SHOOK, HARDY & BACON L.L.P.
Gary Miller (Appearance *Pro Hac Vice*)
gmiller@shb.com
111 S. Wacker Drive, 51st Floor
Chicago, Illinois 60606
Telephone: 312-704-7700
Facsimile: 312-558-1195

Jesse J. Camacho (Appearance *Pro Hac Vice*)
jcamacho@shb.com
Ryan Dykal ((Appearance *Pro Hac Vice*))
rdykal@shc.com
Mary J. Peal (Appearance *Pro Hac Vice*)
mpeal@shb.com
2555 Grand Boulevard
Kansas City, Missouri 64108
Telephone: 816-474-6550
Facsimile: 816-421-5547

Janet L. Hickson (SBN: 198849)
jhickson@shb.com
Mayela C. Montenegro (SBN: 304471)
mmontenegro@shb.com
5 Park Plaza, Suite 1600
Irvine, California 92614
Telephone: 949-475-1500
Facsimile: 949-475-0016

Attorneys for Plaintiff
TELESIGN CORPORATION

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA – SAN FRANCISCO DIVISION

TELESIGN CORPORATION, Plaintiff, v. TWILIO INC., Defendant.	Case No. 3:18-cv-03279-VC **TELESIGN'S FIRST CONSOLIDATED COMPLAINT** **JURY TRIAL DEMANDED**

Contents

I. Procedural History

1. TeleSign Corporation ("TeleSign") initially filed suit against Twilio Inc. ("Twilio) in the Central District of California on April 30, 2015 in case no. 2:15-cv-03240-PSG-SS ("*TeleSign I*"), which was stayed on March 9, 2016 pending *inter partes* review.

2. TeleSign filed a second lawsuit on a related patent against Twilio in the Central District of California on March 28, 2016 in case no. 2:16-cv-02106-PSG-SS ("*TeleSign II*") , which was consolidated with *TeleSign I* and stayed on May 16, 2017 pending *inter partes* review.

3. At the completion of the IPR proceedings, the Central District Court reopened the consolidated case on April 13, 2018, but scheduled a case management conference for July 30, 2018, indicating discovery was not yet open.

4. Because the law on venue had changed, TeleSign did not oppose Twilio's motion to transfer the consolidated case to the Northern District of California, which was granted on May 30, 2018. Plaintiff TeleSign files this First Consolidated Complaint for patent infringement against Defendant Twilio, and on information and belief alleges as follows:[1]

II. Introduction and Parties

5. TeleSign is an industry leader in internet security and user authentication. TeleSign is one of the fastest-growing technology companies in North America, sells to some of the top websites in the world, and is a market leader in two-step-verification technology.

6. TeleSign helps its customers secure billions of end-user accounts worldwide and prevent registration fraud.

7. The technology offered by TeleSign gives businesses the ability to connect a unique identity with every account to verify new registrations and authenticate users. TeleSign helps businesses detect suspicious users and better protect their existing user base from account compromise. TeleSign is trusted by some of the world's largest companies to help prevent fraudulent accounts and stop account takeovers.

[1] Headings are included for readability; the allegations under any given heading are not intended to relate solely to that heading and vice versa. All allegations may be applicable to any Section, Count, or request (and each is incorporated by reference into the other).

8. TeleSign owns United States Patent No. 7,945,034 (the "'034 Patent"), entitled "Process for determining characteristics of a telephone number," and Nos. 8,462,920 (the "'920 Patent"), 8,687,038 (the "'038 Patent"), and 9,300,792, all three entitled "Registration, verification and notification system" (collectively, the "Asserted Patents").

9. Twilio competes directly with TeleSign.

10. Twilio has used, and continues to use, TeleSign's patented technology in connection with products and services that Twilio makes, sells, offers for sell and/or uses without TeleSign's permission, causing TeleSign irreparable harm.

11. In this suit, TeleSign asks the Court to enjoin Twilio from making, using, selling or offering to sell products and services claimed by the Asserted Patents and to award monetary relief for Twilio's past violations.

12. Plaintiff TeleSign is a California corporation, duly authorized to do business in the State of California, with its principal place of business in Marina Del Rey, California.

13. As explained herein, Twilio's infringement has harmed TeleSign. Without authorization, Twilio has made, sold, offered to sell, used and/or imported products and services that infringe TeleSign's patents, and has induced others to infringe TeleSign's patent rights.

14. Since Twilio's initial public offering, it reportedly has a market capitalization over $1 billion.

15. Over 1,000,000 developer accounts have registered with Twilio's platform.

16. Twilio's offerings consist of at least a Programmable Communications Cloud which enables developers to embed voice, messaging, video, and authentication capabilities into developers' applications via Twilio's Application Programming Interfaces ("APIs").

III. Jurisdiction and Venue

17. This is an action for patent infringement arising under the patent laws of the United States, 35 U.S.C. § 1 et seq., including §§ 271 and 281. This Court has original jurisdiction over this patent-infringement action under 28 U.S.C. §§ 1331 and 1338(a).

18. Twilio maintains its principal place of business in San Francisco, California.

19. Twilio is a Delaware corporation with its principal place of business at 375 Beale Street, 3rd Floor, San Francisco, California 94105.

20. Twilio is subject to personal jurisdiction in the State of California and in this Court.

21. Venue is proper in the Northern District of California under 28 U.S.C. § 1400(b).

22. Twilio is responsible for acts of infringement occurring in the Northern District of California. For example, as alleged herein, Twilio has delivered or caused to be delivered infringing products or services in the Northern District of California, has induced persons in this district to infringe TeleSign's patent, is doing business in this district, recruits personnel from this district, employs employees from this district, seeks to employ persons from this district, advertises and markets its products and services in this district, seeks to sell its products and services to residents of this district (including via its website at www.twilio.com), and hosts seminars or shows in this district.

IV. TeleSign and Twilio are Competitors.

23. Twilio offers products and services that are similar to TeleSign's products and services.

24. TeleSign and Twilio both offer two-factor-authentication technology, notification technology to let users know of potentially fraudulent activity, and technology to help prevent fraudulent website registrations.

25. Twilio and TeleSign directly compete for customers and potential customers.

26. For example, in 2015, Twilio began increasing publicity of its phone verification services (*e.g.*, its "Lookup" technology) in direct competition with TeleSign.

27. TeleSign and Twilio market their products using the same or similar channels.

28. TeleSign and Twilio regularly meet or interact with the same customers and potential customers on sales calls and during in-person meetings.

29. Customers have compared and considered using TeleSign and Twilio to provide

services they need.

30. Twilio has told users it was developing technology intended to provide the same features as TeleSign's technology.

31. Users have compared prices of TeleSign's technology to prices of Twilio's technology.

32. TeleSign has suffered price erosion, lost customers, lost goodwill and other harm due to Twilio's infringement of the Asserted Patents.

33. Media reports and third parties consider Twilio and TeleSign as competitors and providers of similar technologies, such as SMS technology and two-factor-authentication technology.

34. Users consider Twilio and TeleSign as competitors.

35. Twilio seeks to take customers from TeleSign.

36. TeleSign sought a preliminary injunction in *TeleSign I* due to harm caused by Twilio's infringement of U.S. Patent No. 7,945,034. *See TeleSign I*, ECF No. 23.

V. The Asserted Patents

37. Collectively, the Asserted Patents are the '034, '920, '083, and '792 patents.

38. The United States Patent and Trademark Office issued the '034 Patent (attached as Exhibit A) on May 17, 2011, the '920 Patent (attached as Exhibit B) on June 11, 2013, the '038 Patent (attached as Exhibit C) on April 1, 2014; and the '792 patent (attached as Exhibit D) just after 12:00 AM ET on March 29, 2016, from U.S. Patent Application Serial No. 14/678,815 (the "'815 Application").

39. TeleSign is the owner of all right, title and interest in the Asserted Patents, including all rights to pursue and collect damages for past, present, and future infringement of the Asserted Patents.

40. The '815 Application had published as United States Publ. No. 2015/0215889 (the "'889 Publication") on July 30, 2015. A true and accurate copy of the '889 Publication is attached

as Exhibit E.

41. TeleSign owns the right, title, and interest in the '815 Application, the '889 Publication.

42. The Asserted Claims of the '034, '920, and '038 Patents are presumed valid and enforceable.

43. Claims 9 and 18 of the '792 Patent are presumed valid and enforceable.

44. U.S. Patent Nos. 8,462,920 and 8,687,038 (asserted in *TeleSign I*) are referred to herein as "Parent Patents" to the '792 Patent.

45. The Patent Office has allowed claims of continuation applications of the '920 and '038 Patents since the Supreme Court's *Alice* decision, including at least to children patents having claims that—for the purposes of a Section 101 inquiry—are similar to, if not broader than, the claims of the '920 and '038 Patents.

46. In *TeleSign 1*, Twilio moved on the pleadings to find the Parent Patents invalid under 35 U.S.C. § 101 as purportedly directed to patent-ineligible subject matter. This Court denied that motion, finding that at least claim-construction was necessary. *TeleSign I*, ECF No. 123. TeleSign disclosed a copy of Twilio's Section 101 motion to the Patent Office before it granted the '792 Patent.

47. As indicated by Exhibit F, the Patent Office considered Twilio's Section 101 motion but still allowed the Application—as shown in Exhibit G—and granted the '792 Patent.

48. The Patent Office granted the '792 Patent well after the Supreme Court decided *Alice* on June 19, 2014. *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 134 S. Ct. 2347 (2014).

49. The claims of the Asserted Patents do not recite a mathematical algorithm.

50. The claims of the Asserted Patents do not recite merely a fundamental economic or longstanding commercial practice.

51. The recited implementation by a computing system or applicability to electronic contacts and registration are integral to the claimed inventions.

52. The claimed solutions in the Asserted Patents are necessarily rooted in computer

technology in order to overcome problems specifically arising in the realm of computer networks.

53. Adhering to the routine, conventional functioning of the prior art would foster problems that the Asserted Patents prevent.

54. The Asserted Patents do not broadly and generically claim 'use of the Internet' to perform an abstract business practice.

55. The Asserted Patents describe technical solutions to technical problems.

56. For example, claims of the '034 Patent are directed to use phone number attributes as a trust indicator, basing registration on, for example, the user's phone carrier and other characteristics, including during real-time processes, occurring while a person is trying to sign up for a website.

57. As another example, the '920 and '038 Patents are directed to verification and notification processes that address the technical problem of fraud relating to events in connection with websites, providing re-verification processes for electronic contacts.

58. By way of further example, claims of the '792 Patent address the technical problem of proliferating fake or fraudulent website/online registrations. Fake online registrations create enormous problems for companies. They can give a false sense of the number of users (real users) that are registered with a company. They can tax a company's technical resources (needing more resources to service accounts that are not actually legitimate accounts). Some websites are besieged with hundreds of thousands, or potentially millions, of attempts per day to create fraudulent registrations. As the popularity of the Internet rose, it became increasingly popular to require users to register at websites to obtain information from the website, order goods through the website, etc.

59. When doing business on the Internet, potential registrants often attempt to register with untraceable or false e-mail addresses and phone numbers, which can "compromise the intended purpose of the registration, create a breach of security and constitute fraud on the web-site owners." '792 Patent at 1:58-60. And as customers seek to register with a website, they expect to be able to register immediately. Moreover, even after a registration occurs, the problem of potential fraud exists, and is reduced by associating a telephone number with data indicating that the telephone

number is verified.

60. The technical solutions of the claimed inventions in the '920, '038 and '792 Patents is to provide, among other things, verification "in real-time," providing an additional layer of security, and thereby reducing fraud. '792 Patent at 8:45-47. A human being, or manual process, or paper-and-pencil process would not address the technical problem and would be too slow to accommodate users' and companies' expectations for being able to timely register online. Further, the technical solution includes receiving a user's phone number in a computing system by way of a user interface such as a website, which accommodates the anonymity of the Internet. The system provides for the immediate sending of a verification code to a user and requires that a user-provided phone number be verified, which occurs by receiving from the user a code that should be the same as the one sent. Again, geographical barriers are broken and the modern demand for Internet-based interactions is accommodated as the user's code is received via the computing interface. Registration is completed based on the received code, arming a company with more knowledge about the reliability of the received user information. The technical solution also addresses the technical problem of online fraud. For example, the system maintains a set of notification events. If an established notification event occurs, a user is notified. Although some systems allow users to provide—at the time that a confirmation message is to be sent—contact information (such as an unverified phone number), the claimed invention sends a message to the formerly verified phone number. The system then receives an acknowledgement of an act associated with the established notification event and associates the telephone number with data indicating that it is verified.

61. As explained in greater detail below, Twilio provides products and services that do the same thing as TeleSign's claimed technology, and Twilio actively encourages others to make, use, sell, offer for sale and/or import infringing products and services, including by using Twilio's products and services.

62. Before the earliest effective filing dates of the Asserted Patents, the claimed technology of the Asserted Claims was not available to customers.

63. In the 2005 or 2006 timeframe, it was neither conventional nor routine to receive a

user's telephone number through a computing interface, send a verification code via SMS (Short Message Service) to the user, receive a submitted verification code through the computing interface, verify the telephone number, complete a registration based on the received information and the verified telephone number, maintain a record of notification events associated with actions that require acknowledgement by a user, transmit a message to the telephone number upon receiving an indication of an occurrence of an established notification event, receive from the user an acknowledgement of an action associated with the established notification event, and associate the telephone number with data indicating that the telephone number is verified, nor was it known or obvious to do this as claimed in the '792 Patent.

64. In the 2005 or 2006 timeframe, it was neither conventional nor routine to receive a user's telephone number through a website, communicate a verification code to the user, receive a submitted verification code, verify the telephone number, establish a notification event and, after identifying the occurrence of the event, re-verifying the electronic contact, including establishing a second connection, communicating a second code, and re-verifying if the submitted code is the same as the communicated code, nor was it known or obvious to do this, as claimed in the '920 and '038 Patents.

VI. The Asserted Claims.

65. The "Asserted Claims" are:

- claims 1-4, 6, 7, 9, 11-14 of the '034 Patent (11 claims);
- claims 1-13, and 19-22 of the '920 Patent (17 claims);
- claims 1-22 of the '038 Patent (22 claims); and
- claims 9 and 18 of the '792 Patent (2 claims).

VII. Description of Twilio's Products

66. "**Lookup Products**" refers to Twilio's "Phone Intelligence" and "Lookup" products.

67. "**2FA Products**" refers to "Authy"; Twilio's "Account Portal" portion of its website (which requires users to log in to); and the following Twilio products and services used to send

authentication codes (including via Twilio's "Super Network"): "Twilio's Engagement Cloud" (including "Verify" and "Notify"), Twilio's "Programmable Communications Cloud" (including "Programmable Voice" and "Programmable Messaging"), and Twilio's "2FA Use Cases" (as explained in, for example, in Twilio's 2016 and 2017 Annual Reports, Exhibits H and I).

68. The products and technologies mentioned above are described more fully below.

69. Twilio refers to itself as providing "building blocks" that can be used to build virtually any use case. The names associated with those building blocks (by which we mean to include products and services), use cases, and other of Twilio's products have changed over time. And certain of Twilio's technologies are not marketed by a product per se, such as when Twilio stores information about users and devices.

70. Twilio's 2017 Annual Report[2] describes products in the following ways:

71. "Engagement Cloud" – "Our Engagement Cloud APIs build upon our Programmable Communications Cloud to offer more fully implemented functionality for a specific purpose, such as two-factor authentication or skills-based routing in a contact center, thereby saving developers significant time in building their applications." (Twilio 2017 Annual Report, p. 6)

72. Products within the "Account Security" facet of Twilio's Engagement Cloud include the following:

- "Authy. Provides user authentication codes through a variety of formats based on the developer's needs. Authentication codes can be delivered through the Authy app on registered mobile phones, desktop, or smart devices or via SMS and voice automated phone calls. In addition, authentication can be determined through a push notification on registered smartphones." (Twilio 2017 Annual Report, p. 12)
- Authy includes Twilio's "Phone Intelligence" technology: https://www.twilio.com/docs/authy/api/phone-intelligence.

[2] Exhibit H (https://www.sec.gov/Archives/edgar/data/1447669/000104746918001207/a2234636z10-k.htm); Exhibit I (https://www.sec.gov/Archives/edgar/data/1447669/000104746917000800/a2230935z10-k.htm).

- "Lookup. Allows developers to validate number format, device type, and provider prior to sending messages or initiating calls." (Twilio 2017 Annual Report, p. 12)
- "Verify. Allows developers to deliver a one-time passcode through SMS or voice to verify that a user is in possession of the device being registered." (Twilio 2017 Annual Report, p. 12)
- "Notify," which Twilio's website says enables one to "[r]each one customer or a million on their preferred channel with just one API call." https://www.twilio.com/notify.

73. "Programmable Communications Cloud" – "Our Programmable Communications Cloud provides a range of products that enables developers to embed voice, messaging and video capabilities into their applications." (Twilio 2017 Annual Report, p. 5) It includes "Programmable Voice" and "Programmable Messaging," which is described as "software products allow developers to build solutions to send and receive text messages globally, and incorporate advanced messaging functionality such as emoji, picture messaging and localized languages. Our customers use Programmable Messaging, through software controls, to power use cases, such as appointment reminders, delivery notifications, order confirmations and customer care." (Twilio 2017 Annual Report, p. 7)

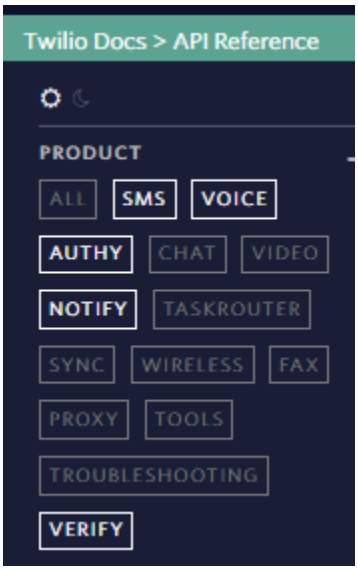
74. "Super Network" – "Our Programmable Communications Cloud is built on top of our global software layer, which we call our Super Network. Our Super Network interfaces intelligently with communications networks globally." (Twilio 2017 Annual Report, p. 7)

75. "Use cases," such as:

- "Alerts and Notifications. Alerting a user that an event has occurred, such as when a table is ready, a flight is delayed or a package is shipped." (Twilio 2017 Annual Report, p. 6)
- "User Security. Verifying user identity through two-factor authentication prior to log-in or validating transactions within an application's workflow. This adds an additional layer of security to any application." (Twilio 2017 Annual Report, p. 6)

- *Two-factor authentication (or "2FA") use cases* – "While developers can build a broad range of applications on our platform, certain use cases are more common. . . . such as two-factor authentication[.]" (Twilio 2017 Annual Report, p. 6, hereinafter "2FA Use Cases")

76. Similarly, Twilio's website refers to its products, often in short hand, such as "SMS," "Voice," "Authy," "Notify," and "Verify," as illustrated by the screen shot below from https://www.twilio.com/docs/api.



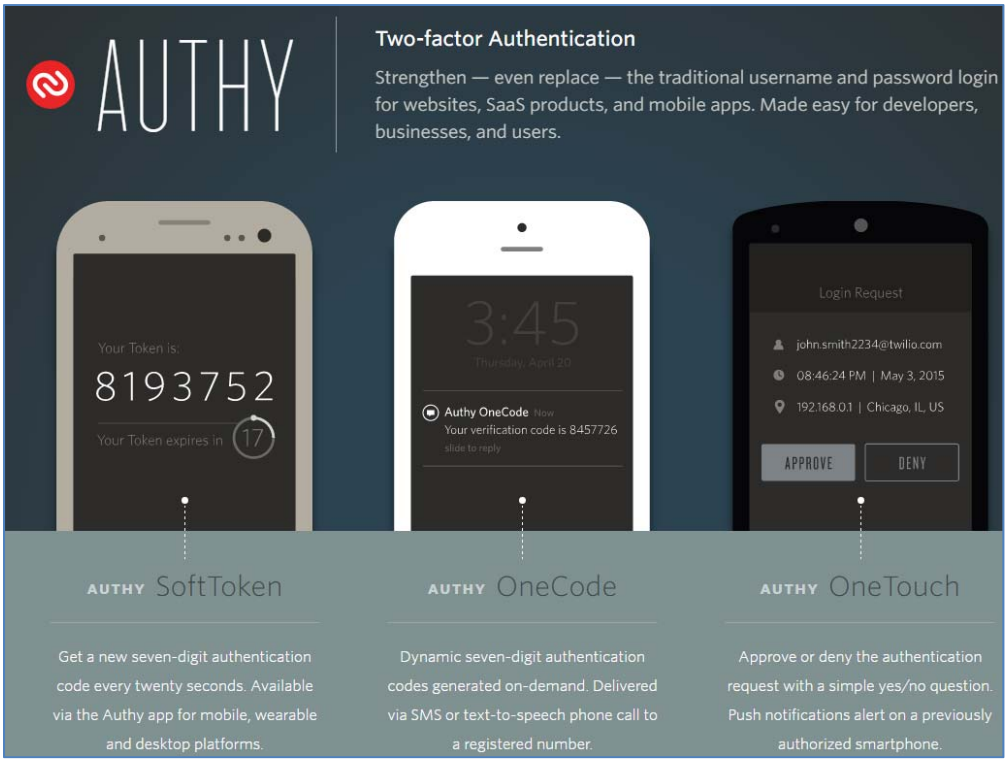
77. Twilio and its customers also make the same or similar functionality available via "add ons" having similar names, which are respectively accused to the extent they are considered different from the base products.

78. Twilio describes its Lookup as used in, and encouraged to be used in, sign-ups of customers.

79. Authy is an online security solution provided by Twilio.[3] Twilio explains that Authy "is trusted by over 10,000 websites and mobile apps," and includes the following screen shot on its website.[4]

[3] "Authy" was the name of a company Twilio acquired. That company's main product was also marketed as "Authy."

[4] Exhibit J (https://www.twilio.com/authy).



80. As Twilio has explained in its SEC filings, Authy has been integrated into Twilio ("With the integration of Authy, we now provide a cloud-based API to seamlessly embed two-factor authentication and phone verification into any application.").[5]

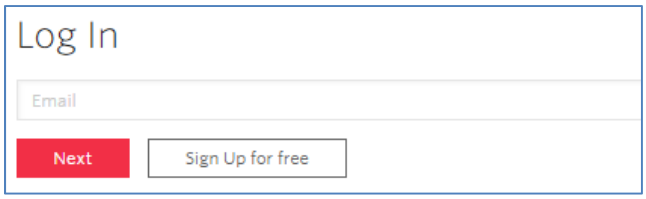
81. The full and precise contours of that technical and business integration are not public.

82. Twilio describes Authy as an online security solution using two-factor authentication. Authy is said to provide a back-end infrastructure for two-factor authentication.

83. Twilio has described Authy as the largest two-factor authentication platform.

84. There were purportedly over one million unique Authy users by August 2014.

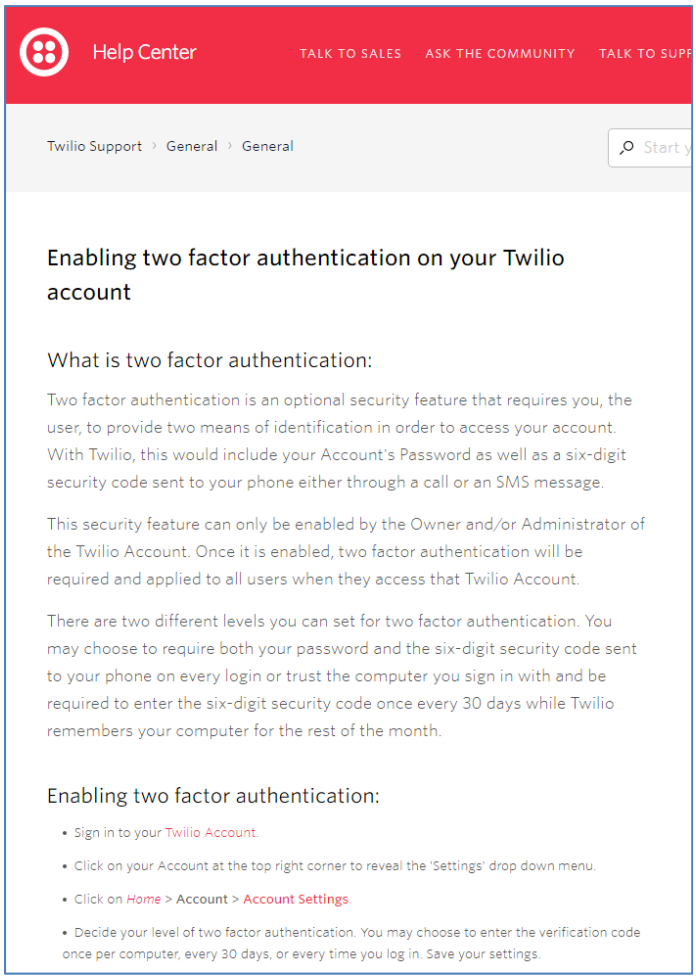
85. The *Twilio Account Portal* is the portion of Twilio's website and technologies provided to users with logging in at https://www.twilio.com/login:



86. Twilio uses the Twilio Account Portal, including its login process and the executable

[5] Exhibit H.

instructions, itself (*e.g.*, "in house"); thus the instructions and the methods are not associated with a customer-facing product name in the same way Authy is. Even so, aspects of Twilio Account Portal are described on Twilio's website (as shown below) on a page entitled "Enabling two factor authentication on your Twilio account," which explains how a user can enable 2FA on an account and how—once enabled—users will be asked to be verified.[6]



87. For example, Twilio uses Twilio Account Portal to control access to Twilio's products and services via, for example, the Twilio Console and the Authy Dashboard, including controlling access to restricted portions of Twilio's website using pages and executable code from https://www.twilio.com/login, https://dashboard.authy.com/signin and beyond https://www.twilio.com/try-twilio). Included as part of Twilio Account Portal are computer-

[6] https://support.twilio.com/hc/en-us/articles/223136307-Enabling-two-factor-authentication-on-your-Twilio-account (Exhibit L).

executable instructions to notify (and that results in notifying) users via their verified phone numbers when an attempt is made to access their Twilio Accounts (*e.g.*, when users or when fraudsters attempt to proceed pass Twilio's login screens). For trial accounts, using two-factor authentication is mandatory.

88. Twilio describes its two-factor authentication as including Authy.

89. Twilio's "Verify" includes two-factor authentication, for example its "Twilio Verify Best Practices" includes recommendations to "Plan A User Registration Flow" and "Register the user for continuous Two-factor Authentication usage," as stated at https://www.twilio.com/docs/verify/developer-best-practices.[7]

90. Twilio describes two-factor authentication as a "use case," and as implemented by Twilio's Programmable Communications Cloud including Programmable Voice and Programmable Messaging.

91. Twilio's "building blocks" include two-factor authentication uses, and messaging and voice products.

92. These "building blocks" include the Twilio REST API (referred also to as the "REST API," "Twilio API," or the "cloud API"), including Twilio Messages, Twilio SMS, Twilio Messaging Copilot, Twilio Short Codes, Twilio Calls, Twilio Voice, Twilio Notify ("Notify"), "Use Case APIs," and TwiML, and supporting SDKs. The "Use Case APIs" are for specific purposes, such as to have its customers implement two-factor authentication and notification services to customers. For example, Twilio explains the following in its SEC Filings: "**Engagement Cloud.** While developers can build a broad range of applications on our platform, certain use cases are more common. Our **Engagement Cloud APIs** build upon **our Programmable Communications Cloud** to offer more fully implemented functionality for a specific purpose, such as two-factor authentication or skills-based routing in a contact center, thereby saving developers significant time in building their applications."

93. The quoted portion of Twilio's 2017 Annual Report above previously stated, in a

[7] Exhibit M.

prior filing with the SEC quoted by TeleSign in its complaint against Twilio (emphasis added): "**Use Case APIs.** While developers can build a broad range of applications on our platform, certain use cases are more common. Our **Use Case APIs** build upon the above products to offer more fully implemented functionality for a specific purpose, such as two-factor authentication, thereby saving developers significant time in building their applications."

94. Twilio implements its products, including its use cases, building blocks, and two-factor authentication, using its Engagement Cloud, Super Network, and hardware.

95. Twilio provides the parts for its customers to make, use, sell, offer for sale or import infringing products, and shows them how to and actively encourages them to do so. By analogy, if TeleSign's patent covered a car, then Twilio provides parts to customers to make and use the claimed car, and provides tutorials on how to make and use such a car and actively encourages customers to do so, particularly, in an infringing manner. Here, the parts of the car correspond to Twilio's self-described building blocks or modules of computer-executable code, as identified above.

96. Twilio's sales force, marketing force, evangelists, and other company representatives have and continued to actively encourage Twilio's customers to use Twilio's products to make, use, offer, sell or import infringing technologies.

VIII. The Accused Products

97. Based on Twilio's website and its SEC filings, and in particular its 2017 Annual Report, TeleSign identifies the following accused products with reference to definitions provided in the preceding section VII describing Twilio's products.

98. "**The '034 Accused Products**" means Twilio's "Lookup Products" and "2FA Products." Note: "Authy" utilizes both Twilio's phone-number-characteristic-determination technology because it includes "Phone Intelligence" and facilitates two-factor authentication.

99. "**The '920 Accused Products**" means Twilio's "2FA Products."

100. "**The '038 Accused Products**" means Twilio's "2FA Products."

101. "**The '792 Accused Products**" means Twilio's "2FA Products."

IX. Twilio's Knowledge of the Asserted Patents.

102. Twilio received a copy of TeleSign's original complaint in *TeleSign I* on or about April 30, 2015. *TeleSign I*, ECF No. 79 at ¶ 29.

103. Twilio became aware of TeleSign's '920, '038, and '034 Patents at least by April 30, 2015, when it was served with the Complaint in *TeleSign I*, which asserted infringement.

104. Through its counsel, Twilio received actual notice of the '792 Patent by March 29, 2016. The original complaint in *TeleSign II* was filed on March 28, 2016 (Eastern Time), and a copy was sent by email to counsel for Twilio on March 29, 2016. Counsel for Twilio responded to that email on March 29, 2016.

105. A copy of the original complaint was duly served on Twilio on March 31, 2016. *TeleSign II*, ECF No. 13.

106. Twilio became aware of the '815 Application—it being a child of the '920 and '038 patents—as part of its diligence in defending against TeleSign's allegations in *TeleSign I*, and this allegation will likely have evidentiary support after a reasonable opportunity for further investigation or discovery.

107. Twilio received a copy of the then pending and published claims when TeleSign filed them as exhibits to *TeleSign I* motion on February 22, 2016. *See* Exhibit N.

108. TeleSign also filed documents in *TeleSign I* showing that TeleSign's '792 Patent was granted after the Patent Office considered (i) Twilio's Motion for Judgment on the Pleadings and (ii) Twilio's *inter partes* review requests for the Parent Patents (and other submitted references). *See* Exhibits O and P.

109. TeleSign provided the prosecution history of the '815 Application to Twilio on March 8, 2016, including the pending claims and the Notice of Publication from the Patent and Trademark Office stating that the application was published as Publ. No. 2015/0215889. *See* Exhibit Q.

110. As part of TeleSign's document production in *TeleSign I*, Twilio received a copy of

the Notice of Publication regarding the '889 Publication and a copy of the Notice of Allowance that indicated that the claims of the '815 Application (which would be the same as those in the '792 Patent) would be allowed.

111. The claims of the '792 Patent did not change during prosecution of the '815 Application.

112. The claims in the '889 Publication (Exhibit E), published on July 30, 2015, are identical (or substantially identical) to the issued claims in Patent No. 9,300,792 (*see* Exhibit D).

113. Thus, Twilio had actual notice of TeleSign's '815 Application and of the '889 Publication as of March 8, 2016. Twilio has and has had actual notice of the '815 Application, the '889 Publication, and the '792 Patent before the filing of this First Amended Complaint.

114. In summary, after Twilio received the *TeleSign I* complaint, it analyzed the patents family, learned of the Parent Patents, learned of the '815 Application (and its filed claims) and of the '889 Publication, and monitored the '815 Application's examination process by the Patent Office, including the Notice of Allowance (Exhibit G)—which would have confirmed that the claims allowed were the same as the claims as filed and that would issue. Twilio also learned of the Issue Notification prior to the '792 Patent's issuance, which would have given Twilio notice that the '792 Patent would issue on March 29, 2016, and these allegations are likely to have evidentiary support after a reasonable opportunity for further investigation or discovery.

115. Twilio's prior knowledge—including its pre-issuance knowledge—is relevant to, among other things, TeleSign's willfulness claims and its demand for damages under 35 U.S.C. § 154(d).

116. TeleSign has complied with 35 U.S.C. § 287(a).

X. Actions Twilio Performs for Its Customers (Regarding Joint Infringement).

117. Under certain direct infringement theories alleged herein, Twilio's customers perform steps of the Asserted Claims.

118. Alternatively, Twilio's customers have contracted with and continue to contract with

Twilio to perform one or more steps of the Asserted Claims, for example the step of having text messages sent to end users.

119. When Twilio performs one or more steps of the Asserted Claims under TeleSign's joint infringement theories, Twilio's performance is attributable to Twilio's customers, the direct infringers.

120. By way of agreements and representations, Twilio commits to providing its services to such customers and making Twilio's services available to them such that Twilio cannot unilaterally refuse to provide its products or services.

121. Twilio obligates itself to provide its products and services to its customers, including the accused products described herein, and Twilio agrees to provide service credits in exchange for failing to meet its obligations and commitments to its customers.

122. Twilio has an API Service Level Agreement with its customers that obligates Twilio to make its API(s) available, essentially, all the time.

123. For example, Twilio's Service Level Agreement promises customers that Twilio will provide its services, thus performing steps that are attributable to Twilio's customers. Twilio promises that its services will be available, including promising to its customers that the Twilio API will be available 99.95% of the time in a month. If Twilio fails, its customers receive a remedy.

124. Twilio claims that it continues to maintain a 99.999% uptime rate for Authy.

125. Twilio promises to provide written notice prior to terminating or suspending its services to customers.

126. Twilio encourages its customers to perform infringing steps (such as phone-number verification), and Twilio will not decline to perform actions that it recommends its users undertake.

127. Twilio requires its customers to indemnify Twilio for claims or liability in connection with the customer applications, indicating that the activity is attributable to Twilio's customers.

128. The total and collective terms of the Service Level Agreement and the Terms of Service show that Twilio is operating as contracted by customers that use the accused products.

129. Twilio's customers indemnify Twilio from potential harm stemming from

intellectual-property claims.

130. Twilio's agreements with its customers protect Twilio from any intellectual-property issues that arise from the customers' use of Twilio's services.

131. Twilio's customers agree to defend, indemnify and hold Twilio and its affiliates harmless against any actual or threatened claim, loss, liability, proceeding, third-party discovery demand, governmental investigation or enforcement action arising out of or relating customers' activities under Twilio's terms of service or customers' acts or omissions in connection with the provision of customers' applications, including, without limitation, any intellectual property claims relating to customers' applications. By way of further example, Twilio's customers agree to indemnify Twilio in any action in connection with intellectual-property claims, as shown in Twilio's Terms of Service at https://www.twilio.com/legal/tos.

132. Twilio's customers make use of the Twilio application-programming interface (API) in an infringing manner, while Twilio has agreed in a "Service Commitment" to make the Twilio API available 99.95% of the time, as shown in Twilio's API Service Level Agreement at https://www.twilio.com/legal/service-level-agreement.

133. Twilio's 2017Annual Report states (p. 30): "We typically provide monthly uptime service level commitments of up to 99.95% under our agreements with customers. If we fail to meet these contractual commitments, then our business, results of operations and financial condition could be adversely affected" and "our business, results of operations and financial condition could be adversely affected if we suffer unscheduled downtime that exceeds the service level commitments we have made to our customers."

134. When Twilio's customers request that Twilio perform one or more steps including by contracting with Twilio to perform steps, the use of the Accused Products and the performance of the claimed technology is attributable to Twilio's customers because they opt (at the instruction, encouragement, and advice of Twilio) to verify their own customers' telephone numbers, but use Twilio to do so (*e.g*, by using Authy to verify the end user's phone number).

135. Twilio's customers' applications instruct Twilio to send text messages, including

when an application has been built with or relying on Authy or Twilio's Engagement Cloud or Programmable Communications Cloud, or when a customer has added Authy to an application.

136. Twilio routes calls and messages for its customers. *E.g.*, *TeleSign I*, ECF No. 55-1 at ¶ 24.

137. Twilio, for example, acts at the direction and control of its customers to perform steps that are attributable to its customers, the direct infringers.

XI. COUNT I - Direct Infringement of the '034 Patent

138. TeleSign repeats and realleges each of the allegations contained in the paragraphs above.

139. Defendant Twilio has infringed the '034 Patent and is liable as an infringer under 35 U.S.C. § 271(a).

140. First example of direct infringement: Twilio directly infringes the '034 Patent when it registers (*e.g.*, stores user-specific information associated with) its own customers who attempt to, for example, register with Twilio via Twilio's Account Portal, based on, for example, information associated with a received phone number, which was determined using its Lookup Products to determine phone-number characteristics of the provided phone number, and a verification message sent to the customer as part of a two-factor authentication process, using, for example, Twilio's 2FA Products.

141. Second example direct infringement: Twilio directly infringes the '034 Patent when it registers (*e.g.*, stores user-specific information associated with) its customers' end users based on, for example, information associated with a received phone number, which was determined using Twilio's Lookup Products to determine phone-number characteristics of a provided phone number, and a verification message sent to the user as part of a two-factor authentication process, using Twilio's 2FA Products.

142. On May 17, 2011, United States Patent No. 7,945,034, entitled "Process for determining characteristics of a telephone number," was duly and legally issued by the United States

Patent and Trademark Office.

143. Plaintiff TeleSign is the owner of the '034 Patent with full rights to pursue recovery of royalties or damages for infringement of the '034 Patent, including full rights to recover past and future damages.

144. Each claim of the '034 Patent is valid and enforceable.

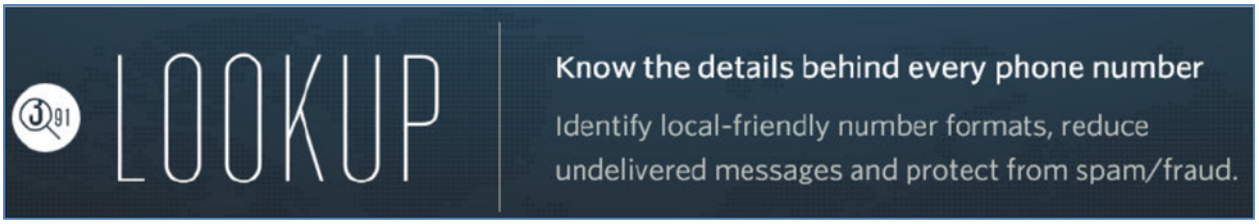
145. Twilio makes, sells, offers for sale, uses and/or imports, in the United States its Lookup Products with its 2FA Products, which directly infringe the '034 Patent Asserted Claims.

146. Defendant Twilio has infringed the '034 Patent and, unless enjoined, will continue to do so, by using, offering for sale and selling services claimed by the '034 Patent.

147. The Lookup Products and 2FA Products are made available through Twilio's website at www.twilio.com.

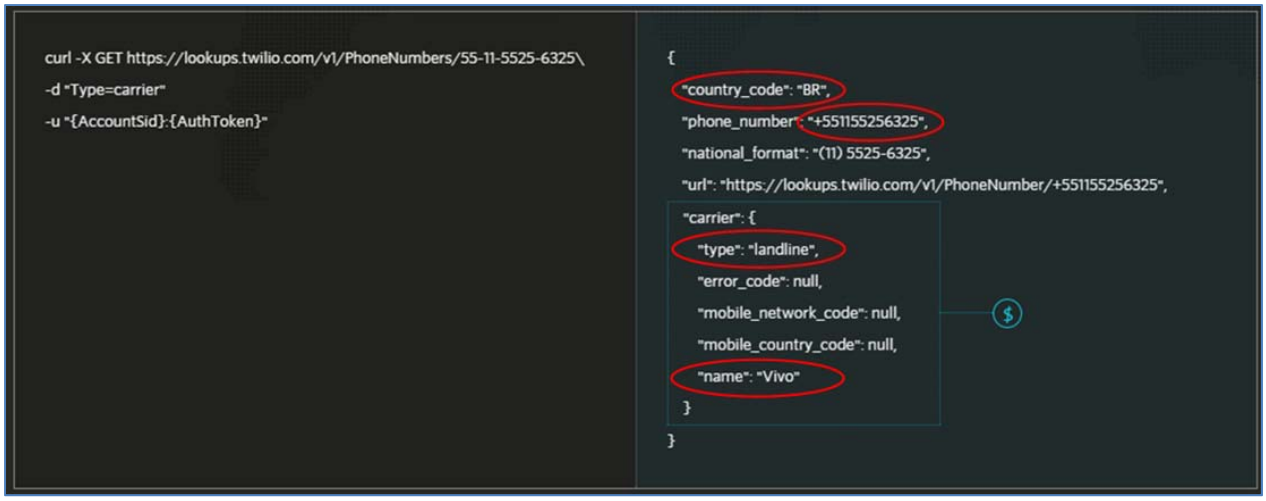
148. The '034 Patent relates to, among other things, using "characteristics of a telephone number" in a registration process. These characteristics could include for example, whether a telephone number is a landline (claim 4), the phone carrier (claim 1), and geographic characteristics such as a country (claim 6).

149. Twilio makes, sells, offers for sale and/or uses, in the United States the Lookup Products, as indicated by, for example, https://www.twilio.com/lookup[8] and as shown in one example below.



150. By way of example only, the screen capture below from https://www.twilio.com/lookup indicates that Twilio's Lookup Products determine at least these characteristics.

[8] Exhibit R.



151. On March 31, 2015, Twilio posted a blog entry stating "Today we're happy to introduce you to a new product called Lookup, an API that will retrieve detailed information about a phone number." https://www.twilio.com/blog/2015/03/introducing-twilio-lookup.html.

152. The screenshot below shows Twilio's Lookup Products as shown at https://www.twilio.com/lookup.

	Format Lookup Free Best for validating inputs	Carrier Lookup .5 cents per request Best for ensuring message delivery	Caller Lookup 1 cent per request Best for identifying inbound callers. US only.	Fraud Lookup Coming Soon Best for preventing account fraud. US only.
Format and Origin	✓	✓	✓	✓
Line Type		✓		
Carrier		✓		
Caller Name			✓	✓
Caller Type			✓	✓
Advanced Line Type				✓
Porting History				✓
Roaming Status				✓

153. Twilio uses its 2FA Products such as two-factor authentication with Twilio customer

accounts.

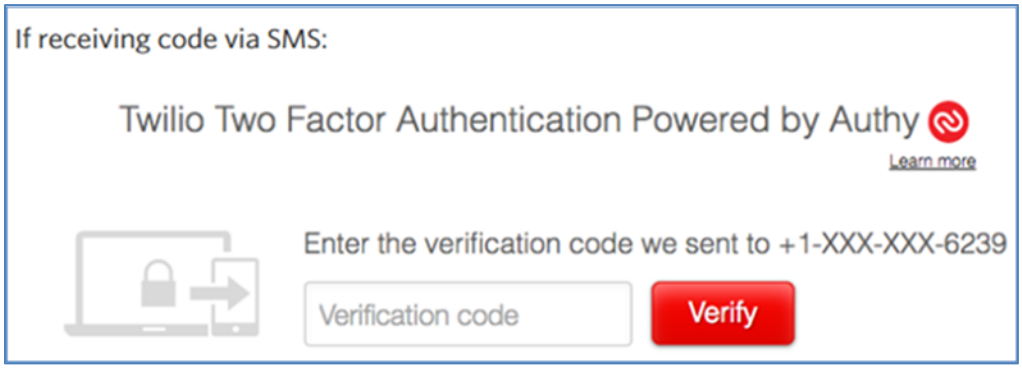
154. For example, Twilio uses two-factor authentication with its Authy development accounts and other accounts that use the Twilio Account Portal, such as customer and developer accounts.

155. By way of further example, Twilio makes two-factor authentication active for "Authy account[s]" that are used for "Authy development" as shown at https://www.twilio.com/blog/2017/10/easily-manage-team-access-to-the-twilio-console.html.

> While a single-user is the easiest way to approach Authy development, keep in mind that there are some limitations:
>
> - Since 2FA is active when you create an Authy account, you cannot share accounts.

156. Twilio uses two-factor authentication including 2FA powered by Authy to secure Twilio customer accounts, as shown at https://www.twilio.com/blog/2017/08/securing-your-twilio-account-with-2fa.html, including registering of customer accounts, and including accounts accessed using Twilio Account Portal.

Securing Your Twilio Account With 2FA



157. When Twilio registers its customers who attempt to, for example, register with Twilio via Twilio's Account Portal, based on, for example, information associated with a received a phone number determined using Twilio's Lookup Products, and a verification message sent to the customer as part of a two-factor authentication process, using, for example, Twilio's 2FA Products, Twilio performs of each step of the methods claimed by the '034 Patent, which will likely have evidentiary support after a reasonable opportunity for further investigation or discovery.

158. When Twilio registers its customers' end users based on, for example, information associated with a received a phone number determined using Twilio's Lookup Products to determine phone-number characteristics of a provided phone number, and a verification message sent to the user as part of a two-factor authentication process, using Twilio's 2FA Products, Twilio performs of each step of the methods claimed by the '034 Patent, which will likely have evidentiary support after a reasonable opportunity for further investigation or discovery.

159. For example, Twilio directly infringes claim 1 of the '034 Patent, which recites a process for telephonically registering a user over one or more communication networks through determining characteristics of a telephone number, comprising five steps.

160. Twilio infringes claim 1 when it registers—including storing user-specific information regarding—users over networks such as the Internet, telephone networks, or other communications networks such as its "Super Network"; electronically determines phone-number characteristics via the Lookup Products, including the characteristics as shown above, such as type of phone (*e.g.*, "type : landline"), phone carrier (*e.g.*, carrier "name : Vivo", and geographic (*e.g.*, "country_code : BR"); connects to a phone or application (*e.g.*, via smart device/computer) associated with the telephone number and sends a verification message as part of a two-factor authentication use case (including Authy) and/or using its Programmable Communications Cloud (*e.g.*, to send a voice message or text the code to the user via its Programmable Voice or Programmable Messaging technologies); and registering the user by, for example, storing information about the user based on the characteristics and the verification message, such as, for example, an indication that the user is verified, flagged, pending verification, not verified, etc.

161. Regarding Twilio's Engagement Cloud, Twilio's 2017 10-K states: "While developers can build a broad range of applications on our platform, certain use cases are more common. Our Engagement Cloud APIs build upon our Programmable Communications Cloud to offer more fully implemented functionality for a specific purpose, such as two-factor authentication or skills-based routing in a contact center, thereby saving developers significant time in building their applications." (Twilio 2017 Annual Report, p. 11)

162. As to Authy, Twilio's 2017 10-K states (emphasis added): "Authy. Provides user authentication codes through a variety of formats based on the developer's needs. **Authentication codes** can be delivered through the Authy app on **registered** mobile phones, desktop, or smart devices or via SMS and voice automated phone calls. In addition, authentication can be determined through a push notification on **registered** smartphones." (Twilio 2017 Annual Report, p. 12)

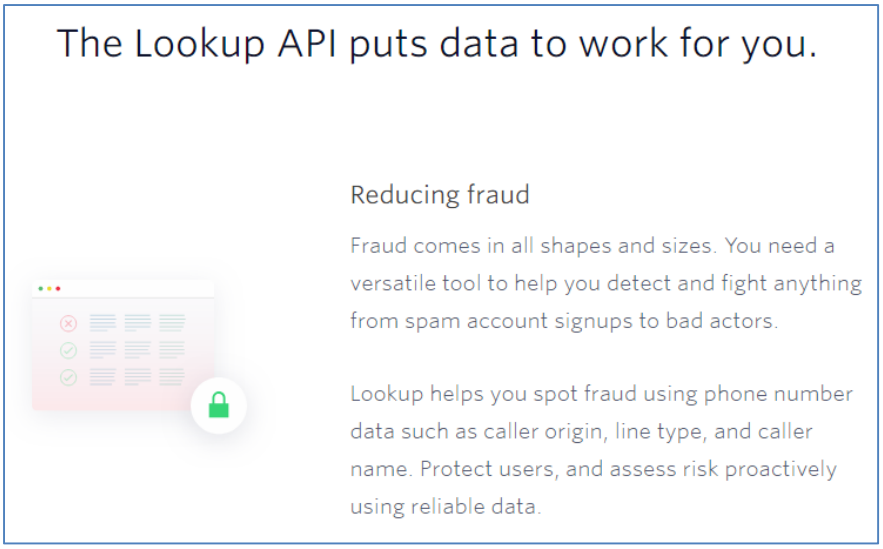
163. As to Lookup, Twilio's 2017 10-K states (emphasis added): "Lookup. Allows developers to validate number format, device type, and provider prior to **sending messages** or initiating calls." (Twilio 2017 Annual Report, p. 12)

164. As to Verify, Twilio's 2017 10-K states (emphasis added): "Verify. Allows developers to deliver a one-time passcode through SMS or voice to verify that a user is in possession of the device being **registered**." (Twilio 2017 Annual Report, p. 12)

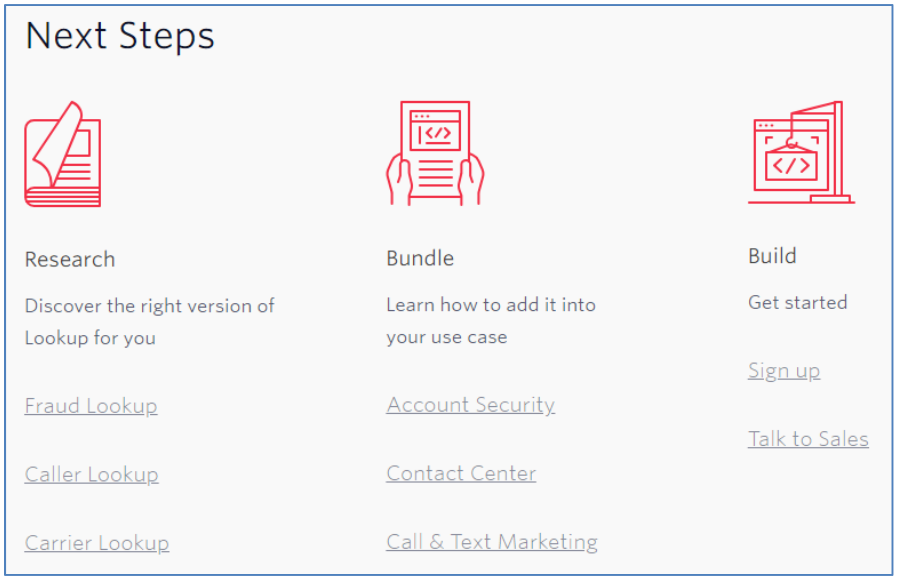
165. Twilio's 2017 10-K describes its "Programmable Communications Cloud" as follows: "Our Programmable Communications Cloud consists of software for voice, messaging, video and authentication that empowers developers to build applications that can communicate with connected devices globally. We do not aim to provide complete business solutions, rather our Programmable Communications Cloud offers flexible building blocks that enable our customers to build what they need." (Twilio 2017 Annual Report, p. 12)

166. Over time Twilio has branded or identified its technology or uses case with different names and as various "building blocks." Regardless, it has used that technology and those "building blocks" as part of its "Programmable Communications Cloud," to infringe the claims of the '034 Patent by carrying out the accused functionality of receiving phone numbers from customers, determining characteristics associated with those phone numbers, facilitating the sending of a verification message to a user associated with the phone number, and storing information about the user including information about a user device based on the characteristics and verification message.

167. Twilio uses its Lookup Products for, among other things, reducing fraud, as explained on its website:

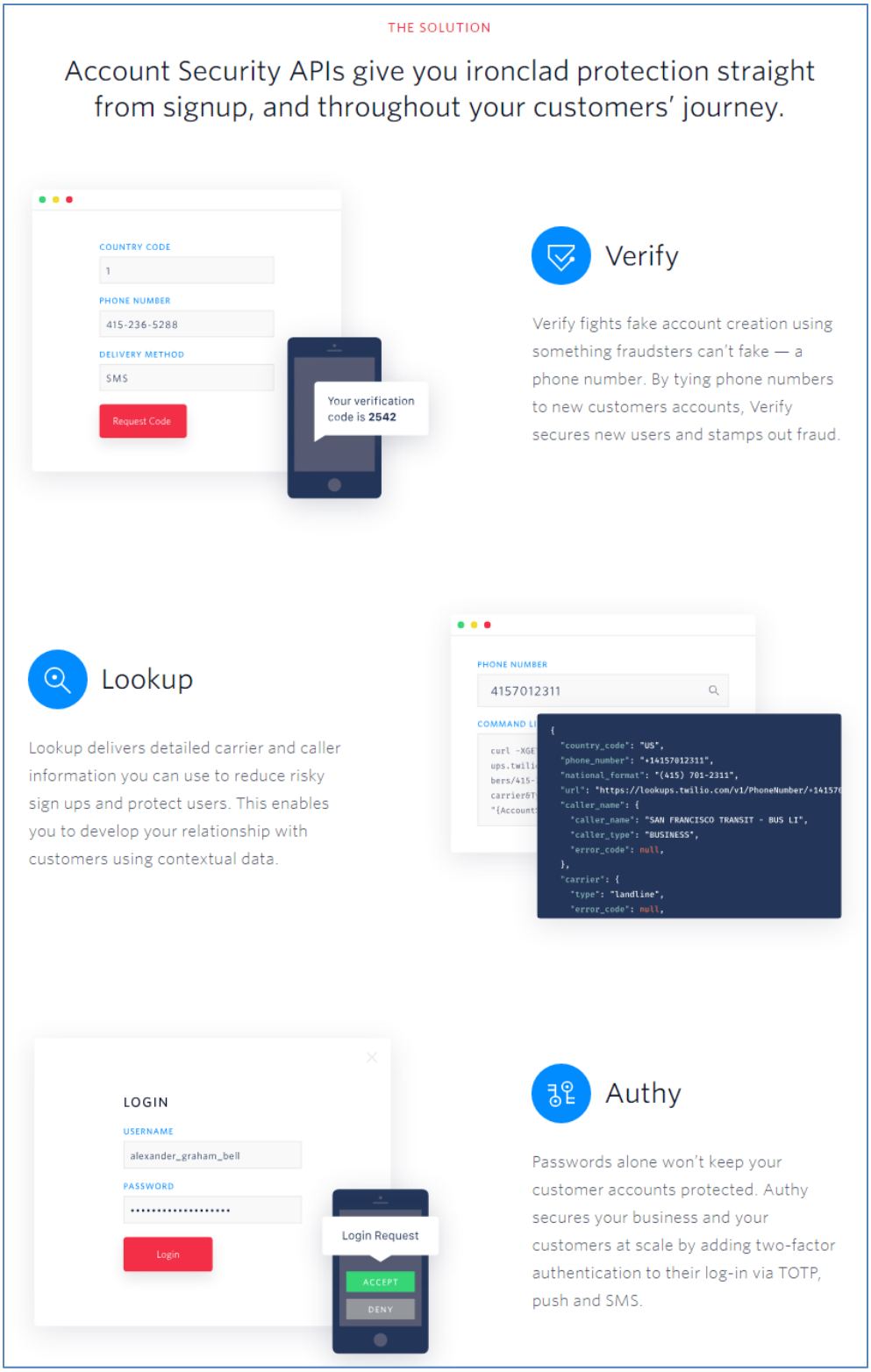


168. Twilio markets its Lookup Products to be bundled as party of "Account Security" use cases:



169. Following the "Account Security" link above presents a single webpage detailing "The Solution" to, among other things, prevent "New Account Fraud," wherein the Twilio advertises all three branded products together: Lookup, Authy, and Verify, including as part of a two-factor authentication use case.[9]

[9] Exhibit S (https://www.twilio.com/solutions/account-security).



170. Twilio's Phone Intelligence product provides information about phone numbers.

171. By way of example, the screen capture below from https://www.twilio.com/docs/authy/api/phone-intelligence indicates that Twilio's Phone Intelligence

product "provides information about a phone number."

> The Authy Phone Intelligence API provides information about a phone number.

172. The Phone Intelligence product determines the type of phone number and the provider of the number.

173. The Phone Intelligence product also determines information based on the "Phone country code."

174. Twilio uses characteristics determined by the Phone Intelligence product in a registration process, which will likely have evidentiary support after a reasonable opportunity for further investigation or discovery.

175. Twilio directly infringes when it performs the accused functionality to verify new or existing customers who register or attempt to register for a Twilio account, which will likely have evidentiary support after a reasonable opportunity for further investigation or discovery.

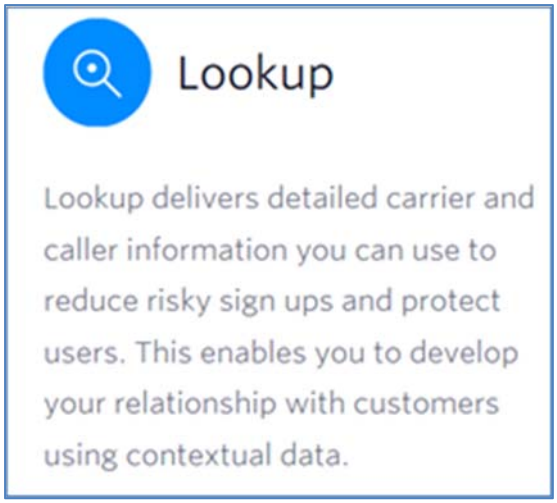
176. Twilio implements authentication for its Twilio accounts.

177. Twilio's processes for verifying its customers include processes that it recommends to its customers, which will likely have evidentiary support after a reasonable opportunity for further investigation or discovery.

178. For example, Twilio implements the Lookup Products and 2FA Products that it recommends to its customers, which will likely have evidentiary support after a reasonable opportunity for further investigation or discovery.

179. Twilio implements the Lookup Products as part of registering users, which will likely have evidentiary support after a reasonable opportunity for further investigation or discovery.

180. Twilio recommends its customers use Lookup for "sign ups" as shown at https://www.twilio.com/solutions/account-security.



181. Twilio recommends its customers use Lookup and Phone Intelligence in connection with its customers' end users, including as shown below with respect to induced infringement allegations relating to the '034 Patent.

182. Twilio instructs its customers to use Lookup to reach their registered customers in the most appropriate ways as shown at https://www.twilio.com/docs/lookup/quickstart.

> Now you're ready to look up your customers' phone numbers and reach them in the most appropriate ways!

183. Twilio recommends using Lookup to "protect yourself from fraud." https://www.twilio.com/docs/lookup/quickstart.

184. Twilio uses the Lookup Products with its accounts that also use 2FA Products, including for registering or signing-up customers, to directly infringe the '034 Patent Asserted Claims, which will likely have evidentiary support after a reasonable opportunity for further investigation or discovery.

185. Twilio's infringement occurs using one or more of Twilio's controlled data centers or internal servers that store user-specific information and/or notification events.

186. TeleSign has been damaged by Twilio's infringement of the '034 Patent and will suffer additional irreparable damage unless Twilio is enjoined from continuing to infringe the '034 Patent.

XII. COUNT II - Active Inducement of Infringement of the '034 Patent

187. TeleSign repeats and realleges each of the allegations contained in the paragraphs above.

188. Defendant Twilio has actively induced infringement of the '034 Patent and is liable as an infringer under 35 U.S.C. § 271(b).

189. Illustrative inducement example. Twilio actively induces its customers to infringe the '034 Patent in violation of 35 U.S.C. § 271(b). Aware of the '034 Patent since TeleSign filed its initial lawsuit on April 30, 2015, Twilio has specifically intended and intends its customers to infringe the '034 Patent and knows that its customers' acts constitute infringement. For example, Twilio knows that its customers infringe the '034 Patent when they follow Twilio's recommendations, encouragements, tutorials, advice, and advertisements to register their end users based on phone-number characteristics determined by Twilio's Lookup Products and on verification messages communicated via Twilio's 2FA Products. Twilio encourages its customers to both check phone-number characteristics and use two-factor authentication when registering users to prevent fraud, among other things. The underlying direct infringement occurs when Twilio's customers register their end users and as part of that registration process, and as instructed and encouraged by Twilio, those customers use Twilio's Lookup Products to determine phone-number characteristics of a received phone number and, also as instructed and encouraged by Twilio, use Twilio's 2FA products to send their end users a 2FA verification message, which the Twilio customer also uses during registration, to, for example, prevent the creation or use of fake online accounts as users attempt to register with Twilio's customers.

190. Twilio had knowledge of the '034 Patent as stated above regarding Twilio's Knowledge of the Asserted Patents.

191. Twilio has specific intent to encourage its customers' direct infringement of the '034 Patent.

192. Twilio has known, or is willfully blind to the fact, that it has been (at least since April 30, 2015) and is actively encouraging acts that constitute infringement of the Asserted Claims of the

'034 Patent, including inducing its customers' infringement.

193. In the face of the knowledge of the '034 Patent as alleged above, Twilio continues (at least past April 30, 2015) to encourage its customers to use the Lookup Products and 2FA Products to make, use, sell, offer to sell and import products and services that infringe the Asserted Claims with knowledge (or willful blindness) that its induced acts constitute patent infringement.

194. Twilio continues, with knowledge of the '034 Patent, to actively promote, encourage and teach customers to build applications that carry out all of the steps of the '034 Patent Asserted Claims.

195. Twilio continues to provide tutorials, including instructional videos, sample code, customer support, demonstrations, and marketing materials that encourage and instruct its customers to infringe the '034 Patent Asserted Claims.

196. In the face of the knowledge of the '034 Patent as alleged above, Twilio continues (past April 30, 2015) to encourage its customers to use the Lookup Products and 2FA Products to make, use, sell, offer to sell and import products and services that infringe the Asserted Claims of the '034 Patent with knowledge (or willful blindness) that its induced acts constitute patent infringement.

197. Twilio continues to offer and instruct its customers to use Lookup Products and 2FA Products, despite knowledge of the '034 Patent Asserted Claims and knowledge that its customers' acts constitute direct infringement of the '034 Patent.

198. Twilio continues to provide tutorials that recommend using verifying and registering techniques in combination with its Lookup Products and 2FA Products.

199. Twilio's customers follow such tutorials to make, use, sale, and offer infringing applications and services, which will likely have evidentiary support after a reasonable opportunity for further investigation or discovery.

200. With knowledge of the '034 Patent and its claims, Twilio has not removed or taken down its instructional materials including tutorials and marketing encouragements, thereby knowing that the customer acts Twilio is inducing constitute patent infringement.

201. With knowledge of the '034 Patent and its claims, Twilio continues to provide instructions and has provided additional instructions, including articles, videos, conferences, customer support, sample code, or webpages.

202. Some articles and tutorials are targeted and interlink with each other and direct uses by cross-references (including via marketing materials that describe the functionality of the Lookup Products and 2FA Products and how they can and should be combined).

203. Twilio continues to offer and link to (and provide new webpages and links to) its tutorials, articles, and other materials that instruct customers to determine characteristics as claimed in the '034 Patent, and register users—all with knowledge (or willful blindness) that these induced acts constitute patent infringement.

204. Twilio's customers use the Lookup Products and 2FA Products or they contract with Twilio for use of Twilio's services that perform steps claimed by the '034 Patent.

205. Twilio advertises and instructs its customers to use the Lookup Products and 2FA Products as claimed by the '034 Patent.

206. Twilio induces its customers to infringe the '034 Patent by, for example, actively encouraging and instructing them to telephonically register a user over one or more communication networks, including by receiving a telephone number, electronically determining the type of phone, the phone carrier and geographic characteristics associated with the telephone number, then connecting to a telephone associated with the telephone number through at least one of the communication networks and communicating a verification message with the telephone over at least one of the communication networks, and registering the user through at least one of the communication networks based on the type of phone, the phone carrier, the geographic characteristics associated with the telephone number and the verification message.

207. Twilio instructs and encourages its customers to infringe the '034 Patent by using Lookup Products and 2FA Products as part of registering end users.

208. Twilio has continued maintaining and adding to its instructions and encouragement to its customers to infringe TeleSign's Asserted Patent Claims with knowledge of the patent claims and

its customers' infringement.

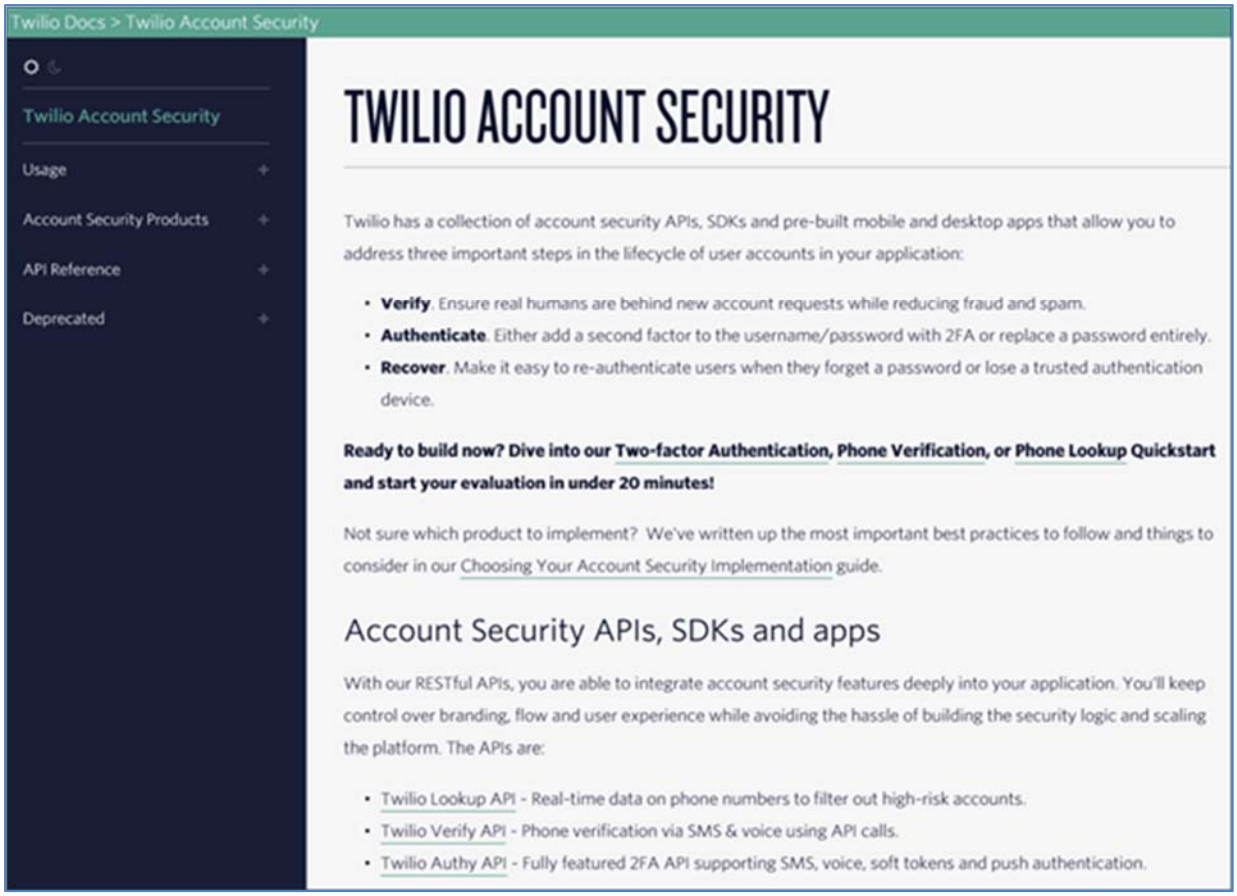
209. Twilio has provided and continues to provide tutorials instructing its customers to use Lookup Products and 2FA Products.

210. For example, Twilio provides Quickstart documents to teach its customers to use its Lookup Products, as shown at https://www.twilio.com/docs/lookup/quickstart.[10]

211. Twilio has provided and continues to provide articles, customer support, and documents including API documentation that encourages its customers to use Lookup Products with its 2FA Products.

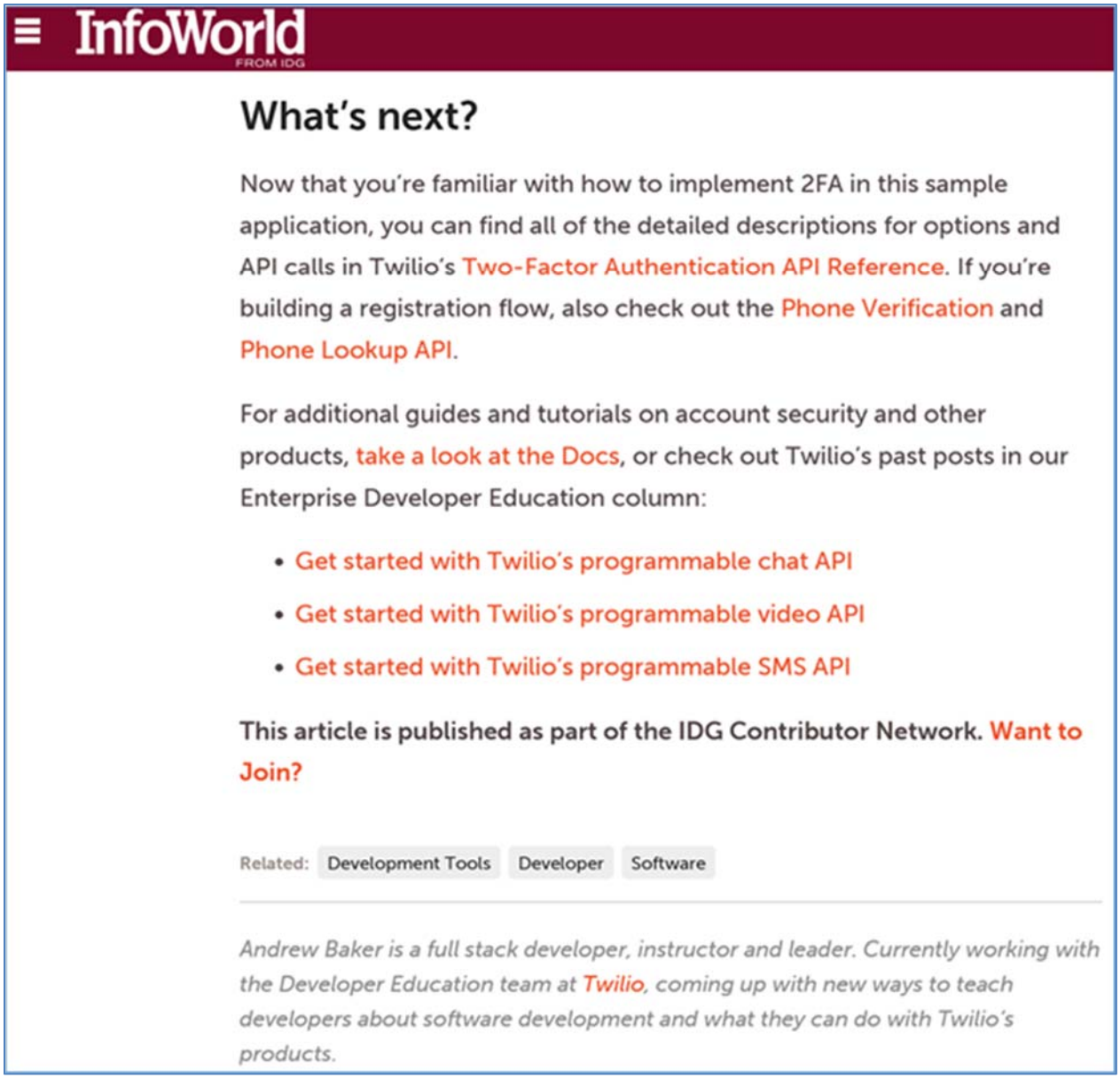
212. By way of example, the screen capture below from https://www.twilio.com/docs/account-security[11] shows that Twilio instructs users to implement the Lookup Products and 2FA Products as part of Twilio's "Account Security," including verification, authentication, and Twilio's Lookup API.

[10] Exhibit T.
[11] Exhibit U.



213. By way of further example, the screen capture below from https://www.infoworld.com/article/3230142/development-tools/getting-started-with-twilio-account-security-using-nodejs-and-mongodb.html[12] shows that Twilio instructs users "building a registration flow" to use the Lookup Products and 2FA Products, including 2FA and Twilio's Phone Lookup API.

[12] Exhibit V.



InfoWorld
FROM IDG

What's next?

Now that you're familiar with how to implement 2FA in this sample application, you can find all of the detailed descriptions for options and API calls in Twilio's Two-Factor Authentication API Reference. If you're building a registration flow, also check out the Phone Verification and Phone Lookup API.

For additional guides and tutorials on account security and other products, take a look at the Docs, or check out Twilio's past posts in our Enterprise Developer Education column:

- Get started with Twilio's programmable chat API
- Get started with Twilio's programmable video API
- Get started with Twilio's programmable SMS API

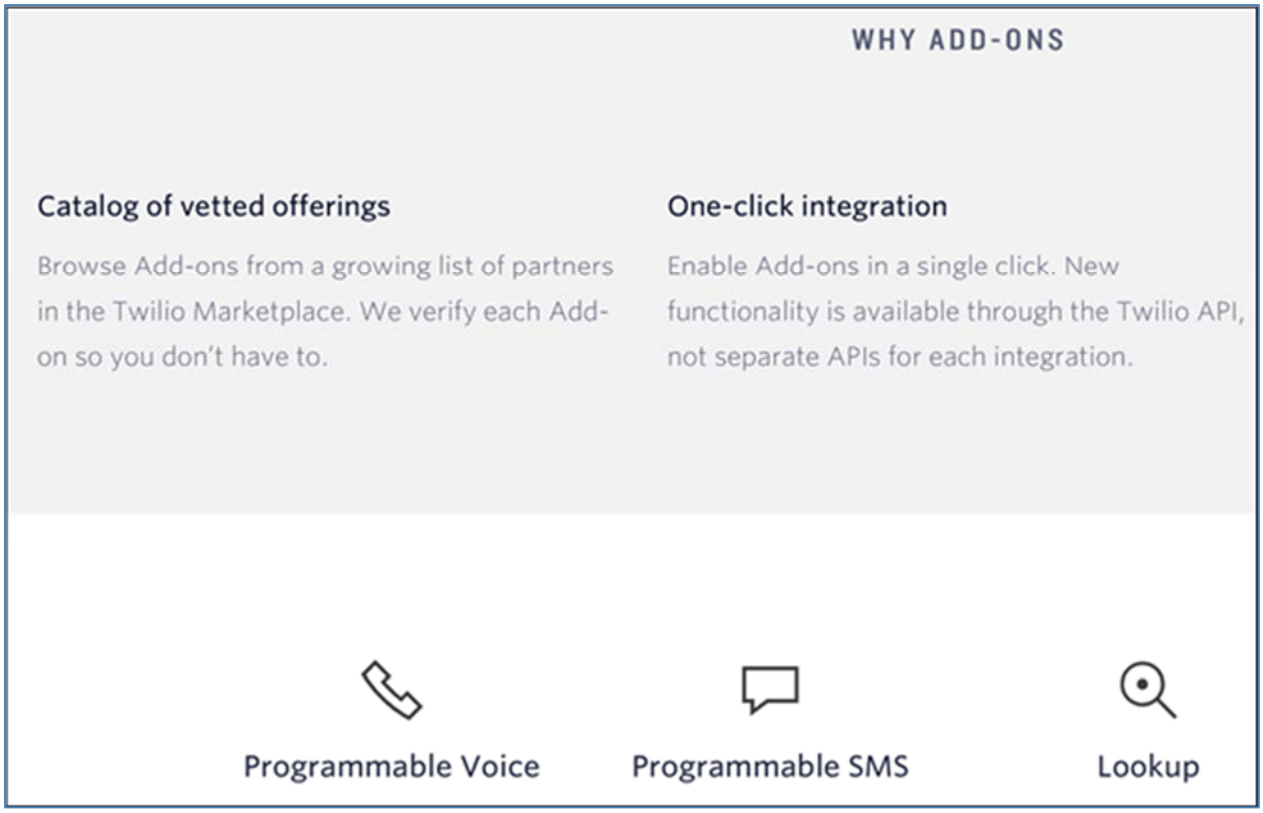
This article is published as part of the IDG Contributor Network. Want to Join?

Related: Development Tools Developer Software

Andrew Baker is a full stack developer, instructor and leader. Currently working with the Developer Education team at Twilio, coming up with new ways to teach developers about software development and what they can do with Twilio's products.

214. By way of further example, the screen capture below from https://www.twilio.com/marketplace/add-ons[13] shows that Twilio instructs customers to "[e]nable Add-ons in a single click," including Lookup and Programmable SMS, and Twilio offers "Add-ons from a growing list of partners in the Twilio Marketplace."

[13] Exhibit W.



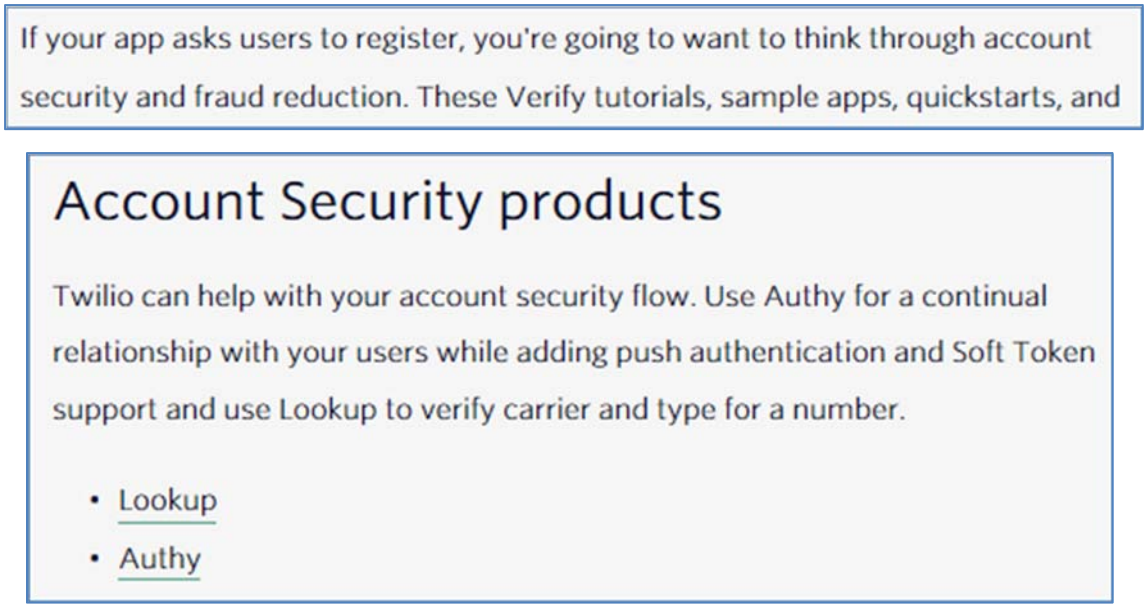
215. Twilio instructs and encourages its customers to implement a registration flow with device verification using Twilio's Verify, for example as described at https://www.twilio.com/docs/verify/quickstart.[14]

> Twilio's Verify API allows you to implement an important high-confidence phone presence check during your sign-up flow. Adding phone verification to your account verification flow will drastically reduce fraudulent signups, and protect future users from having their phones registered with your app by bad actors.
>
> Here we've collected a number of Verify quickstarts in various web languages (and many frameworks). Each one shows you the fastest way to adding an important device verification step to your registration flow. Make sure you have a Twilio account before trying out this Quickstart.

216. Twilio instructs its customers to use two-factor authentication and Lookup to "help with your security flow," and describes when Twilio's customers' "app[s] ask[] users to register" on

[14] Exhibit X.

the same page, as shown at https://www.twilio.com/docs/verify.[15]



217. By way of example, the screen capture below from https://www.twilio.com/docs/api/rest/lookups[16] shows that Twilio instructs its customers to use Twilio Lookup to "[f]ind carrier information," as claimed by the '034 Patent.

218. By way of further example, the screen capture below from https://www.twilio.com/blog/2015/03/introducing-twilio-lookup.html shows that Twilio markets the

[15] Exhibit Y.
[16] Exhibit Z.

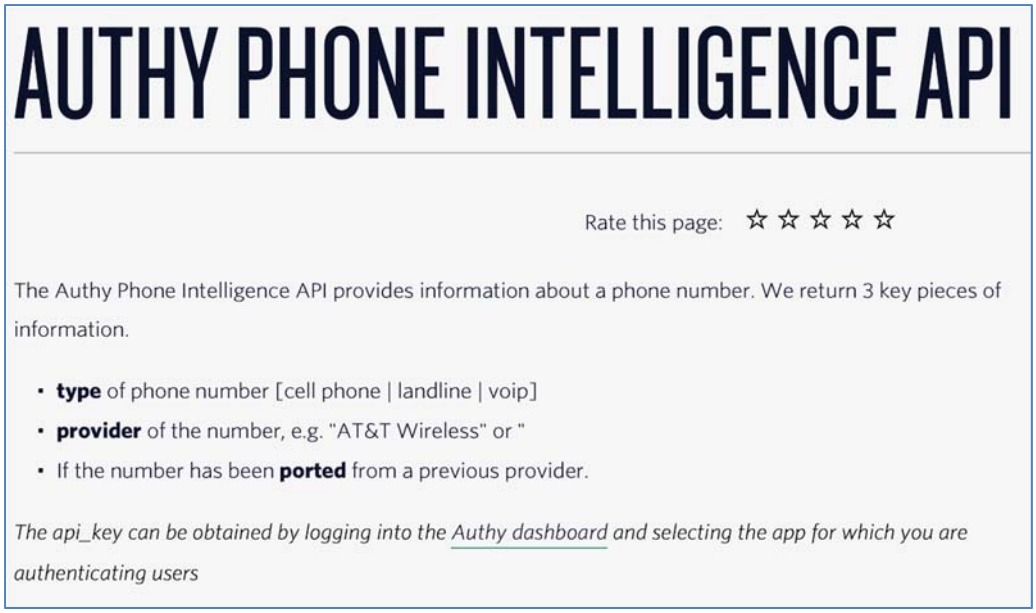
Lookup Products and instructs customers to use them.

> However, some seek to misuse those powers, and use phone numbers from free online providers to create fake profiles to defraud or spam businesses. Carrier & Type Lookup helps businesses identify the carrier behind the phone number to learn which users are more likely to be fraudulent.
>
> Additionally, you can improve deliverability by looking up number types that don't accept all communications. For example, most landline numbers and many VoIP numbers do not accept SMS messages. With Lookup, you can better identify which kind of communications users can accept, based on their number type. This allows businesses to recognize when an alternative delivery method may be needed to successfully send voice and messaging communications.

219. Twilio instructs and encourages its customers to infringe the '034 Patent by using Phone Intelligence as part of registering end users.

220. As an example, the screen capture below from https://www.twilio.com/docs/authy/api/phone-intelligence shows that Twilio instructs customers to use Phone Intelligence, including to "provide[] information about a phone number."

221. By way of further example, Twilio states on the same webpage at https://www.twilio.com/docs/authy/api/phone-intelligence that its customers can "select[] the app for which you are authenticating users, as shown below.



222. Twilio encourages developers to use Authy, Lookup, and/or Verify with respect to sending codes or messages.

223. Twilio encourages developers to use Authy, Lookup, and/or Verify with respect to registered devices or end-user sign-ups.

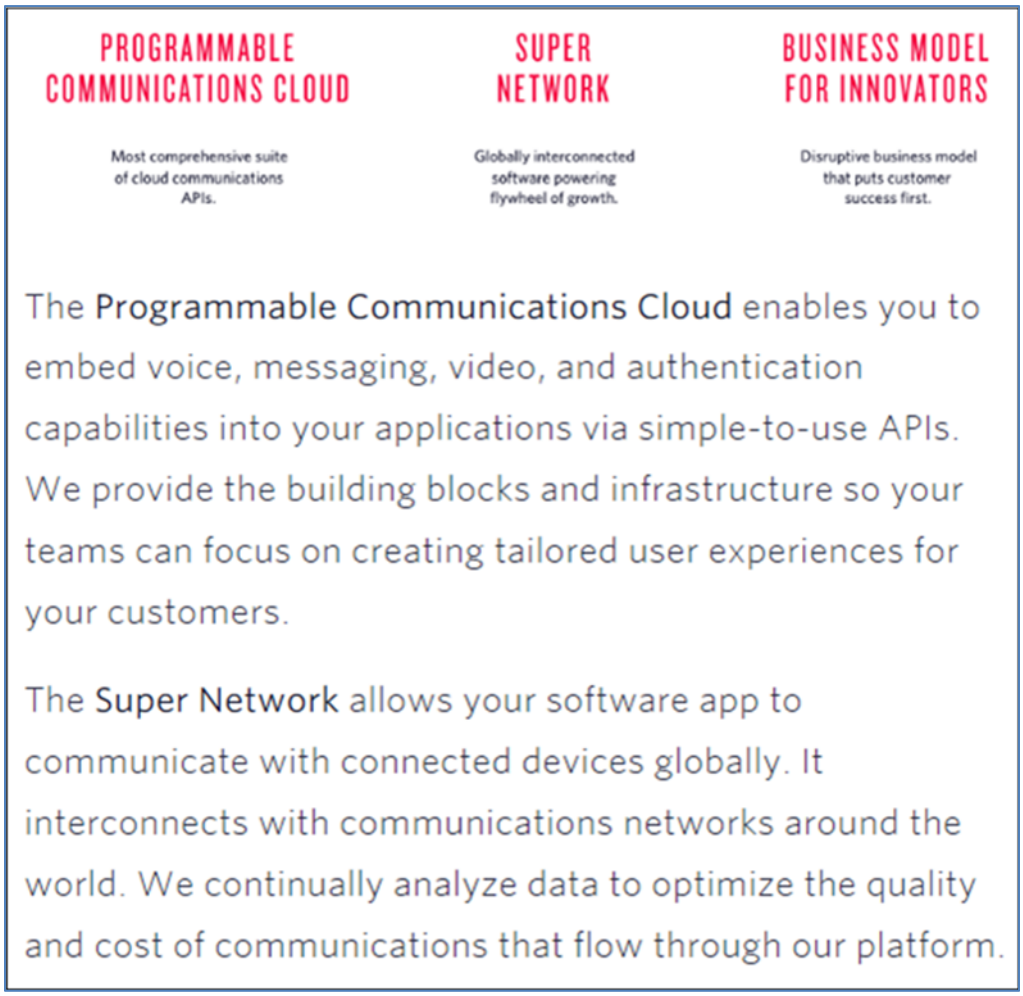
224. As to Authy, Twilio's 2017 10-K states (emphasis added): "Authy. Provides user authentication codes through a variety of formats based on the developer's needs. **Authentication codes** can be delivered through the Authy app on **registered** mobile phones, desktop, or smart devices or via SMS and voice automated phone calls. In addition, authentication can be determined through a push notification on **registered** smartphones." (Twilio 2017 Annual Report, p. 12)

225. As to Lookup, Twilio's 2017 10-K states (emphasis added): "Lookup. Allows developers to validate number format, device type, and provider prior to **sending messages** or initiating calls." (Twilio 2017 Annual Report, p. 12)

226. As to Verify, Twilio's 2017 10-K states (emphasis added): "Verify. Allows developers to deliver a one-time passcode through SMS or voice to verify that a user is in possession of the device being **registered**." (Twilio 2017 Annual Report, p. 12)

227. By way of further example, the screen capture below from https://www.twilio.com/learn/twilio-101/why-businesses-need-programmable-communications

shows that Twilio instructs customers to use its Programmable Communications Cloud and Super Network, including to "embed…authentication capabilities" and "communicate with connected devices globally."



228. Twilio's 2017 10-K describes its "Programmable Communications Cloud" as follows: "Our Programmable Communications Cloud consists of software for voice, messaging, video and authentication that empowers developers to build applications that can communicate with connected devices globally. We do not aim to provide complete business solutions, rather our Programmable Communications Cloud offers flexible building blocks that enable our customers to build what they need." (Twilio 2017 Annual Report, p. 12)

229. By way of further example, the screen capture below from https://www.twilio.com/press/releases/release-twilio-proxy shows that Twilio instructs customers to

use its Engagement Cloud and "the Twilio Two-factor Authentication service for stronger account security."


Twilio Engagement Cloud

Twilio Proxy is part of the Twilio Engagement Cloud, a new suite of Declarative APIs that are embedded with logic for common multi-channel customer experience uses cases. Declarative APIs retain the flexibility of Twilio's programmable APIs, with added business process and logic already built in. These next-generation APIs enable developers to build more rapidly with less coding, and are designed to help businesses get to production scale faster than ever before.

The Twilio Engagement Cloud also includes Twilio Notify, software for orchestrating automated notifications across messaging channels; Twilio TaskRouter, routing software to create smarter contact center workflows; and the Twilio Two-factor Authentication service for stronger account security. To learn more, please visit http://www.twilio.com/engagement-cloud.

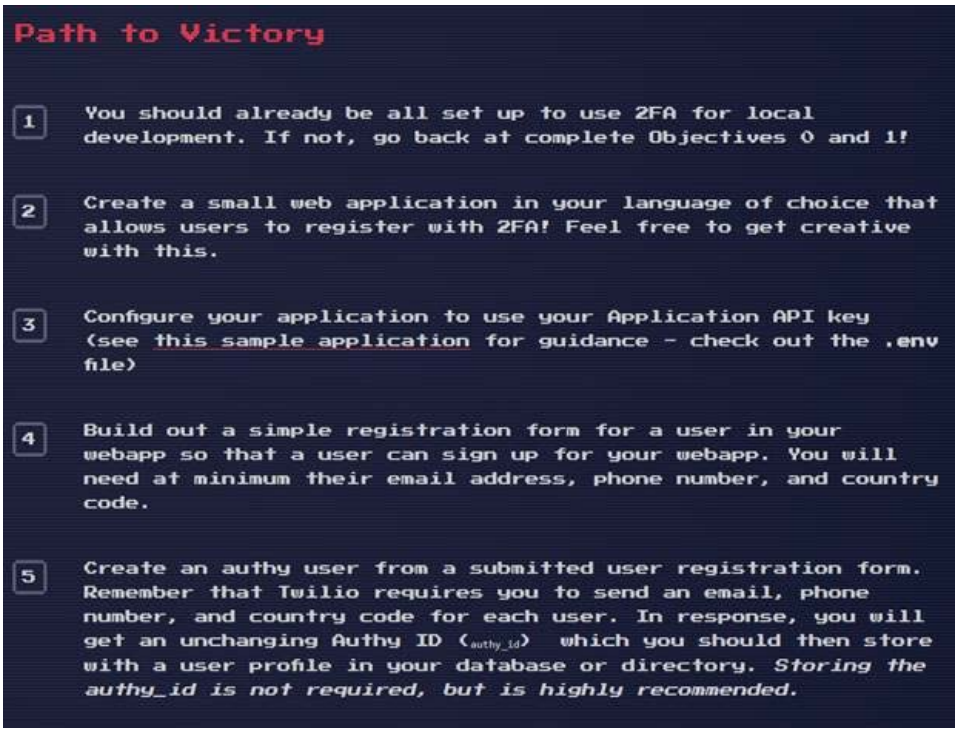
230. Regarding Twilio's Engagement Cloud, Twilio's 2017 10-K states: "While developers can build a broad range of applications on our platform, certain use cases are more common. Our Engagement Cloud APIs build upon our Programmable Communications Cloud to offer more fully implemented functionality for a specific purpose, such as two-factor authentication or skills-based routing in a contact center, thereby saving developers significant time in building their applications." (Twilio 2017 Annual Report, p. 11)

231. By way of further example, Twilio has provided an "interactive, self-paced game" for its customers to "learn how to Twilio," to help its customers "master Voice, SMS, Video or our other products" entitled "Twilio Quest," as shown at https://www.twilio.com/quest/welcome, with knowledge of the asserted patent claims.

232. "Twilio Quest" instructs Twilio customers to implement 2FA during registration of their end users.

233. For example, as shown at https://www.twilio.com/quest/mission/4, Twilio instructs its customers to use its verification to "complete [users'] registration!"

234. Also for example, as shown at https://www.twilio.com/quest/mission/4/objective/38, Twilio tells its customers to "Build out a simple registration form" and "[c]reate an authy user."



235. When Twilio's customers perform all of the claimed steps of the '034 Patent Asserted Claims as instructed by Twilio, Twilio's customers directly infringe the '034 Patent.

236. When Twilio performs one or more steps of the Asserted Claims of the '034 Patent as contracted by its customers, such as receiving a telephone number and determining the type of phone, the phone carrier and geographic characteristics associated with the telephone number, the performance of theses step(s) are attributable to Twilio's customers as described above in Section VIII regarding Twilio's actions attributable to its customers. When Twilio performs one or more

other steps, such as connecting to a telephone associated with the telephone number and communicating a verification message with the telephone, the performance of these step(s) are attributable to Twilio's customers as described above in Section VIII.

237. TeleSign has been damaged by Twilio's inducement of infringement of the '034 Patent and will suffer additional irreparable damage unless Twilio is enjoined from continuing to induce infringement of the '034 Patent.

XIII. COUNTS III & IV - Direct Infringement of the '920 and '038 Patents

238. TeleSign repeats and realleges each of the allegations contained in the paragraphs above.

239. Defendant Twilio has infringed the '920 and '038 Patents and is liable as an infringer under 35 U.S.C. § 271(a).

240. Illustrative direct-infringement example: Regarding Twilio, Twilio's 2017 Annual Report states that as "of December 31, 2017, we had 48,979 Active Customer Accounts and well over one million **registered** developer accounts registered on our platform." (Emphasis added). Twilio directly infringes the '920 and '038 patents when it uses its 2FA Products including, for example, Authy, to verify and re-verify users (customers and/or developers to the extent there's a difference) attempting to, for example, access restricted areas of Twilio's website, including, for example, logging in to Twilio's Account Portal, attempting to perform account maintenance, such as attempting to update a password, username, email address; or attempting to perform some other act that merits user verification. Twilio's Account Portal presents a registration form that receives users' phone numbers, which are verified by Twilio using its 2FA Products. Reverifications are incident to the occurrence of notification events that Twilio establishes, such when Twilio users attempt to log into their Twilio accounts from an unrecognized device, browser, app, etc. (*e.g.*, a device different from the one that was initially used to register with Twilio), change a password, or perform another important action. Twilio customers are considered verified and/or re-verified when they input codes that match the codes send to them via Twilio's 2FA Products.

241. On June 11, 2013, United States Patent No. 8,462,920, entitled "Registration, verification and notification system," was duly and legally issued by the United States Patent and Trademark Office.

242. On April 1, 2014, United States Patent No. 8,687,038, entitled "Registration, verification and notification system," was duly and legally issued by the United States Patent and Trademark Office.

243. Plaintiff TeleSign is the owner of the '920 Patent with full rights to pursue recovery of royalties or damages for infringement of the '920 Patent, including full rights to recover past and future damages.

244. Each claim of the '920 Patent is valid and enforceable.

245. Plaintiff TeleSign is the owner of the '038 Patent with full rights to pursue recovery of royalties or damages for infringement of the '038 Patent, including full rights to recover past and future damages.

246. Each claim of the '038 Patent is valid and enforceable.

247. Twilio makes, sells, offers for sale, uses and/or imports, in the United States the Twilio Account Portal and Authy, which directly infringe the '920 and '038 Patent Asserted Claims.

248. Defendant Twilio has infringed the '920 and '038 Patents and, unless enjoined, will continue to do so, by using, offering for sale and selling services claimed by the '920 and '038 Patents.

249. The Twilio Account Portal and Authy are made available through Twilio's website at www.twilio.com.

250. The '920 and '038 Patents relate to, among other things, verifying a contact by using a verification code, notification, and re-verifying.

251. The Twilio Account Portal and Authy include executable instructions to perform and do perform a verification method as claimed.

XIII(A). First Direct Infringement Example for the '920 and '038 Patents

252. The Twilio Account Portal includes the performance of each step of the methods

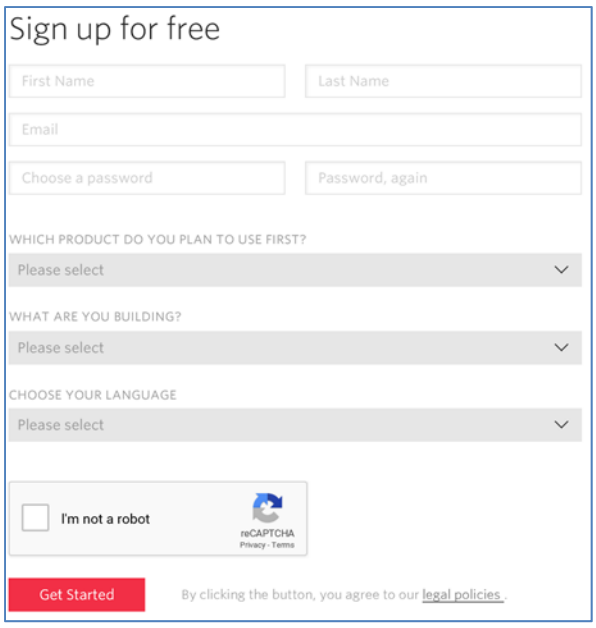
claimed by the '920 and '038 Patents.

253. The Twilio Account Portal uses two-factor authentication including a verification code.

254. The Twilio Account Portal receives information from a customer, such as the customer's email address, password, and telephone number (*e.g.*, a mobile phone number), via an interface such as Twilio's website presented to the customer.

255. An interface is presented when a customer attempts to register with Twilio and to access restricted portions of Twilio's website (*e.g.*, past the login screens at https://www.twilio.com/login; https://dashboard.authy.com/signin; and https://www.twilio.com/try-twilio) or when a customer attempts to enable 2FA account protection on an existing account.

256. For example, in the screenshot below from https://www.twilio.com/try-twilio, customer information (name, email, products of interest, applications of interest, programming language, etc.) is received as a customer attempts to register with Twilio.

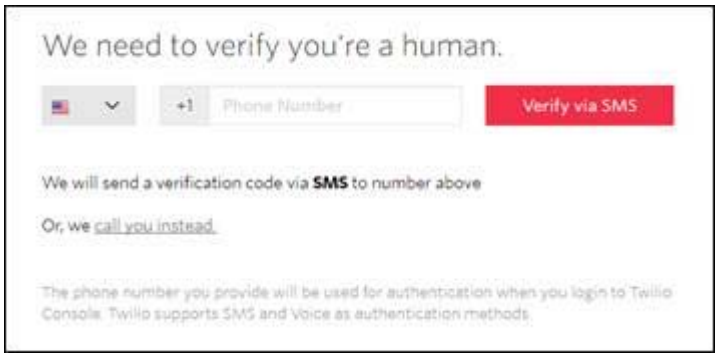


257. The Twilio Account Portal verifies the customer's telephone number by sending a verification code via SMS to the user's telephone number.

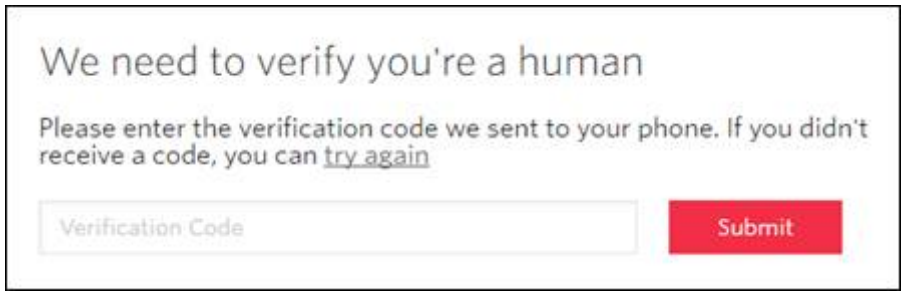
258. For example, the Twilio Account Portal texts the customer a code that is used as a verification code. The Twilio Account Portal also communicates verification codes to customers via

phone calls to customers' devices.

259. As illustratively shown below—after a customer provides the information from the former sign-up screen, Twilio requests a phone number and indicates that the phone number "will be used for authentication" when logging into Twilio's website. This is shown in the screenshot below.



260. The Twilio Account Portal then sends a code to the potential registrant. This is illustrated below.



261. The Twilio Account Portal receives a response from the customer via the aforementioned computing interface (*e.g.*, the Twilio website). The response—a submitted verification code—is a response to the verification code the Twilio Account Portal sent.

262. The Twilio Account Portal verifies the telephone number by checking whether the user-submitted verification code is the same as the verification code that the Twilio Account Portal sent. If it is, the Twilio Account Portal will consider the telephone number verified and will complete a registration of the customer based on the received and verified telephone number. For example, the Twilio Account Portal will store at least some of the information (*e.g.*, name, address, telephone number) if the customer-submitted code matches the code that Twilio Account Portal sent. By way of further example, the Twilio Account Portal also stores an indication enabling 2FA account protection using the verified telephone number for the customer's Twilio account if a match

occurs and the received telephone number was able to be verified.

263. As used herein, the term "Twilio Account Portal" also includes Twilio's executable code for maintaining records (which Twilio does maintain) of one or more notification events associated with actions that require acknowledgement by the user. For example, Twilio Account Portal facilitates the storage of information regarding login attempts, including login attempts from untrusted computers, information regarding attempts to change one's verified phone number, and when a certain number of days have lapsed. The occurrence of those events leads to users being notified.

264. Twilio has two-factor authentication "active" for logging onto to Twilio accounts.

265. By way of example, Twilio has two-factor authentication active for accounts using the Twilio Account Portal, for example "Authy account[s]" that are used for "Authy development," as shown below and stated at https://www.twilio.com/blog/2017/10/easily-manage-team-access-to-the-twilio-console.html.

> While a single-user is the easiest way to approach Authy development, keep in mind that there are some limitations:
>
> - Since 2FA is active when you create an Authy account, you cannot share accounts.

266. Twilio states two-factor authentication including voice and SMS notifications are used, for example, with Twilio customer accounts that are used with a "new device," for example as shown at https://www.twilio.com/blog/2011/11/twilio-two-factor-authentication.html.

> **Phone-Based Two-factor Authentication Is A Better Way to Stay Secure**
>
> **Two-factor authentication with voice and SMS notifications**
>
> Here's how it works, as a user:
>
> 1. You sign up for an online service, and enter your cell (or home) phone number during the sign up process.
> 2. Later, the first time you sign in on a new device or browser, the service either sends you a text message with a verification code or calls you and reads the code back to you.

267. The Twilio Account Portal can also facilitate sending messages to customer devices such as iPads, Android devices, and PCs via apps installed on those devices and associated with the customer (*e.g.*, by way of the user's phone number).

XIII(B). Second Direct Infringement Example for the '920 and '038 Patents

268. Authy includes the performance of each step of the methods claimed by the '920 and '038 Patents.

269. As to Authy, Twilio's 2017 10-K states (emphasis added): "Authy. Provides user authentication codes through a variety of formats based on the developer's needs. **Authentication codes** can be delivered through the Authy app on registered mobile phones, desktop, or smart devices or via SMS and voice automated phone calls. In addition, authentication can be determined through a push notification on registered smartphones." (Twilio 2017 Annual Report, p. 12)

270. Authy includes executable instructions to perform and does perform a verification method as claimed.

271. With reference to the Asserted Claims, Authy receives information from a user, such as the user's telephone number (*e.g.*, mobile phone number) via a form or website. Illustrative computing interfaces include a website presented to the user, a mobile app (such as the Authy Mobile App), or the Authy API (including, for example, the TOTP API).

272. This form or site is presented when a user attempts to access a service, such as a customer's protected application (including one built using an Authy SDK), a protected portion of a customer's website, or when a user attempts to access Authy itself (being a service available to protect registered users).

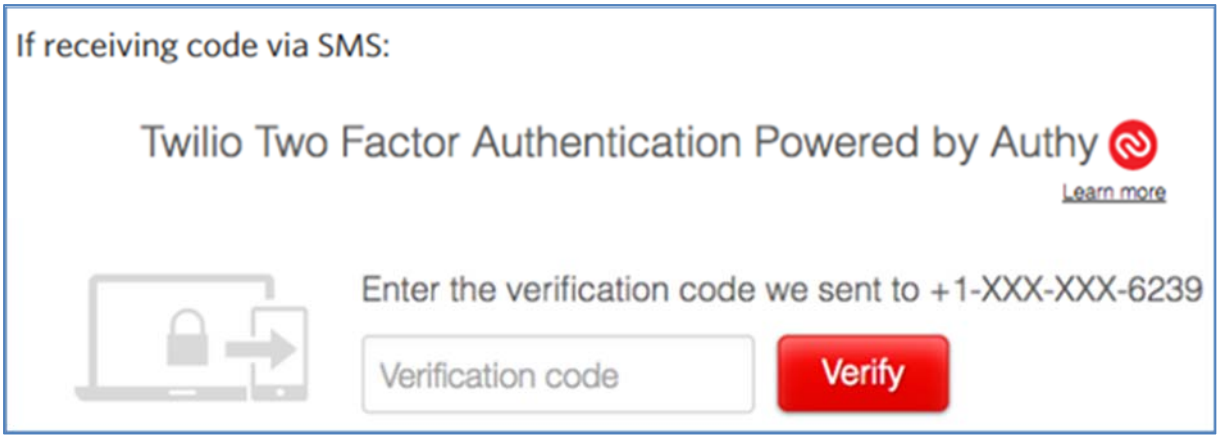
273. Authy verifies the user's telephone number by sending a verification code via SMS to the user's telephone number (or equivalent). For example, Authy facilitates texting the user a code that is used as a verification code (*e.g.*, Authy OneCode). Authy also communicates verification codes to users via phone calls to the user's phone. Authy can also request verification via user devices such as iPads, Android devices, and PCs via apps installed on those devices and associated with the user (*e.g.*, by way of the user's phone number).

274. Authy receives a response from the user via the aforementioned computing interface (*e.g.*, website, a mobile app, an interface utilizing an Authy API). The response—a submitted verification code—is a response to the verification code Authy sent.

275. Authy verifies the telephone number, checking whether the user-submitted verification code is the same as the verification code that Authy sent. If it is, Authy will consider the telephone number verified and will complete the registration of the user based on the received and verified telephone number. For example, Authy will store at least some of the information (*e.g.*, the telephone number or registered device information) if the user-submitted code matches the code Authy sent. By way of further example, Authy also stores an indication allowing SMS token verification using the verified telephone number to be enabled for the user's Authy account if a match occurs and the received telephone number was able to be verified. This completed registration allows a user to access the functionality of Authy (be able to use it).

276. Authy maintains records associated with actions, for example, Authy stores user activities (*e.g.*, "password_reset"), application stats (*e.g.*, "sms_count"), and actions (*e.g.*, "action=login&action_message='Login code'") including adding a new device. Authy facilitates re-verification, which may be established by Authy or Twilio's customer, for example.

277. Authy uses a verification code, as shown at https://www.twilio.com/blog/2017/08/securing-your-twilio-account-with-2fa.html,



278. Authy uses re-verification, for example as shown at https://authy.com/blog/introducing-authy-for-your-personal-computer/.

> When you register your laptop as a new device with the Authy App for PCs, we use the same secure registration process we use with the mobile app by verifying your identity with your cellphone number – something only you have access to.

279. Authy can also facilitate sending messages to user devices such as iPads, Android devices, and PCs via apps installed on those devices (*e.g.*, via Authy OneTouch) and associated with the user (*e.g.*, by way of the user's phone number).

280. Authy then receives a user acknowledgement, directly from the user, or by way of the Authy API (*e.g.*, to verify the user's token). For example, Authy receives an indication from the user that the established event is legitimate.

* * *

281. Over time Twilio has branded or identified its technology or uses cases with different names and as various "building blocks." Regardless, Twilio has used that technology and those "building blocks" as part of its 2FA Products, to infringe the claims of the '920 and '038 Patents by carrying out the accused functionality of, for example, receiving information including at least one electronic contact; verifying by establishing a first telephonic connection, communicating a verification code, receiving a first submitted verification code, and verifying the received electronic contact if the submitted verification code is the same as the communicated verification code; establishing a notification event, and after identifying the occurrence of the established notification event, re-verifying the electronic contact.

282. Regarding Twilio's Engagement Cloud, Twilio's 2017 10-K states: "While developers can build a broad range of applications on our platform, certain use cases are more common. Our Engagement Cloud APIs build upon our Programmable Communications Cloud to offer more fully implemented functionality for a specific purpose, such as two-factor authentication or skills-based routing in a contact center, thereby saving developers significant time in building

their applications." (Twilio 2017 Annual Report, p. 11)

283. As to Verify, Twilio's 2017 10-K states: "Verify. Allows developers to deliver a one-time passcode through SMS or voice to verify that a user is in possession of the device being registered." (Twilio 2017 Annual Report, p. 12)

284. Twilio's 2017 10-K describes its "Programmable Communications Cloud" as follows: "Our Programmable Communications Cloud consists of software for voice, messaging, video and authentication that empowers developers to build applications that can communicate with connected devices globally. We do not aim to provide complete business solutions, rather our Programmable Communications Cloud offers flexible building blocks that enable our customers to build what they need." (Twilio 2017 Annual Report, p. 12)

285. Twilio's infringement is facilitated using one or more of Twilio's controlled data centers or internal servers that store user-specific information and/or notification events.

286. Twilio implements processes for re-verifying users that it recommends to its customers.

287. Twilio recommends that its customers implement on-going two-factor authentication.

288. Twilio instructs its customers to re-verify their end users based on events.

289. Twilio instructs its customers to use two-factor authentication including voice and SMS notifications.

290. TeleSign has been damaged by Twilio's infringement of the '920 and '038 Patents and will suffer additional irreparable damage unless Twilio is enjoined from continuing to infringe the '920 and '038 Patents.

XIV. COUNTS V & VI - Active Inducement of Infringement of the '920 and '038 Patents

291. TeleSign repeats and realleges each of the allegations contained in the paragraphs above.

292. Defendant Twilio has induced infringement of the '920 and '038 Patents and is liable as an infringer under 35 U.S.C. § 271(b).

293. Illustrative inducement example: Twilio actively induces its customers to infringe the '920 and '038 patents in violation of 35 U.S.C. § 271(b). Aware of the '920 and '038 patents since TeleSign filed its initial lawsuit on April 30, 2015, Twilio has specifically intended and intends its customers to infringe the '920 and '038 Patents and knows that its customers' acts constitute infringement. For example, Twilio knows that its customers infringe the '920 and '038 Patents when they follow Twilio's recommendations, encouragements, tutorials, advice, and advertisements to employ 2FA Use Cases or Twilio's 2FA Products to verify their end users and to reverify them incident to the occurrence of notification events (such as attempting to log into their accounts from an unrecognized device, browser, app, etc. (*e.g.*, a device different from the one that was initially used to register with the Twilio customer), change a password, or perform another important action. Underlying direct infringement occurs when Twilio's customers, as instructed and encouraged by Twilio, verify their end users using a phone number received from a registration form, using, for example Twilio's 2FA Products; establish notification events such as those previously mentioned, and then re-verify their end users, using, for example, Twilio's 2FA Products when any of those notification events occur. The Twilio customers' end users are deemed verified when their customers provide a 2FA code that matches the one they were sent.

294. Twilio had knowledge of the '920 and '038 Patents as stated above regarding Twilio's Knowledge of the Asserted Patents.

295. Twilio has specific intent to encourage its customers' direct infringement of the '920 and '038 Patents.

296. Twilio has known, or is willfully blind to the fact, that it has been (at least since April 30, 2015) and is encouraging acts that constitute infringement of the Asserted Claims of the '920 and '038 Patents, including inducing its customers' infringement.

297. Twilio continues, with knowledge of the '920 and '038 Patents, to actively promote, encourage and teach customers to build applications that carry out all of the steps of the '920 and '038 Patents Asserted Claims.

298. Twilio continues to provide tutorials, including instructional videos, sample code,

customer support, demonstrations, and marketing materials that encourage and instruct its customers to infringe the '920 and '038 Patents Asserted Claims.

299. In the face of the knowledge of the '920 and '038 Patents as alleged above, Twilio continues (past April 30, 2015) to encourage its customers to use the 2FA Use Cases or 2FA Products to make, use, sell, offer to sell and import products and services that infringe the Asserted Claims of the '920 and '038 Patents with knowledge (or willful blindness) that its induced acts constitute patent infringement.

300. Twilio continues to offer and link to (and provide new webpages and links to) its tutorials, articles, and other materials that instruct customers to use Twilio's 2FA Use Cases or 2FA Products to provide verification including two-factor authentication including re-verifying.

301. Twilio's customers follow such tutorials to make, use, sell, and offer infringing applications and services, which will likely have evidentiary support after a reasonable opportunity for further investigation or discovery.

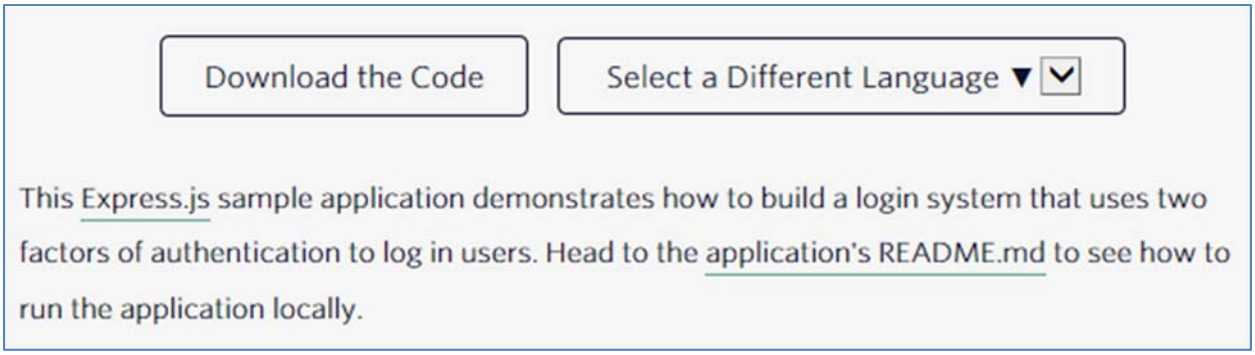
302. Twilio has continued maintaining and added to its instructions and encouragement to its customers to infringe TeleSign's Asserted Patent Claims with knowledge of the patent claims and its customers' infringement.

303. Twilio has provided and continues to provide tutorials instructing its customers to use 2FA Use Cases or 2FA Products.

304. For example, Twilio continues to provide its existing and new tutorials instructing its customers how to "Add[] two-factor authentication (2FA) to your web application" to increase security.

305. For example, at https://www.twilio.com/docs/authy/tutorials/two-factor-authentication-node-express,[17] Twilio provides tutorials to "demonstrate[] how to build a login system that uses two factors of authentication" as shown below.

[17] Exhibit AA.



306. Twilio has provided and continues to provide articles, customer support, and documents including API documentation that encourages its customers to use 2FA Use Cases or 2FA Products.

307. With knowledge of the '920 and '038 Patents and their claims, Twilio has not removed or taken down its instructional materials including tutorials and marketing encouragements, thereby knowing that the customer acts Twilio is inducing constitute patent infringement.

308. With knowledge of the '920 and '038 Patents and their claims, Twilio continues to provide instructions and has provided additional instructions, including articles, videos, conferences, customer support, sample code, or webpages.

309. Twilio continues to offer and link to its tutorials, articles, and other materials that instruct customers to perform verification and notification processes as claimed in the '920 and '038 Patents, including re-verifying users—all with knowledge (or willful blindness) that these induced acts constitute patent infringement.

310. Twilio's customers use the 2FA Use Cases or 2FA Products or they contract with Twilio for use of Twilio's services that perform steps claimed by the '920 and '038 Patents.

311. Twilio advertises and instructs its customers to use the 2FA Use Cases or 2FA Products as claimed by the '920 and '038 Patents.

312. Twilio continues to offer and instruct its customers to use 2FA Use Cases or 2FA Products, despite knowledge of the '920 and '038 Patents Asserted Claims and knowledge that its customers' acts constitute direct infringement of the '920 and '038 Patents.

313. By way of example only, Twilio instructs its customers to use the 2FA Use Cases or

2FA Products, as described at https://www.twilio.com/docs/howto/two-factor-authentication,[18] which states "[w]ith Twilio you can set up your two-factor authentication system to run on a devices [sic] all of your employees already carry with them."

314. Twilio instructs its customers to use two-factor authentication to re-verify.

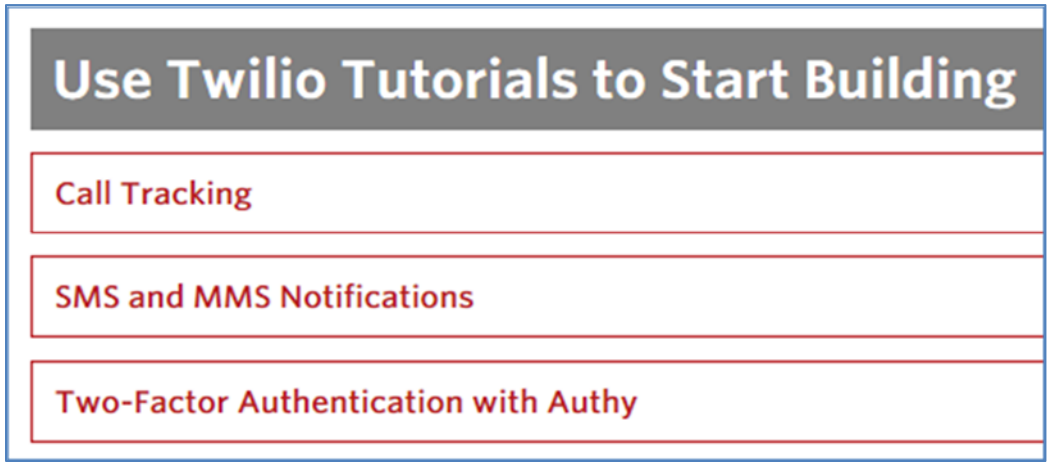
315. For example, Twilio states at https://www.twilio.com/blog/2011/11/twilio-two-factor-authentication.html:[19] "Two-factor authentication with voice and SMS notifications Here's how it works, as a user: 1.You sign up for an online service, and enter your cell (or home) phone number during the sign up process. 2.Later, the first time you sign in on a new device or browser, the service either sends you a text message with a verification code or calls you and reads the code back to you. 3.You enter the verification code on the login page and you are granted access."

316. By way of further example, Twilio encourages and knows that its customers use the 2FA Use Cases or 2FA Products for re-verification, for example when Twilio's customers' end users attempt to use "a new computer or phone" with their account, as shown at https://www.twilio.com/blog/2014/02/send-safely-uses-twilio-two-factor-authentication-nt.html.

> to protect your account on different devices. They'll send a passcode challenge via SMS when you register a new computer or phone with your account. If you need a whole new

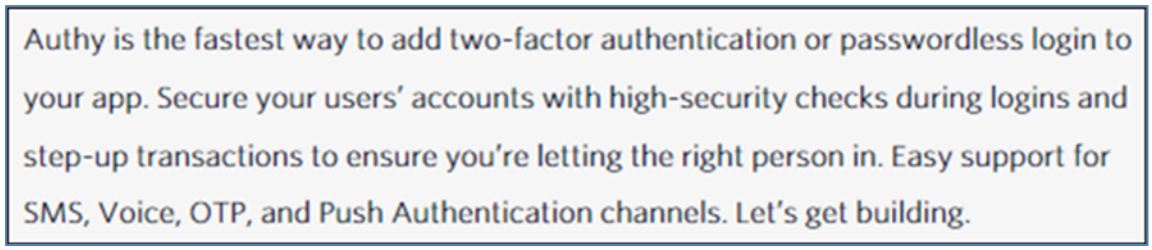
317. On the same webpage, Twilio instruct its customers to "Start Building," including by using Twilio's Tutorial for "Two-Factor Authentication with Authy."

[18] Exhibit BB.
[19] Exhibit CC.



318. Twilio encourages its customers to use two-factor authentication including by implementing Authy.

319. By way of example, the screen capture below from https://www.twilio.com/docs/authy[20] shows that Twilio instructs customers to use two-factor authentication via Authy, including to "[s]ecure your users' accounts with high-security checks during logins and step-up transactions to ensure you're letting the right person in."

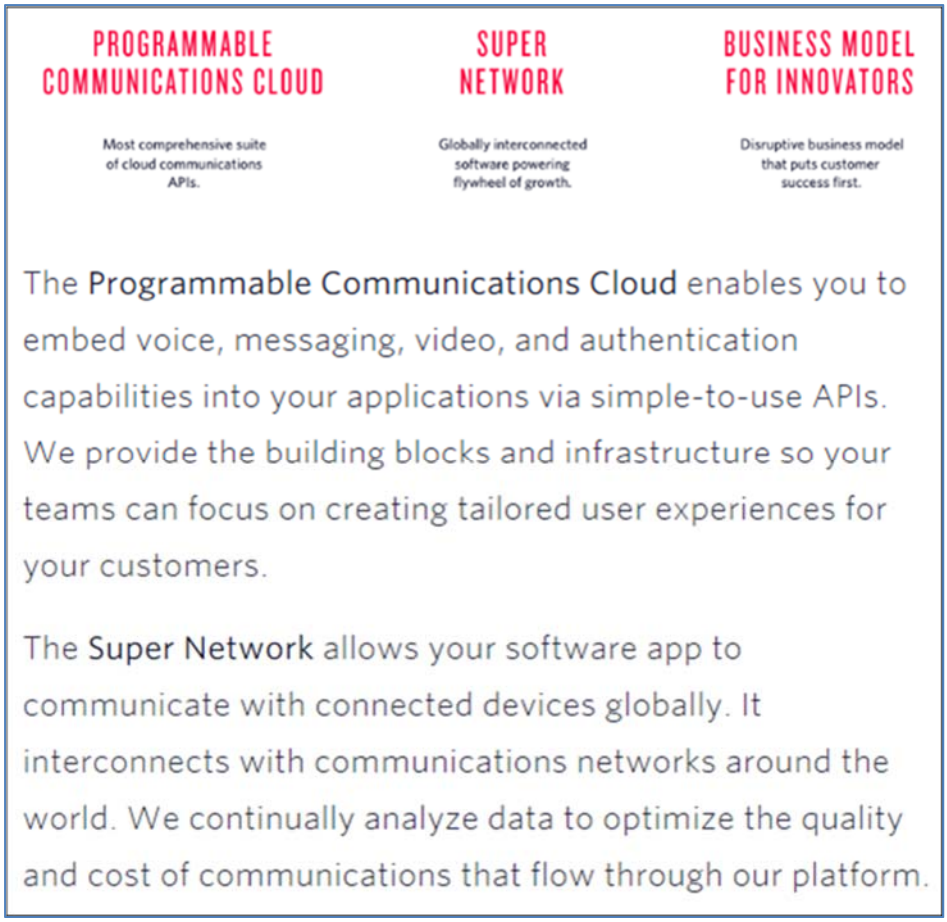


320. By way of example, the screen capture below from https://www.twilio.com/press/releases/release-twilio-proxy shows that Twilio instructs customers to use its Engagement Cloud and "the Twilio Two-factor Authentication service for stronger account security."

[20] Exhibit K.

> Twilio Engagement Cloud
> Twilio Proxy is part of the Twilio Engagement Cloud, a new suite of Declarative APIs that are embedded with logic for common multi-channel customer experience uses cases. Declarative APIs retain the flexibility of Twilio's programmable APIs, with added business process and logic already built in. These next-generation APIs enable developers to build more rapidly with less coding, and are designed to help businesses get to production scale faster than ever before.
> The Twilio Engagement Cloud also includes Twilio Notify, software for orchestrating automated notifications across messaging channels; Twilio TaskRouter, routing software to create smarter contact center workflows; and the Twilio Two-factor Authentication service for stronger account security. To learn more, please visit http://www.twilio.com/engagement-cloud.

321. As an example, the screen capture below from https://www.twilio.com/learn/twilio-101/why-businesses-need-programmable-communications shows that Twilio instructs customers to use its Programmable Communications Cloud and Super Network, including to "embed…authentication capabilities" and "communicate with connected devices globally."



322. Twilio's 2017 10-K describes its "Programmable Communications Cloud" as follows: "Our Programmable Communications Cloud consists of software for voice, messaging, video and authentication that empowers developers to build applications that can communicate with connected devices globally. We do not aim to provide complete business solutions, rather our

Programmable Communications Cloud offers flexible building blocks that enable our customers to build what they need." (Twilio 2017 Annual Report, p. 12)

323. Regarding Twilio's Engagement Cloud, Twilio's 2017 10-K states: "While developers can build a broad range of applications on our platform, certain use cases are more common. Our Engagement Cloud APIs build upon our Programmable Communications Cloud to offer more fully implemented functionality for a specific purpose, such as two-factor authentication or skills-based routing in a contact center, thereby saving developers significant time in building their applications."

324. Twilio encourages developers to use Verify with respect to sending codes or messages.

325. As to Verify, Twilio's 2017 10-K states: "Verify. Allows developers to deliver a one-time passcode through SMS or voice to verify that a user is in possession of the device being registered." (Twilio 2017 Annual Report, p. 12)

326. Twilio's 10-K states that its customer "uses our Programmable Voice products and Programmable Messaging products in its applications to verify new and existing users on its service." (Twilio 2017 Annual Report, p. 28)

327. Twilio instructs and encourages its customers to infringe the '920 and '038 Patents using the accused products above, which store user-specific information and/or notification events.

328. Twilio actively induces customers to directly infringe the '920 and '038 Patents, and Twilio's customers directly infringe by making, using, selling, offering to sell, or importing directly infringing products.

329. When Twilio's customers perform the claimed steps of the '920 and '038 Patents as instructed by Twilio, Twilio's customers directly infringe the '920 and '038 Patents.

330. When Twilio performs one or more steps of the Asserted Claims of the '920 and '038 Patents as contracted by Twilio's customers, such as establishing a first telephonic connection, communicating a first verification code, establishing a second telephonic connection, and/or communicating a second verification code, the performance of the one or more step(s) are

attributable to Twilio's customers as described above in Section VIII regarding Twilio's actions attributable to its customers. When Twilio performs the steps of receiving a second submitted verification code and re-verifying, the performance of the one or more steps are attributable to Twilio's customers as described above in Section VIII.

331. TeleSign has been damaged by Twilio's inducement of infringement of the '920 and '038 Patents and will suffer additional irreparable damage unless Twilio is enjoined from continuing to induce infringement the '920 and '038 Patents.

XV. COUNT VII – Direct Infringement - Direct Infringement of the '792 Patent.

332. TeleSign repeats and realleges each of the allegations contained in the paragraphs above.

333. Defendant Twilio has infringed the '792 Patent and is liable as an infringer under 35 U.S.C. § 271(a).

334. Illustrative direct-infringement example: Regarding Twilio, Twilio's 2017 Annual Report states (p. 9) that as "of December 31, 2017, we had 48,979 Active Customer Accounts and well over one million registered developer accounts registered on our platform." Twilio directly infringes the '792 Patent when it uses its 2FA Products including, for example, Authy, to register users (customers and/or developers to the extent there's a difference) attempting to, for example, access restricted areas of Twilio's website or to otherwise store user-specific information about the user (such as whether they are verified, not verified, in-progress, etc.). Twilio's Account Portal receives users' phone numbers via an interface (*e.g.*, login screen), which are verified by Twilio using its 2FA Products (including its Programmable Messaging Cloud) to send verification messages to users via Twilio's Super Network. Twilio completes the registration of a user based on the user's response the verification messages sent, allowing them to proceed past the login screen if the codes match. Twilio maintains a set of notification events, such when Twilio users attempt to log into their Twilio accounts from an unrecognized device, browser, app, etc. (*e.g.*, a device different from the one that was initially used to register with Twilio), when users try to change their profile (update a

password, contact information, etc.), or when users attempt some other important action that deserves user acknowledgement. When one of those notification events occurs, Twilio uses its 2FA Products to send the user a message via its Super Network indicating the occurrence of the event. Twilio receives acknowledgement of the action when the user, for example, favorably responds to a test message, an in-app message, etc. Receiving the user acknowledgement allows the requested action to occur. Twilio indicates that the phone number is verified when it is (*e.g.*, when both the sent and received 2FA code match).

335. On March 29, 2016, United States Patent No. 9,300,792, entitled "Registration, verification and notification system," was duly and legally issued by the United States Patent and Trademark Office.

336. Plaintiff TeleSign is the owner of the '792 Patent with full rights to pursue recovery of royalties or damages for infringement of the '920 Patent, including full rights to recover past and future damages.

337. Claims 9 and 18 of the '792 Patent are valid and enforceable.

338. Twilio makes, sells, offers for sale, uses and/or imports, in the United States the Twilio Account Portal and Authy, which directly infringe the '792 Patent Asserted Claims.

339. Defendant Twilio has infringed the '792 Patent and, unless enjoined, will continue to do so, by using, offering for sale and selling services claimed by the '792 Patent.

340. The Twilio Account Portal and Authy are made available through Twilio's website at www.twilio.com.

341. The '792 Patent relates to, among other things, verifying a contact by using a verification code in connection with a registration.

342. The Twilio Account Portal and Authy include executable instructions to perform and do perform a verification and notification method as claimed.

XV(A). First Direct Infringement Example for the '792 Patent

343. The Twilio Account Portal uses a two-factor authentication including a verification code.

344. The Twilio Account Portal employs two-factor authentication and provides for users to be notified of the occurrence of notification events.

345. Twilio has two-factor authentication "active" for its customer accounts.

346. As an example, Twilio has two-factor authentication activated for its customers' "Authy account[s]" that are used for "Authy development," as stated at https://www.twilio.com/blog/2017/10/easily-manage-team-access-to-the-twilio-console.html.

> While a single-user is the easiest way to approach Authy development, keep in mind that there are some limitations:
>
> - Since 2FA is active when you create an Authy account, you cannot share accounts.

347. Twilio registers its customers as Twilio account holders.

348. For example, Twilio registers its customers as account holders as shown at https://www.twilio.com/legal/tos.

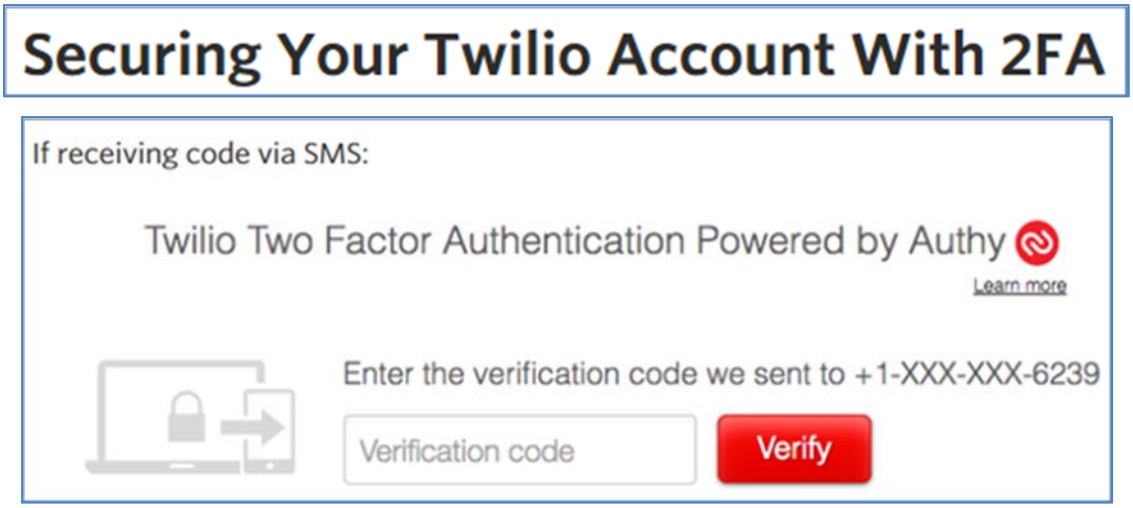
> To be eligible to register for a Twilio account and use Twilio's Services, you must review and accept the terms of this Agreement by clicking on the "I Accept"

349. Twilio informs its customers that they will "have to enable 2FA" to create applications using Twilio technology, for example as shown at https://www.twilio.com/blog/2017/10/easily-manage-team-access-to-the-twilio-console.html.

> For purposes of this post, we're focusing on account setup and user management in relation to Twilio's Authy two-factor authentication (2FA) solution, but the processes outlined below apply to all users of the Twilio Console regardless of the integration you're working with.
>
> If this is your first time setting up a Twilio account, you'll have to enable 2FA in order to create an Authy app. View our blog article about "Securing your Twilio Account With 2FA" for step-by-step instructions.

350. Twilio uses two-factor authentication including two-factor authentication powered by Authy to secure Twilio customer accounts

351. By way of example, as shown at https://www.twilio.com/blog/2017/08/securing-your-twilio-account-with-2fa.html, Twilio uses two-factor authentication for its customer accounts including accounts accessed using the Twilio Account Portal.



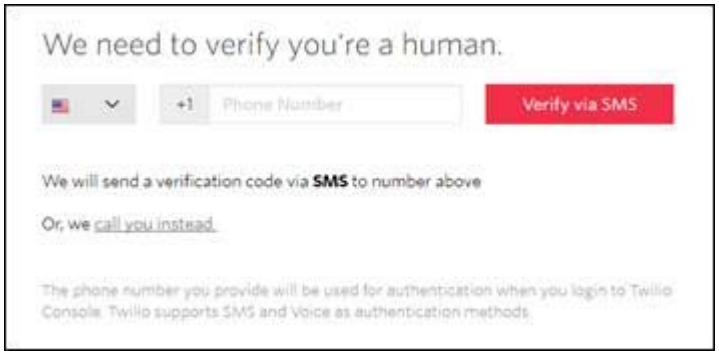
352. The Twilio Account Portal includes the performance of each step of the methods claimed by the '792 Patent.

353. The Twilio Account Portal receives information from a user, such as the user's email address, password, and telephone number (*e.g.*, a mobile phone number), via a computing interface such as Twilio's website presented to the user.

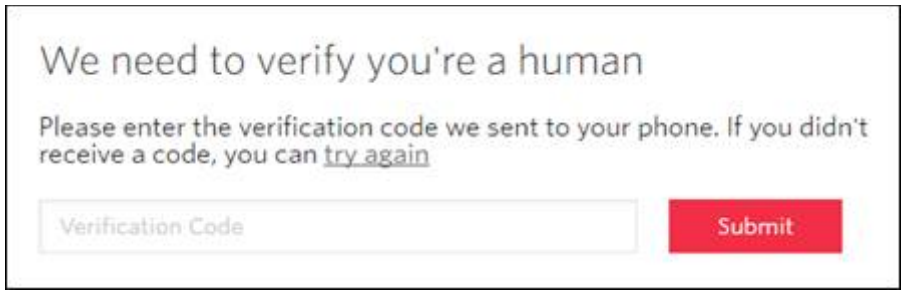
354. This computing interface is presented when a user attempts to register with Twilio and to access restricted portions of Twilio's website (*e.g.*, past the login screens at https://www.twilio.com/login and https://dashboard.authy.com/signin) and/or https://www.twilio.com/try-twilio) or when a user attempts to enable 2FA account protection on an existing account. For example, in the screenshot below, user information (name, email, products of interest, applications of interest, programming language, etc.) is received as a user attempts to register with Twilio.

355. The Twilio Account Portal verifies the user's telephone number by sending a verification code via SMS to the user's telephone number. For example, Twilio Account Portal texts the user a code that is used as a verification code. Twilio Account Portal also communicates verification codes to users via phone calls to the user's phone.

356. As illustratively shown below—after a user provides the information from the former sign-up screen, Twilio requests a phone number and indicates that the phone number "will be used for authentication" when logging into Twilio's website. This is shown in the screenshot below.



357. The Twilio Account Portal then sends a code to the potential registrant. This is illustrated below.



358. The Twilio Account Portal receives a response from the user via the aforementioned computing interface (*e.g.*, the Twilio website). The response—a submitted verification code—is a response to the verification code Twilio Account Portal sent.

359. The Twilio Account Portal verifies the telephone number by checking whether the user-submitted verification code is the same as the verification code that the Twilio Account Portal sent. If it is, the Twilio Account Portal will consider the telephone number verified and will complete a registration of the user based on the received and verified telephone number. For example, Twilio Account Portal will store at least some of the information (*e.g.*, name, address, telephone number) if the user-submitted code matches the code that the Twilio Account Portal sent. By way of further example, the Twilio Account Portal also stores an indication enabling 2FA account protection using the verified telephone number for the user's Twilio account if a match occurs and the received telephone number was able to be verified.

360. As used herein, the term "Twilio Account Portal" also includes Twilio's executable code for maintaining records (which Twilio does maintain) of one or more notification events associated with actions that require acknowledgement by the user. For example, the Twilio Account Portal facilitates the storage of information regarding login attempts, including login attempts from untrusted computers, information regarding attempts to change one's verified phone number, and when a certain number of days have lapsed. The occurrence of those events leads to users being notified.

361. When the Twilio Account Portal receives an indication that a notification event, *e.g.*, established by Twilio or the user, has occurred, it notifies the user and receives acknowledgement, such as by sending a message to the user's verified telephone number. For example, when the Twilio

Account Portal receives an indication that a customer is logging in from an untrusted computer (or other notification event), Twilio Account Portal sends a text message to provide notification to the user.

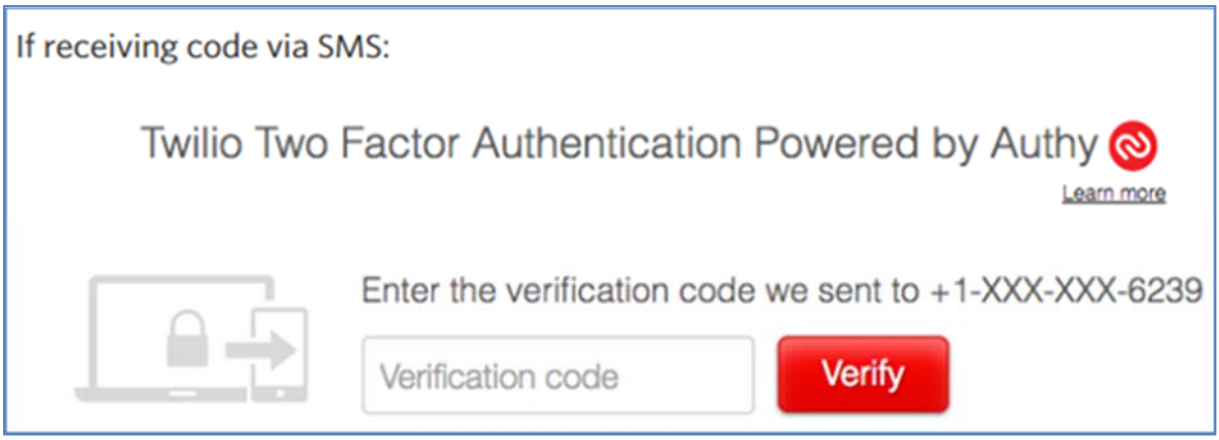
362. The Twilio Account Portal can also facilitate sending messages to user devices such as iPads, Android devices, and PCs via apps installed on those devices and associated with the user (*e.g.*, by way of the user's phone number).

363. The Twilio Account Portal then receives a user acknowledgement from the user (*e.g.*, by way of the Twilio website). For example, Twilio Account Portal receives an indication from the user that the occurrence of the established notification event is (or is not) authorized or expected.

364. The Twilio Account Portal associates a user's telephone number with data indicating it has been verified, which will likely have evidentiary support after a reasonable opportunity for further investigation or discovery.

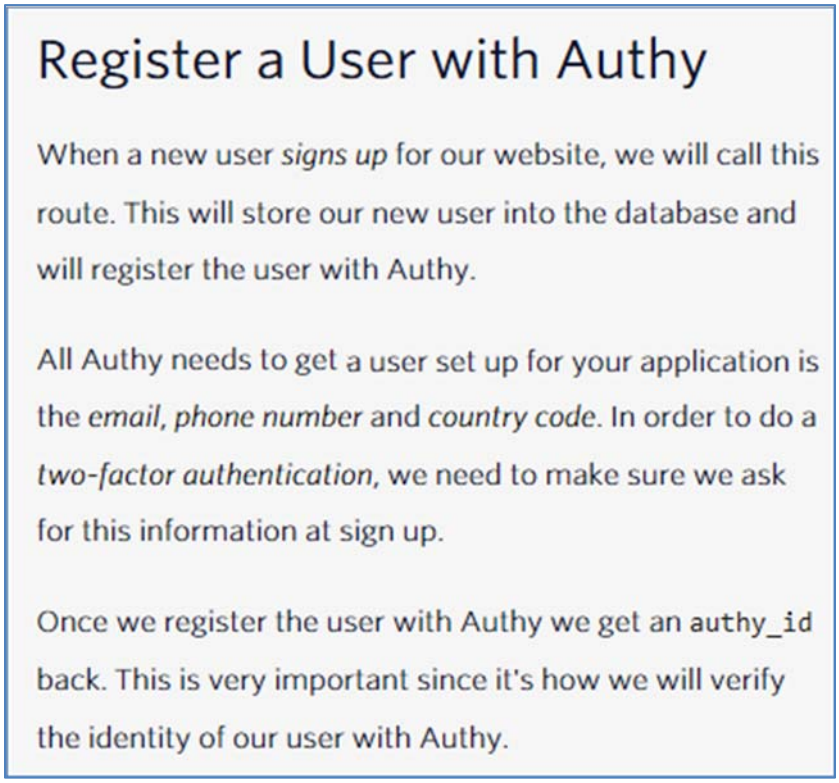
XV(B). Second Direct Infringement Example for the '792 Patent

365. Authy uses a verification code, as shown at https://www.twilio.com/blog/2017/08/securing-your-twilio-account-with-2fa.html,



366. Authy is used in connection with a registration by Twilio.

367. For example, Twilio uses Authy to perform two-factor authentication and "register[s] the user with Authy," as discussed at https://www.twilio.com/docs/authy/tutorials/two-factor-authentication-ruby-sinatra.



Register a User with Authy

When a new user *signs up* for our website, we will call this route. This will store our new user into the database and will register the user with Authy.

All Authy needs to get a user set up for your application is the *email*, *phone number* and *country code*. In order to do a *two-factor authentication*, we need to make sure we ask for this information at sign up.

Once we register the user with Authy we get an `authy_id` back. This is very important since it's how we will verify the identity of our user with Authy.

368. Authy registers users, for example as discussed at https://www.twilio.com/docs/authy/api/users.

> A user may have multiple email addresses but only one phone is associated with each authy_id. Two separate API calls to register a user with the same device and different emails will return the same `authy_id` and store both emails for that user.

369. Authy includes the performance of each step of the methods claimed by the '792 Patent.

370. As to Authy, Twilio's 2017 10-K states (emphasis added): "Authy. Provides user authentication codes through a variety of formats based on the developer's needs. **Authentication codes** can be delivered through the Authy app on **registered** mobile phones, desktop, or smart devices or via SMS and voice automated phone calls. In addition, authentication can be determined through a push notification on **registered** smartphones." (Twilio 2017 Annual Report, p. 12)

371. With reference to the Asserted Claims, Authy receives information from a user, such as the user's telephone number (*e.g.*, mobile phone number) via a computing interface. Illustrative computing interfaces include a website presented to the user, a mobile app (such as the Authy

Mobile App), or the Authy API (including, for example, the TOTP API).

372. This computing interface is presented when a user attempts to access a service, such as a customer's protected application (including one built using an Authy SDK), a protected portion of a customer's website, or when a user attempts to access Authy itself (being a service available to protect registered users).

373. Authy verifies the user's telephone number by sending a verification code via SMS to the user's telephone number (or equivalent). For example, Authy facilitates texting the user a code that is used as a verification code (*e.g.*, Authy OneCode). Authy also communicates verification codes to users via phone calls to the user's phone. Authy can also request verification via user devices such as iPads, Android devices, and PCs via apps installed on those devices and associated with the user (*e.g.*, by way of the user's phone number).

374. Authy receives a response from the user via the aforementioned computing interface (*e.g.*, website, a mobile app, an interface utilizing an Authy API). The response—a submitted verification code—is a response to the verification code Authy sent.

375. Authy verifies the telephone number, checking whether the user-submitted verification code is the same as the verification code that Authy sent. If it is, Authy will consider the telephone number verified and will complete the registration of the user based on the received and verified telephone number. For example, Authy will store at least some of the information (*e.g.*, the telephone number or other registered device information) if the user-submitted code matches the code Authy sent. By way of further example, Authy also stores an indication allowing SMS token verification using the verified telephone number to be enabled for the user's Authy account if a match occurs and the received telephone number was able to be verified. This completed registration allows a user to access the functionality of Authy (be able to use it).

376. Authy maintains records of one or more notification events associated with actions that require acknowledgement by the user. For example, Authy stores user activities (*e.g.*, "password_reset"), application stats (*e.g.*, "sms_count"), registered devices, and actions (*e.g.*, "action=login&action_message='Login code'") including adding a new device. Authy facilitates the

storage of other records of notification events, which may be established by Authy or Twilio's customer, for example.

377. When Authy receives an indication that a notification event occurs, it notifies the user and receives acknowledgement. When Authy receives an indication of an event, Authy sends an SMS message to the verified telephone number, and then receives a user response. For example, when Authy receives an indication of an improper login attempt (or other notification event), Authy sends a text message to provide notification to the user.

378. Authy can also facilitate sending messages to user devices such as iPads, Android devices, and PCs via apps installed on those devices (*e.g.*, via Authy OneTouch) and associated with the user (*e.g.*, by way of the user's phone number).

379. Authy then receives a user acknowledgement, directly from the user, or by way of the Authy API (*e.g.*, to verify the user's token). For example, Authy receives an indication from the user that the established event is legitimate.

380. Authy associates a user's telephone number with data indicating it has been verified, which will likely have evidentiary support after a reasonable opportunity for further investigation or discovery.

* * *

381. Over time Twilio has branded or identified its technology or uses case with different names and as various "building blocks." Regardless, it has used that technology and those "building blocks" as part of its "Programmable Communications Cloud," to infringe the claims of the '792 Patent by carrying out the accused functionality of receiving, from a user, information via a computing interface presented to the user as a result of an attempt by the user to access a service, including a telephone number associated with the user, verifying the telephone number by: establishing a short message service (SMS) connection with the user, communicating a verification code to the user, receiving a submitted verification code that is entered by the user, verifying the telephone number if the submitted verification code is the same as the communicated verification code, completing a registration of the user based on the received information and verified telephone

number, maintaining a record of one or more notification events associated with actions that require acknowledgement by the user, upon receiving an indication of an occurrence of an established notification event, transmitting a message addressed to the verified telephone number indicating the occurrence of the notification event, receiving, from the user, an acknowledgement of an action associated with the established notification event, and associating the telephone number with data indicating that the telephone number is verified.

382. Regarding Twilio's Engagement Cloud, Twilio's 2017 10-K states: "While developers can build a broad range of applications on our platform, certain use cases are more common. Our Engagement Cloud APIs build upon our Programmable Communications Cloud to offer more fully implemented functionality for a specific purpose, such as two-factor authentication or skills-based routing in a contact center, thereby saving developers significant time in building their applications."

383. As to Verify, Twilio's 2017 10-K states: "Verify. Allows developers to deliver a one-time passcode through SMS or voice to verify that a user is in possession of the device being registered." (Twilio 2017 Annual Report, p. 12)

384. Twilio's 2017 10-K describes its "Programmable Communications Cloud" as follows: "Our Programmable Communications Cloud consists of software for voice, messaging, video and authentication that empowers developers to build applications that can communicate with connected devices globally. We do not aim to provide complete business solutions, rather our Programmable Communications Cloud offers flexible building blocks that enable our customers to build what they need." (Twilio 2017 Annual Report, p. 12)

385. Twilio's infringement is facilitated by using one or more of Twilio's controlled data centers or internal servers that store user-specific information and/or notification events.

386. Twilio implements processes for verifying users that it recommends to its customers, which will likely have evidentiary support after a reasonable opportunity for further investigation or discovery.

387. Twilio recommends that its customers implement on-going two-factor authentication.

388. Twilio instructs its customers to use two-factor authentication including voice and SMS notifications.

389. TeleSign has been damaged by Twilio's infringement of the '792 Patent and will suffer additional irreparable damage unless Twilio is enjoined from continuing to infringe the '792 Patent.

XVI. COUNT VIII – Active Inducement of Infringement of the '792 Patent.

390. TeleSign repeats and realleges each of the allegations contained in the paragraphs above.

391. Defendant Twilio has induced infringement of the '792 Patent and is liable as an infringer under 35 U.S.C. § 271(b).

392. Illustrative inducement example: Twilio actively induces its customers to infringe the '792 Patent in violation of 35 U.S.C. § 271(b). Aware of the '792 Patent since its March 29, 2016 issuance via TeleSign filing its second lawsuit, Twilio has specifically intended and intends its customers to infringe the '792 Patent and knows that its customers' acts constitute infringement. For example, Twilio knows that its customers infringe the '792 Patent when they follow Twilio's recommendations, encouragements, tutorials, advice, and advertisements to verify their end users by employing 2FA Use Cases or using Twilio's 2FA Products as part of a registration process and then restrict certain actions (altering an account, changing a password, updating contact information, etc.) based on receiving acknowledgement from the registered end users in response to the occurrence of notification events (such as requests to alter an account, change a password, update contact information, etc.). Underlying direct infringement occurs when, for example, Twilio's customers receives a phone number, for example, from an end user attempting to access a service offered by the customer (*e.g.*, a protected portion of a website or a product or service offered only to registered users, etc.); verifies the telephone number by a Twilio 2FA Use Case or by using Twilio's 2FA Products to send a code to the end user have that end user disclose the same code; registers the user, including storing user-specific information about the user—and allowing access to the service when

the codes match; and when the customer— as instructed and encouraged by Twilio—requires user acknowledgement (*e.g.*, a verification or other permission grant) of an action (as mentioned) incident to the occurrence of a notification event (such as those mentioned). For example, in order to allow an end-user's password to be changed, Twilio's customer uses Twilio's 2FA Products to send a message addressed to the end user to make sure the change request is legitimate. Twilio's customer stores an indication that the received phone number is verified if it is (*e.g.*, both the sent and received 2FA code match).

393. Twilio had knowledge of the '792 Patent as stated above regarding Twilio's Knowledge of the Asserted Patents.

394. Twilio has specific intent to encourage its customers' direct infringement of the '792 Patent.

395. Twilio has known, or is willfully blind to the fact, that it has been (at least since March 31, 2016) and is encouraging acts that constitute infringement of the Asserted Claims of the '792 Patent, including inducing its customers' infringement.

396. Twilio continues, with knowledge of the '792 Patent, to actively promote, encourage and teach customers to build applications that carry out all of the steps of the '792 Patent Asserted Claims.

397. Twilio continues to provide tutorials, including instructional videos, sample code, customer support, demonstrations, and marketing materials that encourage and instruct its customers to infringe the '792 Patent Asserted Claims.

398. In the face of the knowledge of the '792 Patent as alleged above, Twilio continues (past March 31, 2016) to encourage its customers to use the 2FA Use Cases or 2FA Products to make, use, sell, offer to sell and import products and services that infringe the Asserted Claims of the '792 Patent with knowledge (or willful blindness) that its induced acts constitute patent infringement.

399. Twilio continues to offer and link to (and provide new webpages and links to) its tutorials, articles, and other materials that instruct customers to use the 2FA Use Cases or 2FA

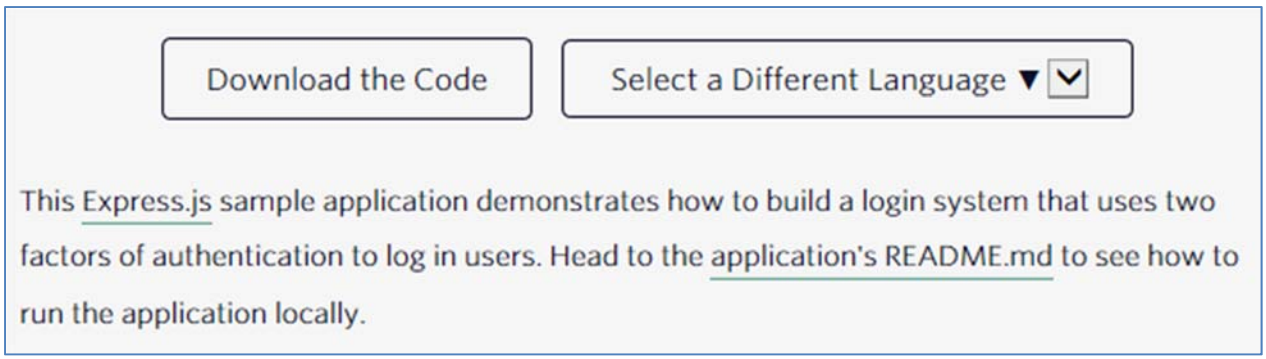
Products, to provide verification including two-factor authentication and including in connection with a notification and registering.

400. Twilio has continued maintaining and added to its instructions and encouragement to its customers to infringe TeleSign's Asserted Patent Claims with knowledge of the patent claims and its customers' infringement.

401. Twilio has provided and continues to provide tutorials instructing its customers to use 2FA Use Cases or 2FA Products.

402. For example, Twilio continues to provide its existing and new tutorials instructing its customers how to "Add[] two-factor authentication (2FA) to your web application" to increase security.

403. For example, at https://www.twilio.com/docs/authy/tutorials/two-factor-authentication-node-express, Twilio provides tutorials to "demonstrate[] how to build a login system that uses two factors of authentication" as shown below.



404. Twilio has provided and continues to provide articles, customer support, and documents including API documentation that encourages its customers to use Lookup Products and 2FA Products.

405. Twilio's customers follow such tutorials to make, use, sale, and offer infringing applications and services, which will likely have evidentiary support after a reasonable opportunity for further investigation or discovery.

406. With knowledge of the '792 Patent and its claims, Twilio has not removed or taken down its instructional materials including tutorials and marketing encouragements, thereby knowing

that the customer acts Twilio is inducing constitute patent infringement.

407. With knowledge of the '792 Patent and its claims, Twilio continues to provide instructions and has provided additional instructions, including articles, videos, conferences, customer support, sample code, or webpages.

408. Some articles and tutorials are targeted and interlink with each other and direct uses by cross-references (including via marketing materials that describe the functionality of the 2FA Use Cases or 2FA Products and how they can and should be combined with registering). Twilio continues to offer and link to its tutorials, articles, and other materials that instruct customers to perform verification processes as claimed in the '792 Patent, and register users—all with knowledge (or willful blindness) that these induced acts constitute patent infringement.

409. Twilio's customers use the 2FA Use Cases or 2FA Products or they contract with Twilio for use of Twilio's services that perform steps claimed by the '792 Patent.

410. Twilio advertises and instructs its customers to use the 2FA Use Cases or 2FA Products as claimed by the '792 Patent.

411. Twilio continues to offer and instruct its customers to use 2FA Use Cases or 2FA Products, despite knowledge of the '792 Patent Asserted Claims and knowledge that its customers' acts constitute direct infringement of the '792 Patent.

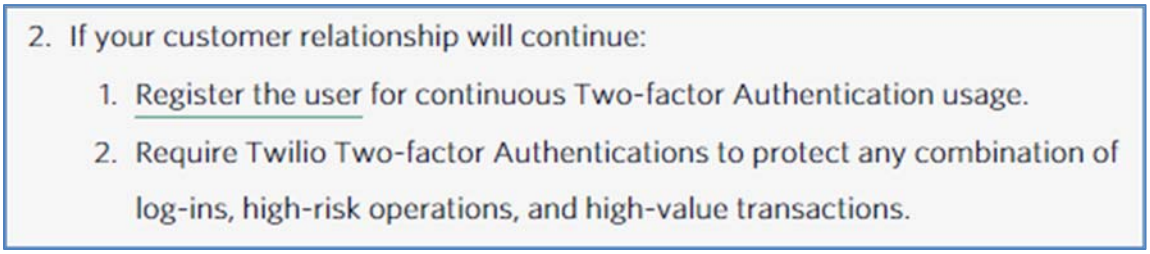
412. By way of another example, Twilio instructs its customers to use two-factor authentication for sign ups and sending codes: "Two-factor authentication with voice and SMS notifications Here's how it works, as a user: 1.You sign up for an online service, and enter your cell (or home) phone number during the sign up process. 2.Later, the first time you sign in on a new device or browser, the service either sends you a text message with a verification code or calls you and reads the code back to you. 3.You enter the verification code on the login page and you are granted access." https://www.twilio.com/blog/2011/11/twilio-two-factor-authentication.html

413. For example Twilio encourages 2FA and verification including "event notification capabilities" as shown at https://www.twilio.com/blog/tag/two-factor-authentication.[21]

[21] Exhibit DD.

414. Twilio encourages and knows that its customers use the 2FA Use Cases or 2FA Products in connection with registering.

415. Twilio instructs its customers and states, for example, that its "currently suggested signup and usage flow" found at https://www.twilio.com/docs/verify/developer-best-practices[22] includes "register[ing] the user for continuous Two-factor Authentication usage."



416. Twilio encourages its customers to use two-factor authentication including by implementing Authy.

417. By way of example, the screen capture below from https://www.twilio.com/docs/authy[23] shows that Twilio instructs customers to use two-factor authentication via Authy, including to "[s]ecure your users' accounts with high-security checks during logins and step-up transactions to ensure you're letting the right person in."

[22] Exhibit M.
[23] Exhibit K.

> Authy is the fastest way to add two-factor authentication or passwordless login to your app. Secure your users' accounts with high-security checks during logins and step-up transactions to ensure you're letting the right person in. Easy support for SMS, Voice, OTP, and Push Authentication channels. Let's get building.

418. Twilio encourages developers to use Verify with respect to sending codes or messages.

419. As to Verify, Twilio's 2017 10-K states (emphasis added): "Verify. Allows developers to deliver a one-time passcode through SMS or voice to verify that a user is in possession of the device being **registered**." (Twilio 2017 Annual Report, p. 12)

420. Twilio's 10-K states that its customer "uses our Programmable Voice products and Programmable Messaging products in its applications to verify new and existing users on its service." (Twilio 2017 Annual Report, p. 28)

421. By way of further example only, Twilio instructs its customers to use the 2FA Use Cases or 2FA Products, as described at https://www.twilio.com/docs/howto/two-factor-authentication,[24] which states "[w]ith Twilio you can set up your two-factor authentication system to run on a devices [sic] all of your employees already carry with them."

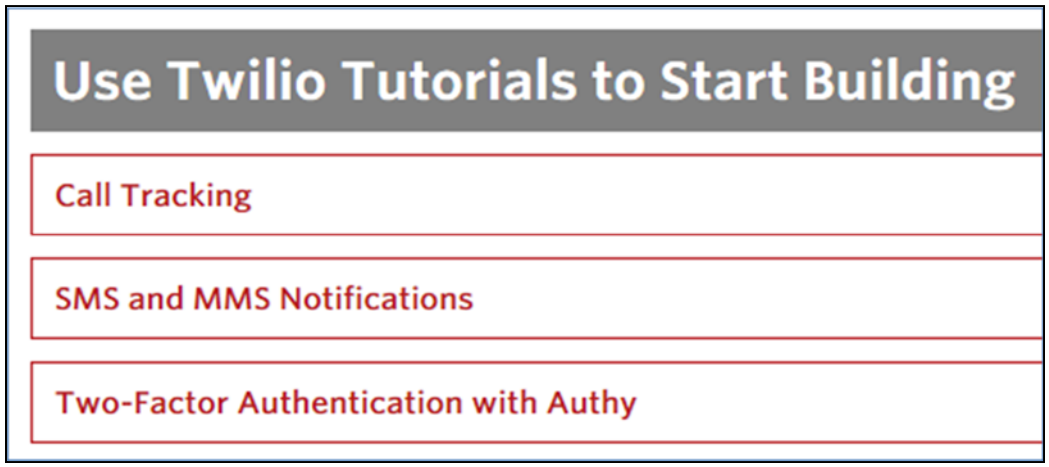
422. Twilio instructs its customers to use two-factor authentication in connection with registering.

423. By way of example, the screen capture below from https://www.twilio.com/press/releases/release-twilio-proxy shows that Twilio instructs customers to use its Engagement Cloud and "the Twilio Two-factor Authentication service for stronger account security."

[24] Exhibit BB.

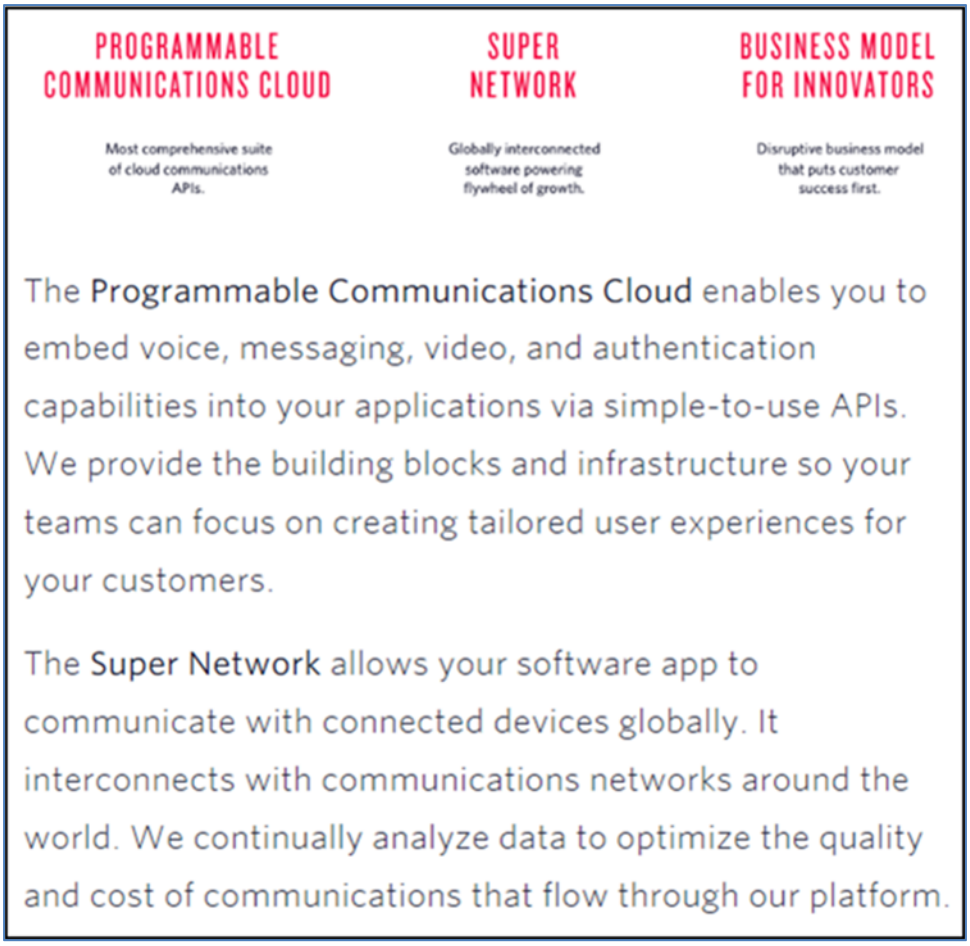
424. Twilio encourages and knows that its customers use 2FA Use Cases or 2FA Products, as shown at https://www.twilio.com/blog/2014/02/send-safely-uses-twilio-two-factor-authentication-nt.html.

425. On the same webpage, Twilio instruct its customers to "Start Building," including by using Twilio's Tutorial for "Two-Factor Authentication with Authy."



426. Twilio encourages its customers to use two-factor authentication including by implementing Authy.

427. By way of further example, the screen capture below from https://www.twilio.com/learn/twilio-101/why-businesses-need-programmable-communications shows that Twilio instructs customers to use its Programmable Communications Cloud and Super Network, including to "embed…authentication capabilities" and "communicate with connected devices globally."



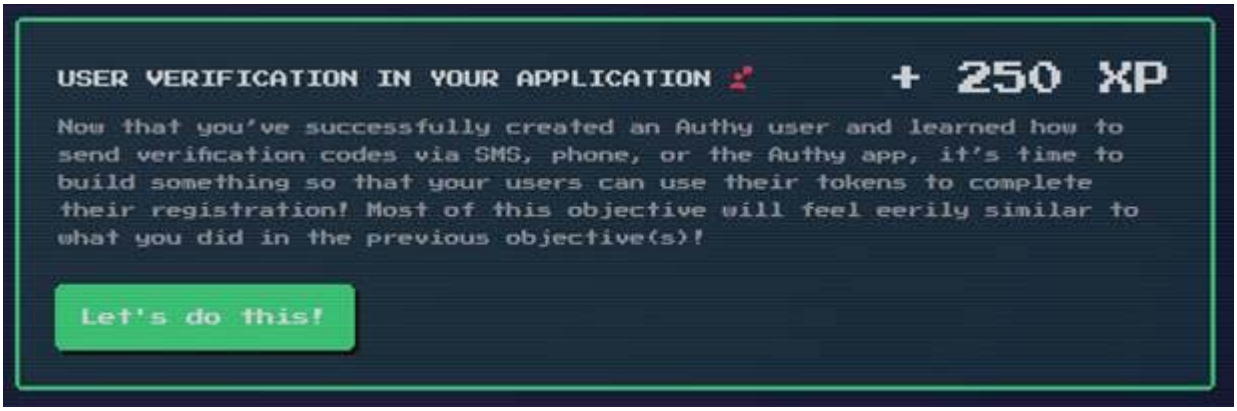
428. Twilio's 2017 10-K describes its "Programmable Communications Cloud" as follows: "Our Programmable Communications Cloud consists of software for voice, messaging, video and authentication that empowers developers to build applications that can communicate with connected devices globally. We do not aim to provide complete business solutions, rather our Programmable Communications Cloud offers flexible building blocks that enable our customers to build what they need." (Twilio 2017 Annual Report, p. 12)

429. Regarding Twilio's Engagement Cloud, Twilio's 2017 10-K states: "While developers can build a broad range of applications on our platform, certain use cases are more common. Our Engagement Cloud APIs build upon our Programmable Communications Cloud to offer more fully implemented functionality for a specific purpose, such as two-factor authentication or skills-based routing in a contact center, thereby saving developers significant time in building their applications."

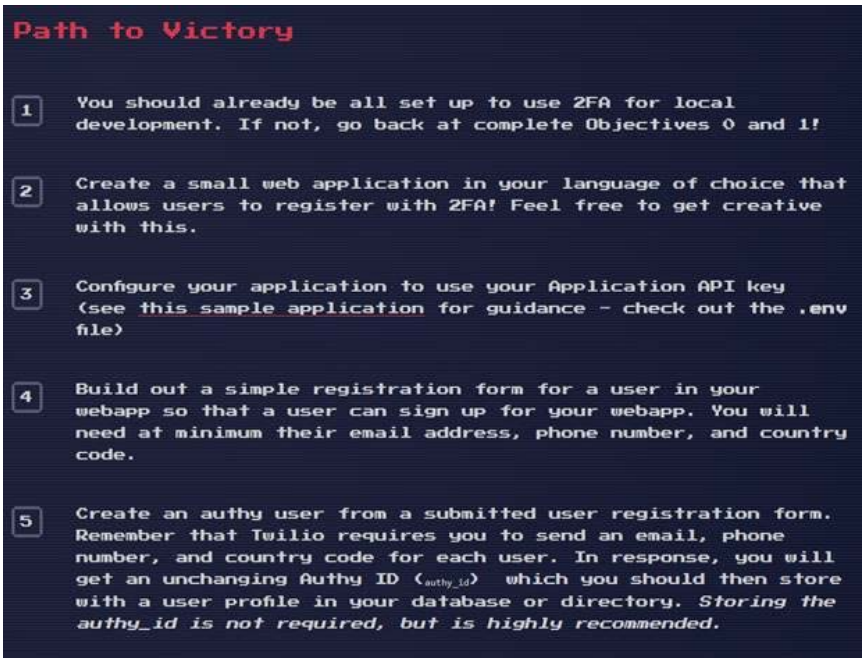
430. By way of further example, Twilio has provided an "interactive, self-paced game" for its customers to "learn how to Twilio," to help its customers "master Voice, SMS, Video or our other products" entitled "Twilio Quest," as shown at https://www.twilio.com/quest/welcome, with knowledge of the asserted patent claims.

431. "Twilio Quest" instructs Twilio customers to implement 2FA during registration of their end users.

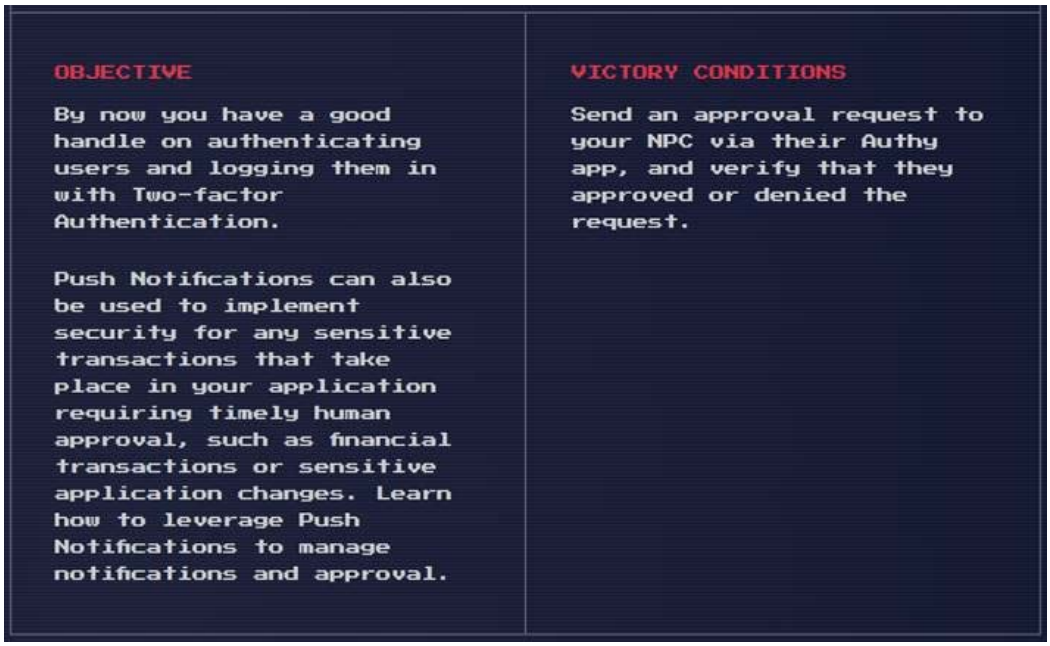
432. For example, as shown at https://www.twilio.com/quest/mission/4, Twilio instructs its customers to use its verification to "complete [users'] registration!"



433. Also for example, as shown at https://www.twilio.com/quest/mission/4/objective/38, Twilio tells its customers to "Build out a simple registration form" and "[c]reate an authy user."



434. By way of further example, Twilio uses Twilio Quest to instruct its customers to notify end users of sensitive transactions (after they have been authenticated and logged in as a user with 2FA), as shown at https://www.twilio.com/quest/mission/4/objective/49.



435. Twilio instructs and encourages its customers to infringe the '792 Patent using the accused products above, which store user-specific information and/or notification events.

436. Twilio actively induces customers to directly infringe the '792 Patent, and Twilio's customers directly infringe by making, using, selling, offering to sell, or importing directly infringing products.

437. When Twilio's customers perform the claimed steps of the '792 Patent as instructed by Twilio, Twilio's customers directly infringe the '792 Patent.

438. When Twilio performs one or more steps of the Asserted Claims of the '792 Patent as contracted by Twilio's customers, such as establishing a short message service (SMS) connection with the user using the received telephone number; and communicating a verification code to the user through the SMS connection; receiving, via the computing interface, a submitted verification code that is entered by the user, the performance of the one or more step(s) are attributable to Twilio's customers as described above in Section VIII regarding Twilio's actions attributable to its customers. When Twilio performs the steps of verifying the telephone number if the submitted

verification code is the same as the communicated verification code, or completing a registration of the user, the performance of the one or more steps are attributable to Twilio's customers as described above in Section VIII.

439. TeleSign has been damaged by Twilio's inducement of infringement of the '920 and '038 Patents and will suffer additional irreparable damage unless Twilio is enjoined from continuing to induce infringement the '792 Patent.

XVII. Twilio's Requests for Post-Grant Proceedings.

440. On December 16, 2015, Twilio requested IPR of claims 1-4, 6, 7, 9, and 11-14 of the '034 Patent. *See* IPR2016-00360. The Patent Office instituted IPR proceedings on these claims on June 28, 2016, and conducted an oral hearing on March 27, 2017.

441. The Patent Office determined that Twilio failed to show that claims 1-4, 6, 7, 9, and 11-14 of the '034 Patent are unpatentable on June 26, 2017.

442. Twilio did not appeal the Patent Office's Final Written Decision in IPR2016-00360.

443. On January 11, 2016, Twilio requested IPR of claims 1-22 of the '038 Patent (IRP2016-00451) and claims 1-10, 13, and 17-22 of the '920 Patent.

444. On July 8, 2016, the Patent Office denied Twilio's requests for IPR of claims of the '038 and '920 Patents.

445. Twilio filed requests for rehearing of the Patent Office's denials of Twilio's requests for IPR of the '038 and '920 Patents on July 29, 2016.

446. On September 29, 2016, the Patent Office denied both of Twilio's requests for rehearing.

447. Twilio did not challenge the asserted claims of the '792 patent in an IPR (claims 9 and 18), which are presumed valid and enforceable.

448. On August 25, 2016, Twilio requested a "covered business method" (CBM) review of claims of the '792 Patent. *See* CBM2016-00099.

449. The Patent Office denied institution of CBM review of the '792 Patent claims on

February 27, 2017.

450. The Patent Office stated in its decision denying CBM review (p. 10) that: "Claims 1 and 10 recite a 'computing interface presented to the user as a result of an attempt by the user to access a service,' completing a registration that 'enables the user to access the service,' 'maintaining a record of one or more notification events associated with actions that require acknowledgement by the user,' transmitting a message 'indicating the occurrence of the notification event,' and receiving an 'acknowledgement of an action associated with the established notification event' from the user."

451. The Patent Office also stated in its decision denying CBM review (pp. 7, 11-12) that: "A 'covered business method patent' is 'a patent that claims a method or corresponding apparatus for performing data processing or other operations used in the practice, administration, or management of a financial product or service, except that the term does not include patents for technological inventions.' . . . In fact, the Specification indicates just the opposite. *See id*. at col. 2, ll. 12–16 ('There are also instances which are not financially based in which notification could benefit both the consumer as well as the business.'), col. 11, ll. 10–42 ('The alert/notification aspect of the present invention can be implemented in a wide variety of scenarios. . . . The present invention is not limited to notifying a user of events that occur with respect to a financial account. Instead, alerts or notifications can be given to the user for any reason.'). The Specification provides multiple examples of services and notification events outside the financial context, such as providing access to information on a secure website and notifying the user of sports scores, airline flight changes, etc."

452. The Patent Office also stated in its decision denying CBM review (p. 13) that: "Further, we do not agree with Petitioner that the 'primary purpose' of the '792 patent relates to finance. *See* Reply 3. The '792 patent describes a need in the art for a more secure way to 'verify[ ] a registrant's identity' during online registration and notify the registrant of designated events because individuals 'often register with untraceable or false e-mail addresses and phone numbers,' which 'can compromise the intended purpose of the registration, create a breach of security and constitute fraud on the web-site owners.'"

XVIII. Willful Infringement

453. All of the preceding paragraphs are incorporated by reference herein.

454. Twilio's infringement of the Asserted Patents is willful.

455. Twilio had knowledge of the Asserted Patents (including actual knowledge).

456. Twilio acted despite an objectively high likelihood that its actions constituted infringement of a valid patent, the Asserted Patents, and the objectively-defined risk was either known to Twilio or so obvious that it should have been known to Twilio.

457. Despite service of the original and First Amended Complaint in *TeleSign I*, and service of the original Complaint in *TeleSign II* and the allegations in this First Amended Complaint in *TeleSign II*, Twilio continues to directly infringe the Asserted Claims.

458. As stated above, TeleSign sought a preliminary injunction in *TeleSign I* due to harm caused by Twilio's infringement of U.S. Patent No. 7,945,034. *See* ECF No. 23.

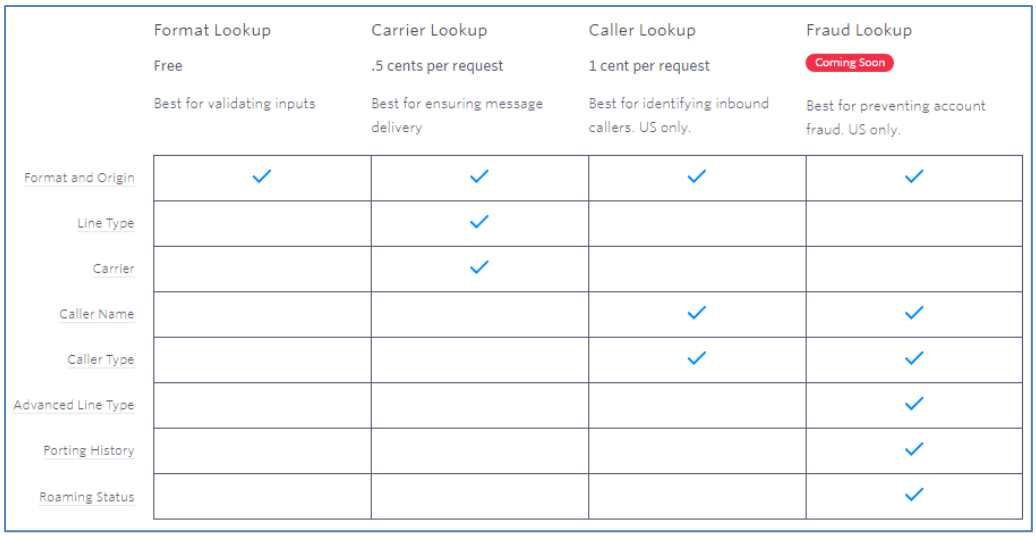
459. Twilio has acted willfully because it continues to make, use, sell, offer for sale, or import the Accused Products despite knowledge of the Asserted Claims.

460. Despite service of the original and First Amended Complaint in *TeleSign I*, and service of the original Complaint in *TeleSign II* and the allegations in this First Amended Complaint in *TeleSign II*, Twilio continues to convey or make available information regarding the accused products including instructions and encouragement to customers to use characteristics of phone numbers and to verify contacts using a code including as described herein.

461. For example, Twilio continues to instruct and encourage its customers to make, use, sell, offer for sale, or import the Accused Products including technologies built with or incorporating the Accused Products despite knowledge of the Asserted Claims.

462. As another example, Twilio was aware that its *inter partes* review proceedings and attempted covered business method patent proceedings against TeleSign's asserted patents did not result in all claims being found unpatentable by the Patent Office, despite Twilio raising alleged prior art references to challenge claims of the asserted patents. For example Twilio's requests to institute *inter partes* review of TeleSign's '922 and '038 patents were denied. And in the face of the

knowledge of the '034 Patent as alleged above, Twilio has continued (at least past April 30, 2015) to encourage its customers to use its Lookup Products and 2FA Products even after the '034 patent survived Twilio's best invalidity challenge via *inter partes* review, with the Patent Office determining that no claim of the '034 patent is invalid. Twilio has even increased the outward marketing and use case of "Lookup" directed specifically to expanded uses of preventing fraud by attributing a dedicated title ("Fraud Lookup") to an aspect of its Lookup Products.



	Format Lookup Free Best for validating inputs	Carrier Lookup .5 cents per request Best for ensuring message delivery	Caller Lookup 1 cent per request Best for identifying inbound callers. US only.	Fraud Lookup Coming Soon Best for preventing account fraud. US only.
Format and Origin	✓	✓	✓	✓
Line Type		✓		
Carrier		✓		
Caller Name			✓	✓
Caller Type			✓	✓
Advanced Line Type				✓
Porting History				✓
Roaming Status				✓

(Excerpt from https://www.twilio.com/lookup)

463. As another example, Twilio was aware that its motion for judgment on the pleadings was denied in *TeleSign I*, regarding the alleged invalidity of three of the Asserted Patents, which are in the same patent family as the '792 Patent. *See TeleSign I*, ECF No. 123.

464. Twilio has contended that the subject matter of the '792 patent is similar to that of related the '920 and '038 patents.

465. The '792 Patent issued despite the Patent Office's consideration of additional prior art and Twilio's Section 101 patent-ineligibility motion—further indicating that the '792 Patent was duly issued and will remain valid.

466. As another example, as explained above regarding Twilio's knowledge, Twilio was aware of TeleSign's '792 pending patent application, its published claims, and the Notice of Allowance indicating those claims would issue as the '792 Patent, as alleged above and was aware

of TeleSign's patent family and TeleSign's allegations regarding Twilio's two-factor authentication technology in *TeleSign I*—but did not avoid or discontinue its infringement of the '792 Patent.

467. Twilio knew of the objectively high risk of infringement of TeleSign's Asserted Patents including the '792 Patent given Twilio's analysis in *TeleSign I*.

468. Twilio continued its infringement of the Asserted Patents despite the denial of its motion for judgment on the pleadings (a patent-ineligibly assertion).

XIX. PRAYER FOR RELIEF

469. TeleSign demands trial by jury for all issues so triable by a jury.

WHEREFORE, TeleSign respectfully requests this Court to:

A. Enter judgment for TeleSign that Twilio has infringed and is infringing one or more claims of the Asserted Patents;

B. Enter judgment for TeleSign that Twilio has actively induced infringement and is actively inducing infringement of one or more claims of the Asserted Patents;

C. Enter judgment for TeleSign that Twilio has willfully infringed and is willfully infringing one or more claims the Asserted Patents;

D. Issue a permanent injunction enjoining Twilio (including its officers, directors, employees, agents, customers and all persons acting in concert with them) from infringing the Asserted Patents;

E. Order that Twilio pay compensatory damages to TeleSign for Twilio's infringement of the Asserted Patents, including but not limited to, damages for lost profits and in no event less than a reasonable royalty;

F. Award damages based TeleSign's provisional rights under 35 U.S.C. § 154(d);

G. Find this to be an exceptional case, award TeleSign treble damages due to Twilio's deliberate and willful conduct, and order Twilio to pay TeleSign's costs of suit and attorneys' fees;

H. Award TeleSign interest and costs under 35 U.S.C. § 284;

I. Award TeleSign pre-judgment interest; and

J. Order such other relief as the Court considers appropriate.

Dated: __July 13, 2018

Signed: _/s/ Mary Jane Peal_____

SHOOK, HARDY & BACON L.L.P.
Gary Miller (Appearance *Pro Hac Vice*)
gmiller@shb.com
111 S. Wacker Drive, 51st Floor
Chicago, Illinois 60606
Telephone: 312-704-7700
Facsimile: 312-558-1195

Jesse J. Camacho (Appearance *Pro Hac Vice*)
jcamacho@shb.com
Ryan Dykal (Appearance *Pro Hac Vice*)
rdykal@shb.com
Mary J. Peal (Appearance *Pro Hac Vice*)
mpeal@shb.com
2555 Grand Boulevard
Kansas City, Missouri 64108
Telephone: 816-474-6550
Facsimile: 816-421-5547

Janet L. Hickson (SBN: 198849)
jhickson@shb.com
Mayela C. Montenegro (SBN: 304471)
mmontenegro@shb.com
5 Park Plaza, Suite 1600
Irvine, California 92614
Telephone: 949-475-1500
Facsimile: 949-475-0016

Attorneys for Plaintiff
TELESIGN CORPORATION