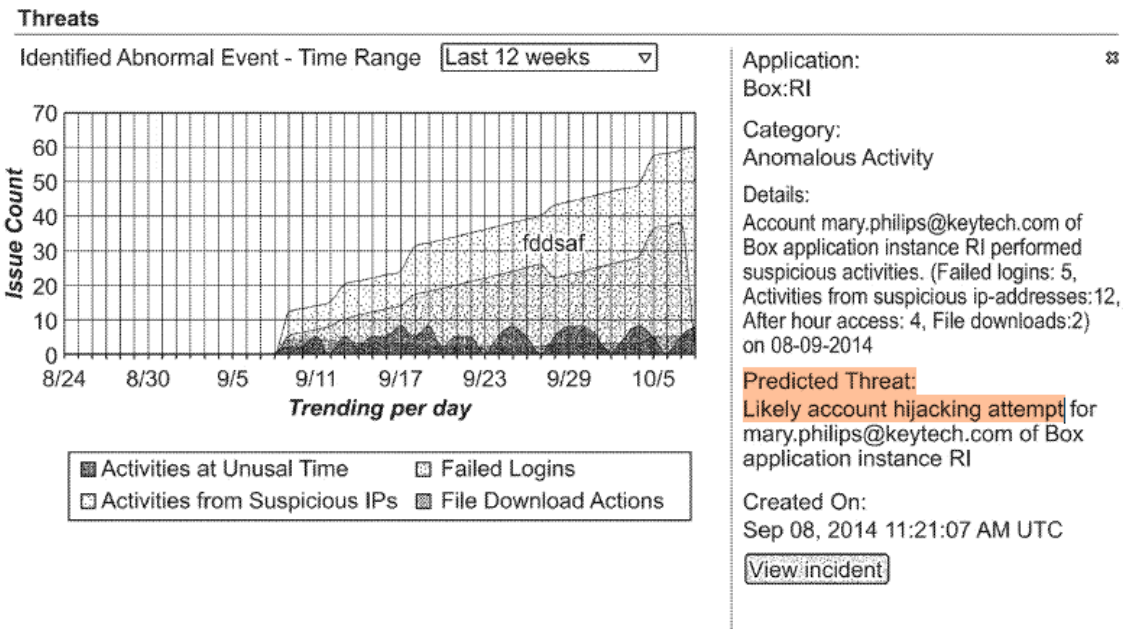


FIG. 8C (Cont.)

FIG. 8C (orange annotations added). EX1003, ¶140.

**9. Claims 9-16**

Claims 9-16 are method claims that recite elements identical or near-identical to those of system claims 1-8, respectively, and are obvious for the same reasons as claims 1-8. *See* EX1065 (claims listing, showing claims 1-8 and 9-18 in columns 1 and 2, respectively); *supra* Sections VII.C.1–VII.C.8; EX1003, ¶141.

**10. Claims 17-18**

Claims 17-18 are method claims that recite elements identical or near-identical to those of system claims 5 and 8, respectively, but depend from dependent claim 12, which recites elements identical or near-identical to those of system claim 4. Thus, claims 17-18 are obvious for the same reasons as claims 4, 5 and 8. *See* EX1065 (claims listing, showing claims 4, 5 and 8, and 17-18 in columns 1 and 2, respectively); *supra* Sections VII.C.4, VII.C.5, VII.C.8; EX1003, ¶142.

**11. Claims 19-21 And 23-25**

Claims 19-21 and 23-25 are substantively identical to claims 1-3 and 5-7, respectively, and are obvious for the same reasons as claims 1-3 and 5-7. *See* EX1065 (claims listing, showing claims 1-3 and 5-7, and 19-21 and 23-25 in columns 1 and 3, respectively); *supra* Sections VII.C.1–VII.C.3, VII.C.5-VII.C.7; EX1003, ¶143.

**12. Claims 26-28 And 30**

Claims 26-28 and 30 are method claims that recite elements identical or near-identical to those of system claims 1-3 and 5, respectively, and are obvious for the same reasons as claims 1-3 and 5. *See* EX1065 (claims listing, showing claims 1-3 and 5-7, and 19-21 and 23-25 in columns 1 and 4, respectively); *supra* Sections VII.C.1–VII.C.3, VII.C.5; EX1003, ¶144.

**VIII. NO OBJECTIVE INDICIA OF NON-OBVIOUSNESS**

Petitioner is not aware of any evidence of objective indicia of non-obviousness having a nexus to the challenged claims.

**IX. CONCLUSION**

Based on the Grounds presented herein, Petitioner respectfully requests that the Board institute IPR of claims 1-21, 23-28, and 30 of the '426 patent.

Respectfully submitted,

Dated: December 30, 2025

By: /Andrew M. Mason/

Andrew M. Mason, Reg. No. 64,034  
andrew.mason@klarquist.com  
KLARQUIST SPARKMAN, LLP  
One World Trade Center, Suite 1600  
121 S.W. Salmon Street  
Portland, Oregon 97204  
Tel: 503-595-5300  
Fax: 503-595-5301

Counsel for Petitioner

**CERTIFICATE OF COMPLIANCE WITH  
TYPE-VOLUME LIMITATION PURSUANT TO 37 C.F.R. § 42.24**

This brief complies with the type-volume limitation of 37 C.F.R. § 42.24(a)(1)(i).

The brief contains 11,611 words, excluding the parts of the brief exempted by 37 C.F.R. § 42.24(a).

The brief has been prepared in a proportionally spaced typeface using Microsoft Word for O365 in a 14-point Times New Roman font.

Dated: December 30, 2025

By: /Andrew M. Mason/

Andrew M. Mason, Reg. No. 64,034  
andrew.mason@klarquist.com  
KLARQUIST SPARKMAN, LLP  
One World Trade Center, Suite 1600  
121 S.W. Salmon Street  
Portland, Oregon 97204  
Tel: 503-595-5300  
Fax: 503-595-5301

Counsel for Petitioner

**CERTIFICATE OF SERVICE  
IN COMPLIANCE WITH 37 C.F.R. § 42.6(e)(4)**

The undersigned certifies that the **PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 12,231,426 and EXHIBITS 1001–1012, 1014-1044, 1048-1055, 1057-1063, and 1065-1066** were served on December 30, 2025, via **Express Mail** on the Patent Owner at the following address of record as listed on the USPTO Patent Center:

Brian Galvin  
Galvin Patent Law LLC  
2916 NW Bucklin Hill Road, Suite 485  
Silverdale, WA 98383

By: /Andrew M. Mason/  
Andrew M. Mason, Reg. No. 64,034  
andrew.mason@klarquist.com  
KLARQUIST SPARKMAN, LLP  
One World Trade Center, Suite 1600  
121 S.W. Salmon Street  
Portland, Oregon 97204  
Tel: 503-595-5300  
Fax: 503-595-5301

Counsel for Petitioner