UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

TWILIO, INC.,

Plaintiff,

v.

TELESIGN CORPORATION,

Defendant.

Case No. 16-CV-06925-LHK

ORDER GRANTING IN PART AND DENYING IN PART DEFENDANT'S MOTION TO DISMISS

Re: Dkt. No. 31

Plaintiff Twiilio, Inc. ("Twilio" or "Plaintiff") filed a patent infringement suit against Defendant Telesign Corporation ("Telesign" or "Defendant") and alleged that Defendant infringed the claims of U.S. Patent Nos. 8,306,021 ("the '021 Patent"), 8,837,465 ("the '465 Patent"), 8,755,376 ("the '376 Patent"), 8,738,051 ("the '051 Patent"), 8,737,962 ("the '962 Patent"), 9,270,833 ("the '833 Patent"), and 9,226,217 ("the '217 Patent") (collectively, the "Asserted Patents"). Before the Court is Defendant's Motion to Dismiss, which seeks to dismiss all seven Asserted Patents. ECF No. 31 ("Mot."). Due to the breadth of Defendant's Motion to Dismiss, the Court will issue its decision in two orders. This order covers the '962, '833, '021, '465, and '376 patents. Having considered the submissions of the parties, the relevant law, and the record in this case, the Court GRANTS IN PART and DENIES IN PART Defendant's Motion to Dismiss

with respect to these patents.

I. BACKGROUND

A. Factual Background

1. The Parties

Plaintiff Twilio is a Delaware corporation with its primary place of business in San Francisco, California. ECF No. 1 ("Compl.") ¶ 1. Plaintiff's co-founder, Jeffrey Lawson, is a co-inventor on three of the Asserted Patents. ECF No. 45 at 1. Defendant Telesign is a California corporation with its principal place of business in Marina Del Rey, California. Compl. ¶ 15.

2. The Twilio Patents

Plaintiff's complaint and the parties' briefing divides the asserted patents into four families: (1) the '962 and '833 patents (the "Score Patents"), (2) the '051 patent (the "Delivery Receipts Patent"), (3) the '021, '465, and '376 patents (the "Platform Patents"), and (4) the '217 patent (the "Path Selection Patent"). As mentioned above, this order covers the '962, '833, '021, '465, and '376 patents, which are the patents from the Score Patents and Platform Patents families. An overview of the two patent families follows.

a. The Score Patents

i. Specification

The '962 patent is titled "Method and System for Preventing Illicit Use of a Telephony Platform." Compl, Ex. E ('962 patent). It was filed on July 24, 2013 and issued on May 27, 2014. It claims priority to a provisional application, which was filed on July 24, 2012.

The '833 patent is also titled "Method and System for Preventing Illicit Use of a Telephony Platform." Compl., Ex. F ('833 patent). It was filed on April 15, 2014 as a divisional application of the '962 patent. It issued on February 23, 2016. Its specification is identical to the '962 patent, and it also claims priority to the same July 24, 2012 provisional application.

The Score Patents generally relate to "preventing illicit use of a telephony platform." '962 patent at col. 1:15. As the Background section of the specification explains, "[t]elephone fraud has long been a problem for telephony systems." *Id*. at col. 1:20-21. However, in recent years,

"the opportunities for telephony fraud is [sic] even greater." *Id.* at col. 1:22-23. This is because "[t]he recent development of new telephony platforms . . . enable[] nefarious parties to create programs that commit telephony fraud." *Id.* at col. 1:23-26. Examples of such fraud include toll fraud, chargebacks, and "us[ing] valuable resources for improper uses that would otherwise be used for legitimate applications." *Id.* at col. 1:26-33.

The Score Patents purport to address telephony fraud through a method of "fraud scoring," which "monitor[s], measure[s], and detect[s] instances of illicit use that occur within or through the communication platform." *Id.* at col. 4:4-6. Figure 1 shows how this fraud scoring mechanism is deployed within a communication platform:

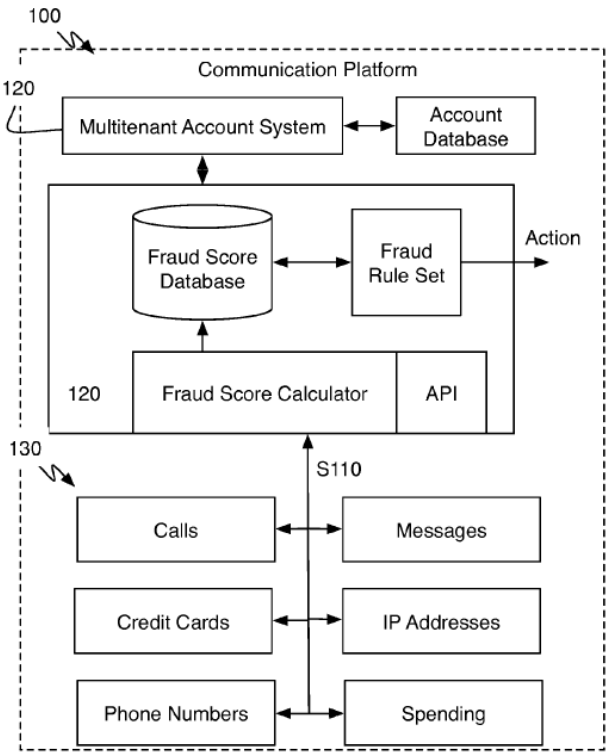

FIGURE 1

As Figure 1 illustrates, the fraud scoring method functions as a component of a communication platform. *Id.* at Fig. 1. The communication platform includes a multitenant account system, which "manage[s] and facilitate[s] the accounts within the communication platform." *Id.* at col. 3:28-29. It also includes "operational components" which include "any servers, databases, processors or other resources that either define account configuration, account usage, or other

aspects of the account within the platform." *Id*. at col. 5:33-36. The fraud scoring method utilizes the multitenant account system and the operational components of the communication platform. *Id*. at col. 2:16-35, 5:30-32, Fig. 1.

Figure 2 illustrates the operation of the fraud scoring method within the communication platform:

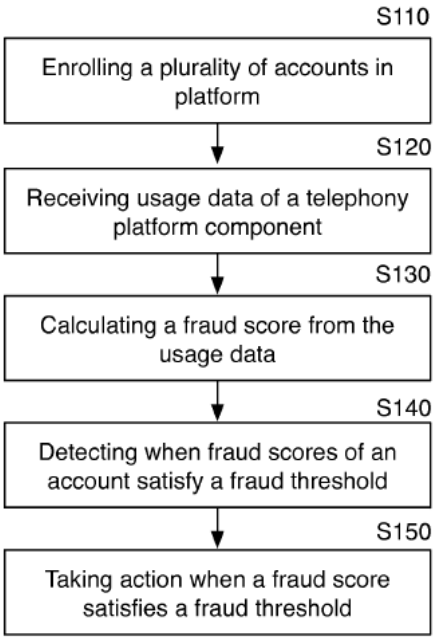

FIGURE 2

The first step, "enrolling a plurality of accounts in the platform," refers to general account set up and configuration activities. *Id*. at col. 6:50-51. This includes associating an account with phone number(s), billing information, and relevant internet resources. *Id*. at col. 7:13-50. In the system, it is possible to create sub-accounts that correspond to a single, base account. *Id*. at col. 3:54-58. "For example, an application developer may create a customer service application, and then allow end users to signup as customers within his account." *Id*. at col. 3:60-63. The customers' accounts would then be sub-accounts of the customer service application's account. *See id.* This allows both the customer and the customer service application to modify the customer accounts. *Id*. at col. 3:63-66.

The remaining steps describe the core fraud detection functionality. First, at step S120, the

fraud score method "receive[s] usage data of a telephony platform component." *Id*. at col. 7:51-52, Fig. 2. This step "functions to collect data used to calculate a fraud score." *Id*. at col. 7:53. Usage data can be pulled from "a variety of data sources," including "call history databases, messaging history databases, account databases, credit card hash databases, account databases, client device information databases, IP address databases, phone number databases, credit card or spending databases, API logs, and/or any suitable machine containing data useful for calculating a fraud score." *Id*. at col. 4:38, 8:3-9. For example, usage data stored in a call history database can include "call duration, account(s) associated with a call, call destination endpoints, caller endpoints, carrier origin of a call, destination carrier, frequency of calls, number of concurrent calls for an account, or any suitable parameter of call data." *Id*. at col. 10:6-8.

Next, at step S130, the fraud score method "calculat[es] a fraud score from the usage data." *Id*. at col. 8:55-56, Fig 2. This "functions to process usage data to generate metric that reflects the likelihood that illicit use of the telephony platform is occurring." *Id*. at col. 8:56-58. To calculate a fraud score, the method uses a set of fraud rules. *Id*. at col. 8:58-59. Fraud rules can either be conditions within a single account, or patterns across multiple accounts. *Id*. at col. 8:64-66. When a fraud rule is triggered, the corresponding account(s) are assigned a fraud score, which is generally a "numeric value" but may be a "label or any suitable construct to communicate fraud likelihood." *Id*. at col. 9:16-18, 23-25. A single account may have multiple fraud rules (and, as a result, multiple fraud scores) associated with it, which reflect different fraud detection heuristics. *Id*. at col. 9:30-36.

Next, at step S140, the method "detect[s] when fraud scores of an account satisfy a fraud threshold." *Id*. at col. 11:64-65, Fig. 2. This "function[s] to monitor and assess when a scenario of illicit behavior is occurring based on the fraud scores." *Id*. at col. 11:65-67. In one example, this is achieved by summing all the fraud scores across an account, and detecting when the sum is higher than a numeric threshold. *Id*. at col. 12:12-16.

Finally, at step S150, the method "tak[es] action when a fraud score satisfies a fraud threshold." *Id*. at col. 12:27-28. This "functions to react to fraud scores that indicate illicit

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.