

EXHIBIT 6

**Analysis of Infringement of U.S. Patent No. 8,291,010 by TD Ameritrade, Inc.
(Based on Public Information Only)**

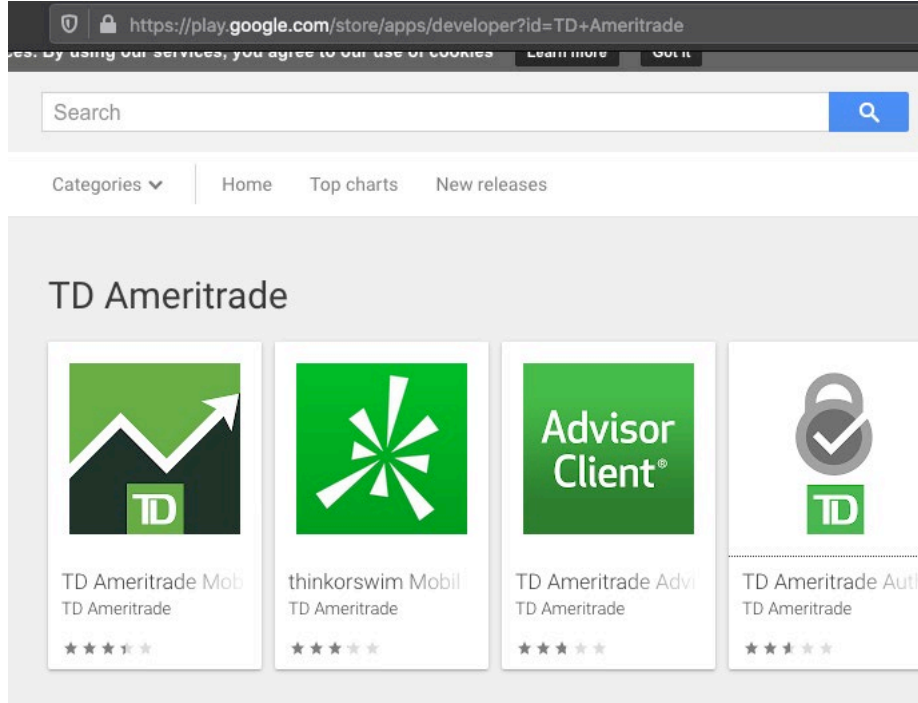
Communication Interface Technologies, LLC (“CIT”) provides this preliminary and exemplary infringement analysis regarding the alleged infringement of U.S. Patent No. 8,291,010, entitled “*Virtual Connection of a Remote Unit To A Server*” (“the ‘010 patent” or “TD Ameritrade”). The following chart illustrates an exemplary analysis regarding infringement by TD Ameritrade’s mobile application(s) including the TD Ameritrade Mobile App, thinkorswim Mobile: Trade. Invest. Buy & Sell App, TD Ameritrade Authenticator, along with any hardware and/or software for provisioning that mobile device application (“Accused Instrumentalities”). Upon information and belief, the exemplary version herein and previous versions of the Accused Instrumentalities operated materially in the same manner prior to expiration of the patents-in-suit.

The analysis set forth below is based only upon information from publically available resources regarding the Accused Instrumentalities. TD Ameritrade has not yet provided any non-public information.

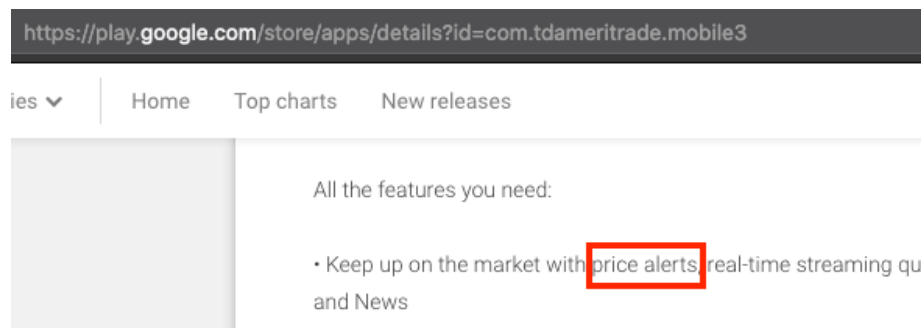
Unless otherwise noted, CIT contends that TD Ameritrade directly infringes the ‘010 patent in violation of 35 U.S.C. § 102(b) by offering to sell, making, using, and/or importing the Accused Instrumentalities. The following exemplary analysis demonstrates infringement.

Unless otherwise noted, CIT believes and contends that each element of each claim asserted herein is literally met by the provision of the Accused Instrumentalities. However, to the extent that TD Ameritrade attempts to allege that any element is not literally met, CIT believes and contends that such elements are met under the doctrine of equivalents. More specifically, in the analysis of the Accused Instrumentalities, CIT did not identify any substantial differences between the elements of the claims and the corresponding features of the Accused Instrumentalities, as set forth herein. In each instance, the identified feature of the Accused Instrumentalities performs at least substantially the same function in substantially the same way to achieve substantially the same result as the corresponding element.

CIT notes that the present claim chart and analysis are necessarily preliminary in that CIT has not obtained substantial evidence. TD Ameritrade nor has TD Ameritrade disclosed any detailed analysis for its non-infringement position, if any. Further, CIT reserves the right to supplement and/or amend the positions taken in this preliminary infringement analysis, including with respect to literal infringement and infringement under the doctrine of equivalents, further information obtained by CIT, including but not limited to information adduced through information exchanges, expert discovery, claim construction, expert discovery, and/or further analysis.

	Claim 1	TD Ameritrade Downloadable App Service
1	A method comprising:	<p>A method is specified for use on a user device like a handheld or tablet.</p> <p>See https://play.google.com/store/apps/developer?id=TD+Ameritrade</p> 
1a	establishing, at a computing device, a communication session supporting communication between a first program executing at an application layer of the computing device and a remote server;	<p>Wireless push notification messages are sent over Transport Layer Security (TLS) sessions. The push message includes an encrypted push token as per Endnote #1. The push notification message is sent over TLS sessions from the TD Ameritrade server to the TD Ameritrade App (application program, application layer of the user's smartphone (mobile handset) or tablet).</p> <p>In the TD Ameritrade application, for example, a push notification contains information about TD Ameritrade accounts, investments and banking.</p>

See <https://play.google.com/store/apps/details?id=com.tdameritrade.mobile3>



Also, the Server Application and the client-side App establish a separate TLS session for each communication, in addition to the traditional client-server communications. For example, the TD Ameritrade mobile program establishes a TLS session with the TD Ameritrade App.

The TLS session used for client-server communications between the TD Ameritrade Server and the TD Ameritrade App correspond to the recited communication.

TLS sessions use a full handshake sequence that is used to establish communication. An abbreviated handshake sequence that is used to resume the TLS session from a dormant state to an active state whereby new payload data can be sent via the connection again.

See Endnote #2 for a discussion of the virtual session aspects of TLS.

Mobile applications communicate with their application server via TLS. TLS connections are established at the time the app is installed or launched. Subsequent connections are made at a later time using a session token. See Endnote#2 for a discussion of TLS.

See https://threema.ch/press-files/cryptography_whitepaper.pdf - Android TLS sessions.

See <https://www.icir.org/johanna/papers/conext17android.pdf> - Android secure connections between client app and server are ubiquitously used.

		<p>See https://developer.android.com/training/articles/security-ssl. – “The (SSL)—now technically known as Transport Layer Security (TLS)—is used for encrypted communications between clients and servers.” Note that certificates and keys are used to help create Android Device Tokens used in Push Notifications. See Endnotes #1, and #2.</p>
1b (i)	subsequent to deactivation of the established communication session,	<p>See Endnote #2. Note when the application data phase is finished, the session is placed back into the inactive state. Hence the end of application data phase is used to place the session into the inactive state.</p>
1b (ii)	the computing device receiving an incoming communication from the remote server, wherein the incoming communication is not in response to a request sent by the computing device;	<p>As per Endnote #1, the remote server causes a push notification message to be sent to the computing device. Part of this push notification message (incoming communication) is forwarded to the TD Ameritrade App running on the user’s smartphone or tablet. The push notification message is asynchronously initiated by the remote server (Server) as opposed to being sent in response to a request sent by the user.</p>
1c	at the application layer, the computing device reading a set of information included in the incoming communication;	<p>An app-specific device token included in the incoming communication is used by the TD Ameritrade App on the device to activate or to send the new incoming information to the user.</p> <p>See Endnote #1 for a discussion of how each Push Notification message sent to the TD Ameritrade App includes an app-specific device token. The app-specific device token is used by the TD Ameritrade App running on the user’s smartphone or tablet.</p> <p>When the push notification has been received by the TD Ameritrade App, the app provides user interface capabilities that allow the user to click application data included in the push message payload. When the user clicks this information, the app evaluates this information and causes the TD Ameritrade App to launch.</p>
1d	in response to determining that the set of information read at the application layer includes information identifying the first program executing at the	<p>The remote server sends a push notification message to the TD Ameritrade App on the smartphone or tablet operated by a specified user. As per Endnote #1, the push notification message is processed by the operating system and the app-specific device token included in the message (incoming communication) is forwarded from the OS to the</p>

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.