

Secure Authentication Technologies LLC v. Plaid Inc.

The Honorable Judge Dale A. Kimball
Case No. 2:25-cv-00514-DAK-JCB

Defendant's Motion to Dismiss Under
Federal Rule of Civil Procedure 12(b)(6)

'090 Patent



The '090 Patent

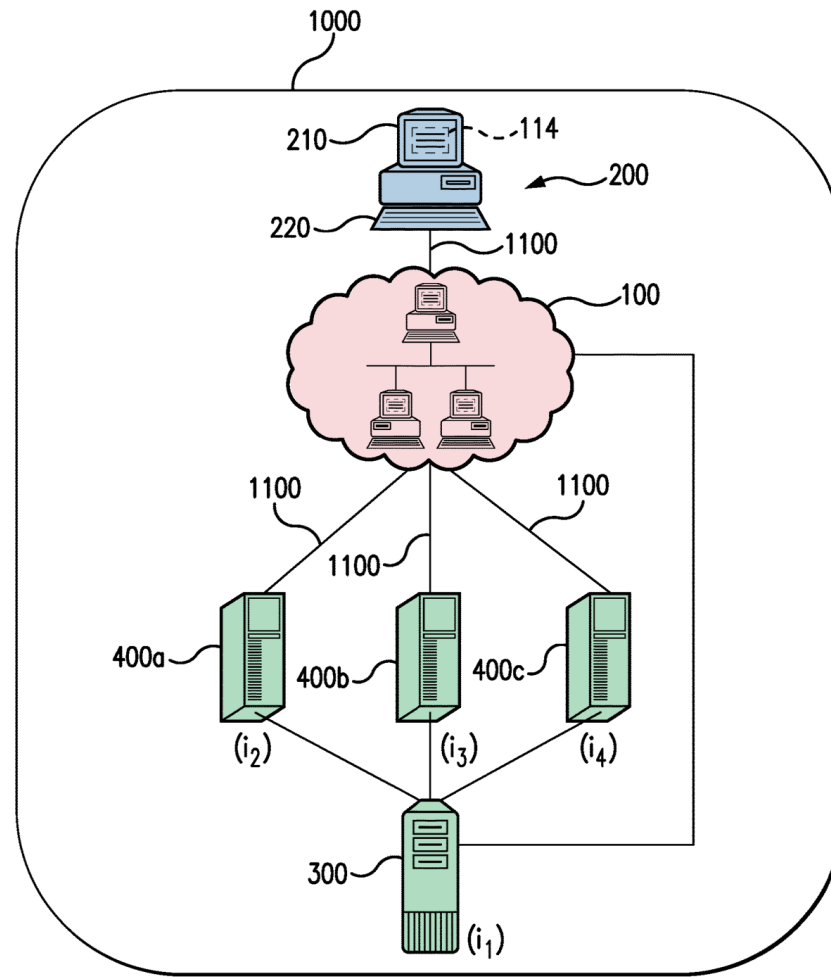


FIG. 1

Claim 1 of the '090 Patent

1. A method for permitting a third-party entity to gain access, in a secure manner, to an online account held by an account holder that is secured by a multi-factor authentication protocol, comprising the following steps performed by the third-party entity:

collecting the account holder's credentials;

encrypting the account holder's credentials using one or more processors;

storing the account holder's encrypted credentials using one or more processors, wherein the encrypted credentials are stored in a data store;

verifying the account holder's credentials by accessing, via one or more processors, the online account using the account holder's credentials;

receiving a multi-factor authentication request from the online account, the multi-factor authentication request indicating that a response is required from the account holder before further access to the online account is granted;

prompting the account holder for a response and receiving the response thereto from the account holder; and transmitting the account holder's response to the online account to satisfy the multi-factor authentication request.

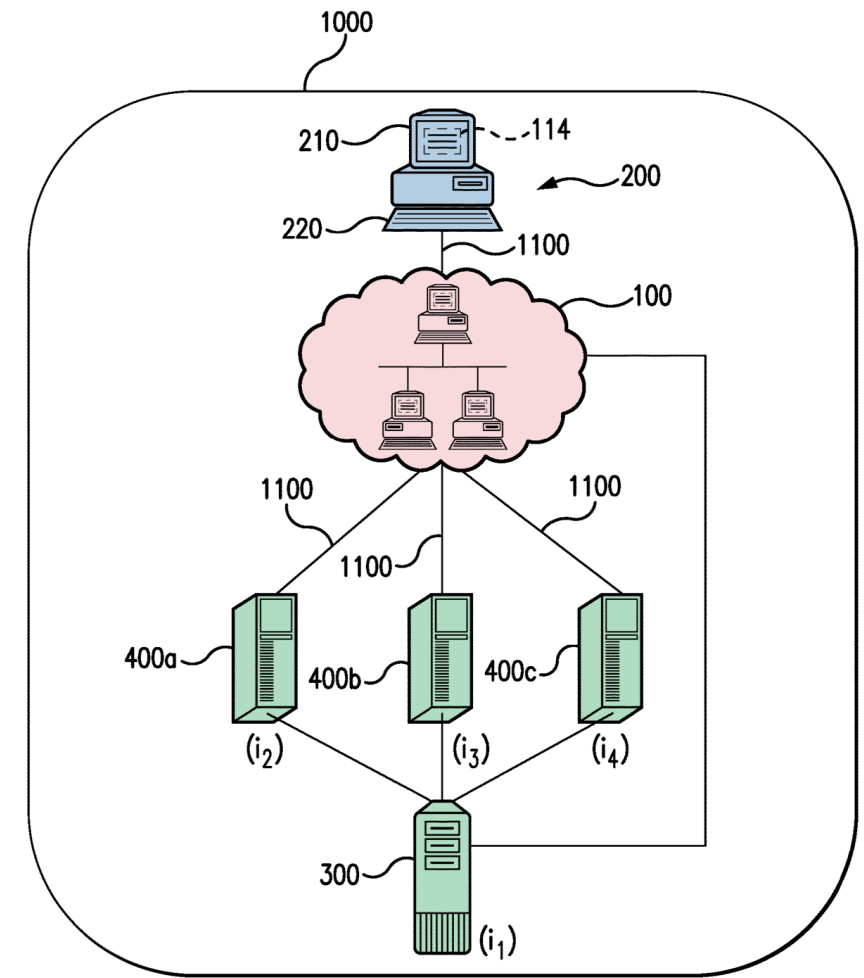


FIG. 1

35 U.S.C. § 101 – Patent-Eligible Subject Matter



“Whoever invents or discovers any **new and useful process, machine, manufacture, or composition of matter**, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.”

35 U.S.C. § 101

35 U.S.C. § 101 – Patent-Eligible Subject Matter



The Supreme Court has “long held that this provision contains an important implicit exception: Laws of nature, natural phenomena, and **abstract ideas are not patentable.**”

Alice Corp. v. CLS Bank Int’l, 573 U.S. 208, 216 (2014)

35 U.S.C. § 101 – Patent-Eligible Subject Matter



“Laws of nature, natural phenomena, and abstract ideas are the basic tools of scientific and technological work. [M]onopolization of those tools through the grant of a patent might tend to **impede innovation more than it would tend to promote it.**”

“We have repeatedly emphasized this . . . concern that patent law not inhibit further discovery by **improperly tying up the future use of these building blocks of human ingenuity.**”

Alice Corp. v. CLS Bank Int’l, 573 U.S. 208, 216 (2014)

Alice: Two-Step Test for Eligibility Under § 101

1

Step One: “We must first determine whether the claims at issue are **directed to a patent-ineligible concept.**”

2

Step Two: “We have described step two of this analysis as a search for an **inventive concept**” that is “sufficient to ensure that the patent in practice amounts to **significantly more** than a patent upon the [ineligible concept] itself.”

Dismissal Is Appropriate at the Pleadings Stage



“[W]e have repeatedly affirmed § 101 rejections at the motion to dismiss stage, before claim construction or significant discovery has commenced.”

Cleveland Clinic Found. v. True Health Diagnostics LLC, 859 F.3d 1352, 1360 (Fed. Cir. 2017)



“Eligibility under 35 U.S.C. § 101 is a question of law, based on underlying facts. Like other legal questions based on underlying facts, this question may be, and frequently has been, resolved on a Rule 12(b)(6) or (c) motion.”

SAP Am., Inc. v. InvestPic, LLC, 898 F.3d 1161, 1166 (Fed. Cir. 2018)

The Claims of the '090 Patent Are Ineligible

1

Step One: The claims are directed to the **abstract idea of using a third-party intermediary to facilitate a transaction**

2

Step Two: The claims have **no inventive concept** because the claims recite only known components functioning in their routine manner

The Claims of the '090 Patent Are Ineligible

1

Step One: The claims are directed to the **abstract idea of using a third-party intermediary to facilitate a transaction**

2

Step Two: The claims have **no inventive concept** because the claims recite only known components functioning in their routine manner

Alice Step One – What Is the Focus of the Claims?



“[W]e have described the **first-stage inquiry as looking at the ‘focus’ of the claims, their ‘character as a whole.’**”

Elec. Power Grp., LLC v. Alstom S.A., 830 F.3d 1350, 1353 (Fed. Cir. 2016)



“We have approached the Step 1 directed to inquiry by asking what the patent asserts to be the **focus of the claimed advance** over the prior art. In conducting that inquiry, we must **focus on the language of the [a]sserted [c]laims themselves**, considered in light of the specification.”

Yu v. Apple, Inc., 1 F.4th 1040, 1043 (Fed. Cir. 2021)

Claim 1 – Using a Third-Party Intermediary to Facilitate a Transaction

1. A method for permitting a third-party entity to gain access, in a secure manner, to an online account held by an account holder that is secured by a multi-factor authentication protocol, comprising the following steps performed by the third-party entity:

- collecting the account holder's credentials;
- encrypting the account holder's credentials using one or more processors;
- storing the account holder's encrypted credentials using one or more processors, wherein the encrypted credentials are stored in a data store;
- verifying the account holder's credentials by accessing, via one or more processors, the online account using the account holder's credentials;
- receiving a multi-factor authentication request from the online account, the multi-factor authentication request indicating that a response is required from the account holder before further access to the online account is granted;
- prompting the account holder for a response and receiving the response thereto from the account holder; and
- transmitting the account holder's response to the online account to satisfy the multi-factor authentication request.

Using a Third-Party Intermediary to Facilitate a Transaction Is an Abstract Idea

Alice Corp. v. CLS Bank Int'l



“Petitioner’s claims involve a method of exchanging financial obligations between two parties using a **third-party intermediary** to mitigate settlement risk. . . .

On their face, the claims before us are drawn to the concept of intermediated settlement, *i.e.*, the use of a third party to mitigate settlement risk. . . . **The use of a third-party intermediary . . . is also a building block of the modern economy.”**

Alice Corp. v. CLS Bank Int'l, 573 U.S. 208, 219–20 (2014)

Using a Third-Party Intermediary to Facilitate a Transaction Is an Abstract Idea

Universal Secure Registry LLC v. Apple Inc.



“The claims are directed to a method for enabling a transaction between a user and a merchant, where the merchant is given a time-varying code instead of the user’s secure (credit card) information. The **time-varying code . . . allows a third party or credit card company to approve or deny the transaction** based on the secure information without the provider gaining access to the secure information.”

“[A]llowing a **financial transaction between two parties using a third-party intermediary** to mitigate information security risks . . . is itself an **abstract idea**.”

Universal Secure Registry LLC v. Apple Inc., 10 F.4th 1342, 1349–50 (Fed. Cir. 2021)

Using a Third-Party Intermediary to Facilitate a Transaction Is an Abstract Idea

cxLoyalty, Inc. v. Maritz Holdings Inc.



“[C]laim 1 is directed to **‘facilitating, or brokering, a commercial transaction . . . between a purchaser using a first form of value . . . and a seller transacting in a second form of value.’**”

“**[T]he [graphical user interface] in claim 1 takes the place of the human acting as an intermediary, communicating with both the participant and the vendor . . . to complete the transaction.’** Because representative claim 1 is directed to **transfers of information relating to a longstanding commercial practice**, the claim is directed to an abstract idea.”

cxLoyalty, Inc. v. Maritz Holdings Inc., 986 F.3d 1367, 1376–77 (Fed. Cir. 2021)

Using a Third-Party Intermediary to Facilitate a Transaction Is an Abstract Idea

Internet Payments Patents Ltd. v. PayPal Inc.



“[C]laim 1 is directed to a method of exchanging and matching messages from the customer and merchant to allow the merchant to obtain payment authorization without obtaining identifying information about the customer.”

“Claim 1 describes the necessary order of steps to carry out the **abstract idea of facilitating purchases using an intermediary** by allowing the merchant to obtain payment authorization without obtaining the customer’s payment data (such as credit card number).”

Internet Payments Pats. Ltd. v. PayPal Inc., 2026 WL 212953, at *6, *12 (N.D. Cal. Jan. 27, 2026)

Non-Abstract Ideas Are More Concrete

PowerBlock Holdings, Inc. v. iFit, Inc.



“Claim 1 is limited to a **particular type of dumbbell**: a selectorized dumbbell with a stack of nested left weight plates, a stack of nested right weight plates, a handle, and a movable selector with different adjustment positions, where moving the selector to different adjustment positions changes the number of left and right weight plates coupled to the dumbbell.”

PowerBlock Holdings, Inc. v. iFit, Inc., 146 F.4th 1366, 1372 (Fed. Cir. 2025)

Non-Abstract Ideas Are More Concrete

Core Wireless Licensing S.A.R.L. v. LG Electronics, Inc.



“Claim 1 of the ’476 patent requires ‘an application summary that can be reached directly from the menu,’ **specifying a particular manner by which the summary window must be accessed.** The claim further requires the application summary window list a limited set of data, ‘each of the data in the list being selectable to launch the respective application and enable the selected data to be seen within the respective application.’ **This claim limitation restrains the type of data that can be displayed in the summary window.** Finally, the claim recites that the summary window ‘is displayed while the one or more applications are in an un-launched state,’ **a requirement that the device applications exist in a particular state.**”

Core Wireless Licensing S.A.R.L. v. LG Electronics, Inc., 880 F.3d 1356, 1362–63 (Fed. Cir. 2018)

The Claims Require No Specific Technological Improvement



“The first step in the *Alice* inquiry in this case asks **whether the focus of the claims is on the specific asserted improvement in computer capabilities** (*i.e.*, the self-referential table for a computer database) or, instead, **on a process that qualifies as an ‘abstract idea’ for which computers are invoked merely as a tool.**”

Enfish, LLC v. Microsoft Corp., 822 F.3d 1327, 1335–36 (Fed. Cir. 2016)



“Our prior cases have made clear that **mere automation of manual processes using generic computers does not constitute a patentable improvement** in computer technology.”

Credit Acceptance Corp. v. Westlake Servs., 859 F.3d 1044, 1055 (Fed. Cir. 2017)

The Claims Require No Specific Technological Improvement

1. A method for permitting a third-party entity to gain access, in a secure manner, to an online account held by an account holder that is secured by a multi-factor authentication protocol, comprising the following steps performed by the third-party entity:

- collecting the account holder's credentials;
- encrypting the account holder's credentials using one or more processors;
- storing the account holder's encrypted credentials using one or more processors, wherein the encrypted credentials are stored in a data store;
- verifying the account holder's credentials by accessing, via one or more processors, the online account using the account holder's credentials;
- receiving a multi-factor authentication request from the online account, the multi-factor authentication request indicating that a response is required from the account holder before further access to the online account is granted;
- prompting the account holder for a response and receiving the response thereto from the account holder; and
- transmitting the account holder's response to the online account to satisfy the multi-factor authentication request.

The Claims Require No Specific Technological Improvement

1. A method for permitting a third-party entity to gain access, in a secure manner, to an online account held by an account holder that is secured by a multi-factor authentication protocol, comprising the following steps performed by the third-party entity:

collecting the account holder's credentials;

encrypting the account holder's credentials using one or more processors;

storing the account holder's **encrypted credentials** using one or more processors, wherein the **encrypted credentials** are stored in a data store;

verifying the account holder's credentials by accessing, via one or more processors, the online account using the account holder's credentials;

receiving a **multi-factor authentication request** from the online account, the **multi-factor authentication request** indicating that a response is required from the account holder before further access to the online account is granted;

prompting the account holder for a response and receiving the response thereto from the account holder; and transmitting the account holder's response to the online account to satisfy the **multi-factor authentication request**.

Encryption Is An Age-Old Concept

1900 BC

Hieroglyphics
in an Ancient
Egyptian Tomb



1940

Mechanical &
Electromechanical
Encryption Machines



1975 – TODAY

Encryption Is
Ubiquitous





Encryption Is an Age-Old Concept and an Abstract Idea

Torus Ventures LLC v. Cawley Partners, LLC



“[C]laim 1 of the ’844 is directed to **the abstract idea of ‘encrypting data that has already been encrypted’** or ‘encrypting a bit stream of data that has already been encrypted and associated with its decryption algorithm.’”

“The Court’s conclusion is further supported by the fact that the operative steps of the claim can be performed by a human with pen and paper. (*See, e.g.*, Dkt. No. 73 at 8:22-10:2 (**‘[E]ncrypting data and encrypting messages has been done for hundreds of years.’**)).”

Torus Ventures LLC v. Cawley Partners, LLC, 2025 WL 1799327, at *6 (E.D. Tex. June 30, 2025) (citation omitted)

Authentication Is An Abstract Idea



“[W]e conclude that, at *Alice* step one, the asserted claims are directed to a method for **verifying the identity of a user** to facilitate an economic transaction, for which computers are merely used in a conventional way, rather than a technological improvement to computer functionality itself.”

Universal Secure Registry LLC v. Apple Inc., 10 F.4th 1342, 1350 (Fed. Cir. 2021)

Multi-Factor Authentication Is An Age-Old Concept



The Claims Recite Only Results-Based Functional Language; No “How”



“Claim 1 recites a method for routing information **using result-based functional language**. The claim requires the functional results of ‘converting,’ ‘routing,’ ‘controlling,’ ‘monitoring,’ and ‘accumulating records,’ but **does not sufficiently describe how to achieve these results in a non-abstract way.**”

Two-Way Media Ltd. v. Comcast Cable Commc'ns, LLC, 874 F.3d 1329, 1337 (Fed. Cir. 2017)



“As we have ‘repeatedly’ held, **to avoid ineligibility, ‘a claim must have the specificity required to transform the claim from one claiming only a result to one claiming a way of achieving it.’**”

Realtime Data LLC v. Array Networks Inc., 2023 WL 4924814, at *8 (Fed. Cir. Aug. 2, 2023)

The Claims Recite Only Results-Based Functional Language; No “How”

1. A method for permitting a third-party entity to gain access, in a secure manner, to an online account held by an account holder that is secured by a multi-factor authentication protocol, comprising the following steps performed by the third-party entity:

- collecting the account holder's credentials;
- encrypting the account holder's credentials using one or more processors;
- storing the account holder's encrypted credentials using one or more processors, wherein the encrypted credentials are stored in a data store;
- verifying the account holder's credentials by accessing, via one or more processors, the online account using the account holder's credentials;
- receiving a multi-factor authentication request from the online account, the multi-factor authentication request indicating that a response is required from the account holder before further access to the online account is granted;
- prompting the account holder for a response and receiving the response thereto from the account holder; and
- transmitting the account holder's response to the online account to satisfy the multi-factor authentication request.

Plaintiff's Step One Arguments Fail

1

The claimed solution did not exist “before computers were invented”

2

The claims provide a “technological solution to a technological problem”

3

The claims require “specialized” computer hardware

4

Claim construction is required

Plaintiff's Step One Arguments Fail

1

The claimed solution did not exist “before computers were invented”

2

The claims provide a “technological solution to a technological problem”

3

The claims require “specialized” computer hardware

4

Claim construction is required

Plaintiff's "Before Computers Existed" Argument Is Wrong

Plaintiff's Opposition

Indeed, Defendant *never alleges* that the process described in the claims—collecting and encrypting credentials and using them to satisfy a multi-factor authentication request without user intervention—is a known practice that humans performed well before computers were invented.

Plaintiff's Opp. at 1–2

Defendant does not argue that the patent here is such “a quintessential ‘do it on a computer’ patent” or that the claimed solution existed before computers were invented.

Plaintiff's Opp. at 9

But the claims do not merely facilitate a transaction in a way that was known before computers existed.

Plaintiff's Opp. at 22

Plaintiff's "Before Computers Existed" Argument Is Legally Wrong



“[T]he use of **generic machine learning technology** in carrying out the claimed methods for generating event schedules and network maps.”

Recentive Analytics, Inc. v. Fox Corp., 134 F.4th 1205, 1212–14 (Fed. Cir. 2025)



“[E]lectric vehicle charging stations that are connected to a network. The stations are connected to the local power grid, and electric vehicles connect to the stations by way of an electrical connector.”

ChargePoint, Inc. v. SemaConnect, Inc., 920 F.3d 759, 764, 766–70 (Fed. Cir. 2019)

Plaintiff's "Before Computers Existed" Argument Is Factually Wrong



Plaintiff's Step One Arguments Fail

1

The claimed solution did not exist “before computers were invented”

2

The claims provide a “technological solution to a technological problem”

3

The claims require “specialized” computer hardware

4

Claim construction is required

The Claims Provide No “Technological Solution”

Plaintiff's Opposition

In order for the system to work on an ongoing basis, the individual would need to provide an authentication code every time the financial management system accessed any of the individual's accounts that were protected by such protocols.

Plaintiff's Opp. at 3

More accurately, the claims are directed to the technological solutions of enabling a third-party to gain secure access to online accounts that are otherwise protected by a multi-factor authentication protocol (Claim 1), and enabling future access without requiring the account holder to be present (Claim 2), as SAT pleaded in its complaint.

Plaintiff's Opp. at 13

The Claims Require User Input

1. A method for permitting a third-party entity to gain access, in a secure manner, to an online account held by an account holder that is secured by a multi-factor authentication protocol, comprising the following steps performed by the third-party entity:

collecting the account holder's credentials;

encrypting the account holder's credentials using one or more processors;

storing the account holder's encrypted credentials using one or more processors, wherein the encrypted credentials are stored in a data store;

verifying the account holder's credentials by accessing, via one or more processors, the online account using the account holder's credentials;

receiving a multi-factor authentication request from the online account, the multi-factor authentication request indicating that a response is required from the account holder before further access to the online account is granted;

prompting the account holder for a response and receiving the response thereto from the account holder; and

transmitting the account holder's response to the online account to satisfy the multi-factor authentication request.

2. The method of claim 1, further comprising the steps of: storing one or more of the account holder's endpoints for the online account in a data store associated with the online account; and

utilizing said one or more endpoints to permit the third-party to gain access to the online account, or information pertaining to the online account, without requiring a response by the account holder to any subsequent multi-factor authentication requests.

The Claims Provide No “Technological Solution”



“To be patent eligible, software inventions must make ‘non-abstract improvements to existing technological processes and computer technology.’”

Dropbox, Inc. v. Synchronoss Techs., Inc., 815 F. App’x 529, 535 (Fed. Cir. 2020)

Plaintiff's Step One Arguments Fail

1

The claimed solution did not exist “before computers were invented”

2

The claims provide a “technological solution to a technological problem”

3

The claims require “specialized” computer hardware

4

Claim construction is required

The Claims Require No “Specialized Computer Hardware”

Plaintiff's Opposition

Further, the solution disclosed in the '090 patent can only be implemented using specialized computer hardware.

Plaintiff's Opp. at 10

The Claims Require No “Specialized Computer Hardware”



“[We] have **repeatedly held that features that are not claimed are irrelevant** as to step 1 or step 2 of the *Mayo/Alice* analysis.”

Am. Axle & Mfg., Inc. v. Neapco Holdings LLC, 967 F.3d 1285, 1293 (Fed. Cir. 2020)

The Claims Require No “Specialized Computer Hardware”

1. A method for permitting a third-party entity to gain access, in a secure manner, to an online account held by an account holder that is secured by a multi-factor authentication protocol, comprising the following steps performed by the third-party entity:

- collecting the account holder's credentials;
- encrypting the account holder's credentials using one or more processors;
- storing the account holder's encrypted credentials using one or more processors, wherein the encrypted credentials are stored in a data store;
- verifying the account holder's credentials by accessing, via one or more processors, the online account using the account holder's credentials;
- receiving a multi-factor authentication request from the online account, the multi-factor authentication request indicating that a response is required from the account holder before further access to the online account is granted;
- prompting the account holder for a response and receiving the response thereto from the account holder; and
- transmitting the account holder's response to the online account to satisfy the multi-factor authentication request.

Plaintiff's Step One Arguments Fail

1

The claimed solution did not exist “before computers were invented”

2

The claims provide a “technological solution to a technological problem”

3

The claims require “specialized” computer hardware

4

Claim construction is required

Plaintiff's Unsupported Claim Construction Argument Should Be Ignored

Plaintiff's Opposition

To the extent there is any dispute about what kind of “processors” the claims require or what the “encrypting” limitation entails, “the court must proceed by adopting the non-moving party’s constructions”—here, that the “processors” are specialized processors that can implement the “encrypting” limitation, which requires 256-bit bank-level encryption and headless browsing—or by resolving claim construction first.

Plaintiff's Opp. at 12

Plaintiff's Unsupported Claim Construction Argument Should Be Ignored



“[W]hile Sanderling identified terms it wanted the district court to construe before deciding Snap’s motion, Sanderling failed to provide proposed constructions for those terms. Sanderling also **failed to explain why any proposed constructions were not frivolous or how its constructions would make any difference to the *Alice* analysis.** Thus, the district court did not err by resolving the motion to dismiss without first undertaking claim construction.”

Sanderling Mgmt. Ltd. v. Snap Inc., 65 F.4th 698, 704 (Fed. Cir. 2023)

Plaintiff's Cited Cases Are Inapplicable

InsideSales.com, Inc. v. SalesLoft, Inc.,

No. 2:16-cv-859-DAK, 2017 WL 2559932, at *2 (D. Utah June 13, 2017)

Systems and methods that track when emails are opened and monitor where and for how long the recipient visits specific portions of the website



Plaintiff's Cited Cases Are Inapplicable

InsideSales.com, Inc. v. SalesLoft, Inc.



“Certified mail or return-receipt delivery only notifies the sender that the mail was delivered, not opened or acted upon. SalesLoft’s abstract idea challenge is without merit as there is **no credible argument that a patent on a system and methods for ‘monitoring website activity’ claims a longstanding commercial practice.** The functionalities claimed in the patents were not imaginable before the Internet. **Even after email came into use, the functionality claimed in the patents did not exist until plaintiff’s invention solved the technical problems associated with how email normally worked.”**

InsideSales.com, Inc. v. SalesLoft, Inc., No. 2:16-cv-859-DAK, 2017 WL 2559932, at *2 (D. Utah June 13, 2017)

Plaintiff's Cited Cases Are Inapplicable

InsideSales.com, Inc. v. SalesLoft, Inc.



“Rather, the patents claim something far more valuable: systems and methods that provide notice when a sent email has been opened, not just delivered. In addition, the systems and methods can identify whether the recipient clicks on an embedded hyperlink and monitor where and for how long the recipient visits specific portions of the website. **This type of information for a salesperson is not a longstanding business practice.**”

“**In this case, the patents-in-suit overcame the problem of finding out whether a user opened an email or clicked on a link within the email. Those are problems confined to the Internet, and the patents provide Internet-based solutions.**”

InsideSales.com, Inc. v. SalesLoft, Inc., No. 2:16-cv-859-DAK, 2017 WL 2559932, at *2, *3 (D. Utah June 13, 2017)

Plaintiff's Cited Cases Are Inapplicable

InsideSales.com, Inc. v. SalesLoft, Inc.



1. A system for monitoring website behavior of an email recipient, comprising:
control logic configured to modify an outgoing email addressed to the email recipient and sent using an email client configured to allow a sender to send the outgoing email and access one or more personal or corporate emails belonging to the sender, wherein the control logic configured to modify the outgoing email is further configured to edit the outgoing email to include a tracking code, wherein the tracking code is uniquely associated with the outgoing email, the email recipient, the sender or the business entity associated with the sender or a combination thereof, and wherein the tracking code is inserted into a hyperlink in the modified outgoing email; and
control logic configured to monitor the website behavior of the email recipient using information contained in the modified outgoing email;
wherein upon the email recipient clicking on the hyperlink, a connection to a remote server is made in which the tracking code is transmitted to the remote server; the remote server being used to manage a website referenced by the hyperlink; and
wherein upon receipt of the tracking code by the remote server, the remote server is able to use the tracking code to monitor the website behavior of the email recipient.

InsideSales.com, Inc. v. SalesLoft, Inc., No. 2:16-cv-859-DAK, 2017 WL 2559932, at *4 (D. Utah June 13, 2017) (citing cl. 1 of the '533 patent)

Plaintiff's Cited Cases Are Inapplicable

CosmoKey Solutions GmbH & Co. KG v. Duo Security LLC,

15 F.4th 1091, 1094 (Fed. Cir. 2021)

Method of authenticating a user to a transaction terminal

Fig. 7

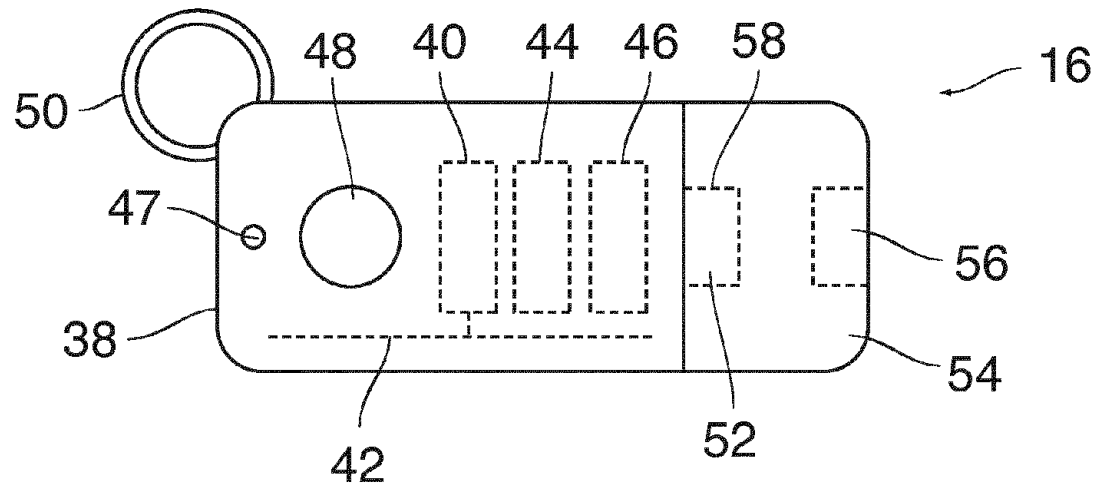
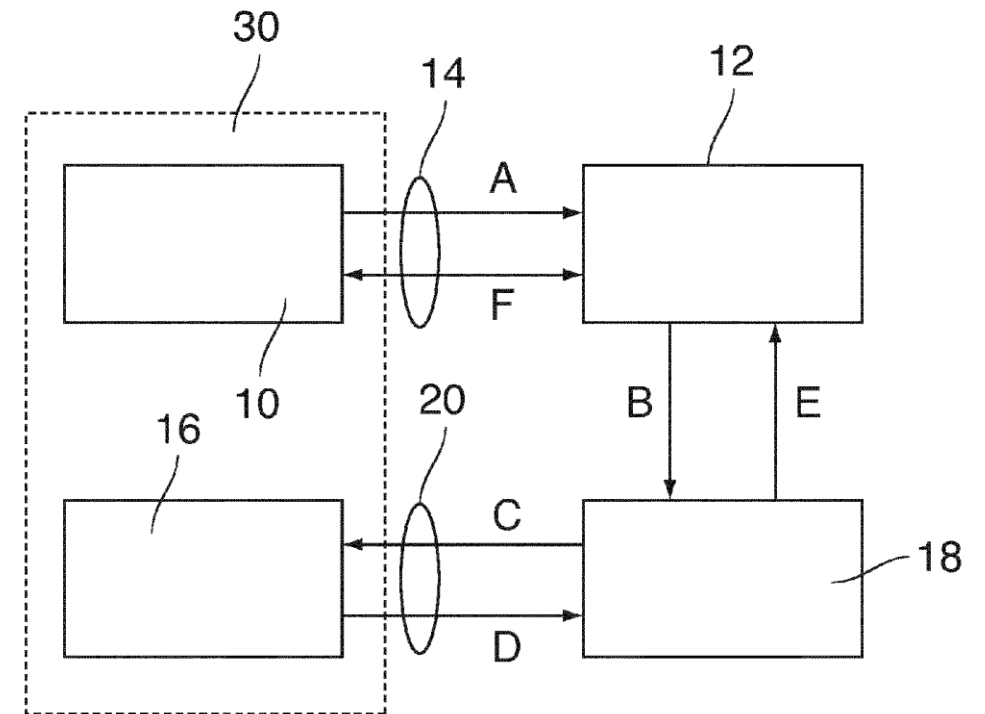


Fig. 5

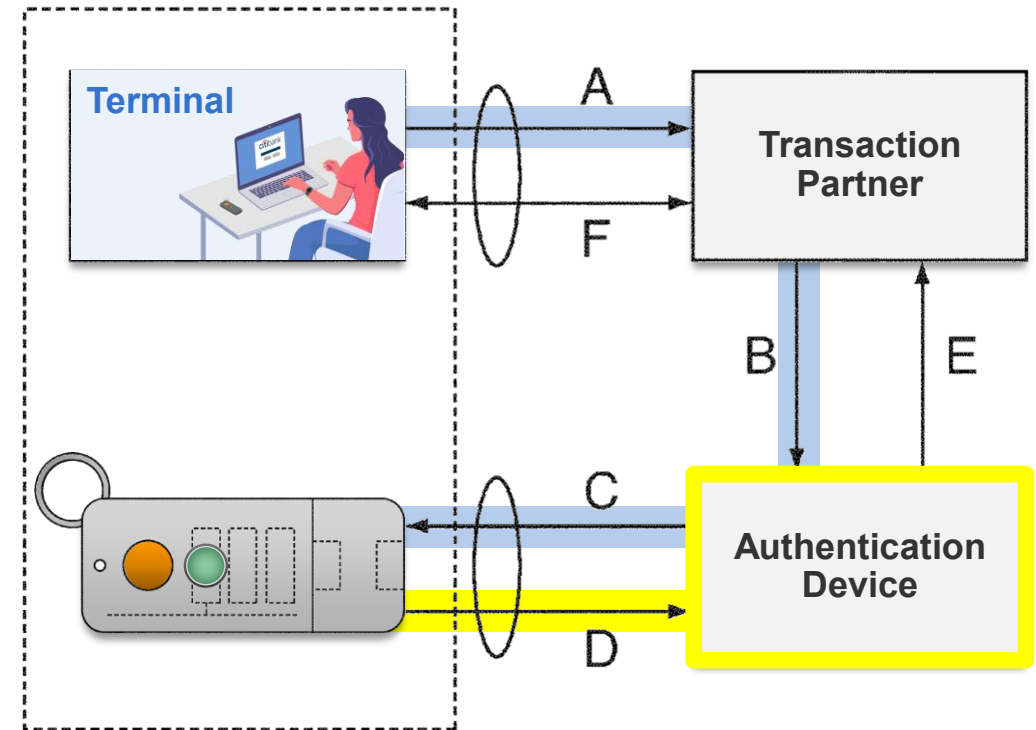
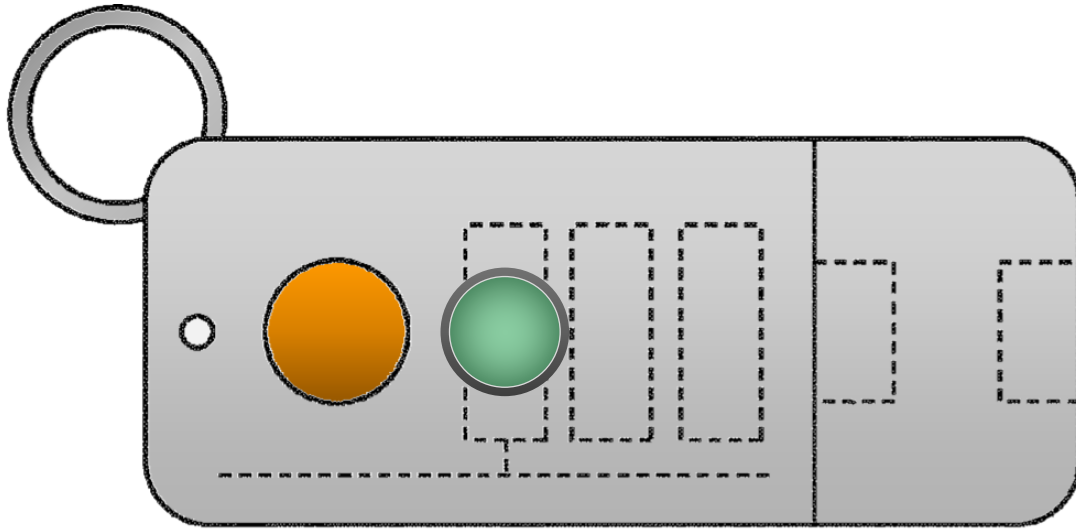


Plaintiff's Cited Cases Are Inapplicable

CosmoKey Solutions GmbH & Co. KG v. Duo Security LLC,

15 F.4th 1091, 1094 (Fed. Cir. 2021)

Method of authenticating a user to a transaction terminal



Plaintiff's Cited Cases Are Inapplicable

CosmoKey Solutions GmbH & Co. KG v. Duo Security LLC



1. A method of authenticating a user to a transaction at a terminal, comprising the steps of:
transmitting a user identification from the terminal to a transaction partner via a first communication channel,
providing an authentication step in which an authentication device uses a second communication channel for checking an authentication function that is implemented in a mobile device of the user,
as a criterion for deciding whether the authentication to the transaction shall be granted or denied, having the authentication device check whether a predetermined time relation exists between the transmission of the user identification and a response from the second communication channel,
ensuring that the authentication function is normally inactive and is activated by the user only preliminarily for the transaction,
ensuring that said response from the second communication channel includes information that the authentication function is active, and
thereafter ensuring that the authentication function is automatically deactivated.

“Here, the claim limitations are more specific and recite an improved method for overcoming hacking by ensuring that the authentication function is normally inactive, activating only for a transaction, communicating the activation within a certain time window, and thereafter ensuring that the authentication function is automatically deactivated. The specification explains that these features in combination with the other elements of the claim constitute an improvement that increases computer and network security, prevents a third party from fraudulently identifying itself as the user, and is easy to implement and can be carried out even with mobile devices of low complexity.”

CosmoKey Solutions GmbH & Co. KG v. Duo Security LLC, 15 F.4th 1091, 1099 (Fed. Cir. 2021) (citing cl. 1 of the '903 patent)

SAT Exhibit 2003, page 51

Plaintiff's Step One Arguments Fail

1

The claimed solution did not exist “before computers were invented”

2

The claims provide a “technological solution to a technological problem”

3

The claims require “specialized” computer hardware

4

Claim construction is required

Plaintiff's Step One Arguments Fail



The claimed solution did not exist “before computers were invented”



The claims provide a “technological solution to a technological problem”



The claims require “specialized” computer hardware



Claim construction is required

The Asserted Claims of the '090 Patent Are Ineligible

1

Step One: The claims are directed to the abstract idea of using a third-party intermediary to facilitate a transaction

2

Step Two: The claims have **no inventive concept** because the claims recite only known components functioning in their routine manner

Alice Step Two



“We have described step two of this analysis as a search for an ‘inventive concept’—*i.e.*, an element or combination of elements that is ‘sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself.’”

Alice Corp. v. CLS Bank Int’l, 573 U.S. 208, 217–18 (2014)

Alice Step Two



“Claim limitations that recite **conventional, routine and well understood applications in the art** are insufficient to supply an inventive concept.”

BSG Tech LLC v. Buyseasons, Inc., 899 F.3d 1281, 1290 (Fed. Cir. 2018)



“We have repeatedly held that such **invocations of computers and networks that are not even arguably inventive are ‘insufficient to pass the test of an inventive concept in the application’** of an abstract idea.”

Electric Power Group, LLC v. Alstom S.A., 830 F.3d 1350, 1355 (Fed. Cir. 2016)

The Claims Require Only Conventional Components

1. A method for permitting a third-party entity to gain access, in a secure manner, to an online account held by an account holder that is secured by a multi-factor authentication protocol, comprising the following steps performed by the third-party entity:

- collecting the account holder's credentials;
- encrypting the account holder's credentials using one or more processors;
- storing the account holder's encrypted credentials using one or more processors, wherein the encrypted credentials are stored in a data store;
- verifying the account holder's credentials by accessing, via one or more processors, the online account using the account holder's credentials;
- receiving a multi-factor authentication request from the online account, the multi-factor authentication request indicating that a response is required from the account holder before further access to the online account is granted;
- prompting the account holder for a response and receiving the response thereto from the account holder; and
- transmitting the account holder's response to the online account to satisfy the multi-factor authentication request.

Alice Step Two

Alice Corp. v. CLS Bank Int'l



- 26.** A data processing system to enable the exchange of an obligation between parties, the system comprising:
a communications controller,
a first party device, coupled to said communications controller,
a data storage unit having stored therein
(a) information about a first account for a first party, independent from a second account maintained by a first exchange institution, and
(b) information about a third account for a second party, independent from a fourth account maintained by a second exchange institution; and
a computer, coupled to said data storage unit and said communications controller, that is configured to
(a) receive a transaction from said first party device via said communications controller;
(b) electronically adjust said first account and said third account in order to effect an exchange obligation arising from said transaction between said first party and said second party after ensuring that said first party and/or said second party have adequate value in said first account and/or said third account, respectively; and
(c) generate an instruction to said first exchange institution and/or said second exchange institution to adjust said second account and/or said fourth account in accordance with the adjustment of said first account and/or said third account, wherein said instruction being an irrevocable, time invariant obligation placed on said first exchange institution and/or said second exchange institution.

Alice Corp. v. CLS Bank Int'l, 573 U.S. 208, 226 (2014) (citing cl. 26 of the '375 patent)

SAT Exhibit 2003, page 58

The Claims Require Only Conventional Components



“[T]he claims recite both a **generic computer element** — a **processor** — and a series of generic computer ‘components’ that merely restate their individual functions.”

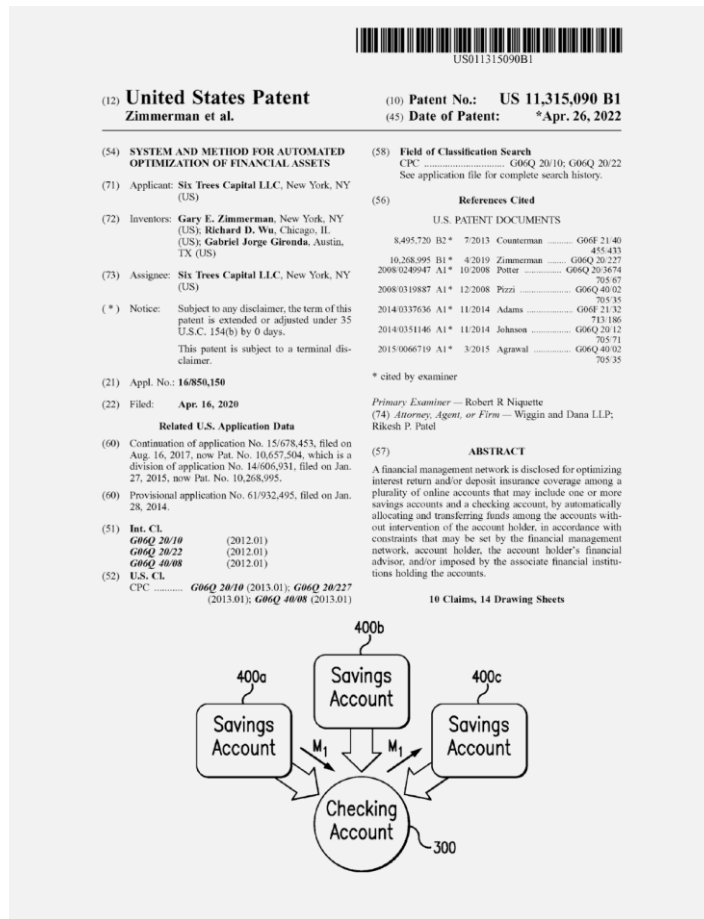
Intell. Ventures I LLC v. Cap. One Fin. Corp., 850 F.3d 1332, 1341 (Fed. Cir. 2017)



“No such inventive concept is present here. Instead, the claims ‘add’ only **generic computer components** such as an ‘**interface,**’ ‘**network,**’ and ‘**database.**’”

Mortg. Grader, Inc. v. First Choice Loan Servs. Inc., 811 F.3d 1314, 1324 (Fed. Cir. 2016)

The Claims Require Only Conventional Components



As described herein, the one or more processors of the financial management network 100 perform multiple processes that permit an account holder to access account information across his various accounts and that permit the financial management network 100 to interface with banks holding the one or more user accounts, and in particular to permit the financial management network 100 to login as the user by using the user's credentials stored in credential data store 120. Once logged into a user's account, these processes

data network 1100. Either or both of credential data store 120 and rule data store 130 may be configured as a database, for example, a relational database or key-value data storage system. Credential data store 120 and/or rule data store 130

Conventional Components Are Legally Insufficient

cxLoyalty, Inc. v. Maritz Holdings Inc.



“The claims apply the abstract idea on a computer by replacing the human intermediary with a GUI and API, but as the Board concluded, **representative claim 1 ‘merely recites generic and conventional computer components (i.e., ‘processor,’ ‘GUI,’ and ‘API’) and functionality for carrying out’ the abstract idea. And the ‘communication of information by GUIs and APIs’ was ‘well-known in the prior art.’ Accordingly, the claims do not survive step two.**”

cxLoyalty, Inc. v. Maritz Holdings Inc., 986 F.3d 1367, 1377 (Fed. Cir. 2021)

Conventional Components Are Legally Insufficient

Prism Technologies LLC v. T-Mobile USA, Inc.



1. A method for controlling access, by at least one **authentication server**, to protected computer resources provided via an **Internet Protocol network**, the method comprising:
 - receiving, at the at least one **authentication server** from at least one **access server**, identity data associated with at least one client computer device, the identity data forwarded to the at least one access server from the at least one client computer device with a request from the at least one client computer device for the protected computer resources;
 - authenticating, by the at least one authentication server, the identity data received from the at least one access server, the identity data being stored in the at least one authentication server;
 - authorizing, by the at least one authentication server, the at least one client computer device to receive at least a portion of the protected computer resources requested by the at least one client computer device, based on data associated with the requested protected computer resources stored in at least one database associated with the at least one authentication server; and
 - permitting access, by the at least one authentication server, to the at least the portion of the protected computer resources upon successfully authenticating the identity data and upon successfully authorizing the at least one client computer device.

Prism Techs. LLC v. T-Mobile USA, Inc., 696 F. App'x 1014, 1016 (Fed. Cir. 2017) (citing cl. 1 of the '345 patent)

The Dependent Claims Lack Any Inventive Concept

Plaintiff does not argue the dependent claims separately from claim 1

Claims 4 and 9

The credentials are “collected via a **user interface**.”

and/or 400c. In embodiments, client interface 200 may be, for example, a desktop or terminal computer, or may be a mobile device incorporating a computer such as a smart-phone, PDA, wearable computer, laptop computer, or tablet computer. It will be understood that **any device capable** of connecting to data network 1100 may be configurable as a suitable **client interface**.

Claims 5 and 10

The account holder’s credentials are “collected from a **data store**”

data network 1100. Either or both of credential data store 120 and rule data store 130 may be configured as a **database**, for example, a relational database or key-value data storage system. Credential data store 120 and/or rule data store 130

The Dependent Claims Lack Any Inventive Concept

Plaintiff does not argue the dependent claims separately from claim 1

Claims 2 and 7

“storing one or more of the account holder’s **endpoints** for the online account in a data store” and “utilizing” them “to permit the third-party to gain access to the online account, or information pertaining to the online account, without requiring a response by the account holder to any subsequent multi-factor authentication requests”

authentication request and gain access to the site. Once the product program 110 has access to the American Express site, it adds to the user data stored by the site an additional multi-factor authentication endpoint, e.g., an additional phone number or email address, that is accessible either directly by the product program 110 or, in some cases, via a third-party software service provider, and to which subsequent authentication codes may be sent.

Plaintiff Merely Repeats Its Step One Arguments at Step Two

Plaintiff's Opposition

[T]he patent here explains that the “network implements unique and inventive concepts that permit it to act as proxy for the user and respond to any multifactor authentication . . . in a way that does not require user intervention, while simultaneously maintaining rigid security measures to avoid unauthorized access to the user’s accounts by other parties,” ’090 patent at 18:53–60 (citation omitted). To do this, the claims “leverag[e] specialized computer hardware and software, computer logic, and encryption, to overcome a method of security that was intended to be impenetrable.”

Plaintiff's Opp. at 16

The Claims Require User Input

1. A method for permitting a third-party entity to gain access, in a secure manner, to an online account held by an account holder that is secured by a multi-factor authentication protocol, comprising the following steps performed by the third-party entity:

collecting the account holder's credentials;

encrypting the account holder's credentials using one or more processors;

storing the account holder's encrypted credentials using one or more processors, wherein the encrypted credentials are stored in a data store;

verifying the account holder's credentials by accessing, via one or more processors, the online account using the account holder's credentials;

receiving a multi-factor authentication request from the online account, the multi-factor authentication request indicating that a response is required from the account holder before further access to the online account is granted;

prompting the account holder for a response and receiving the response thereto from the account holder; and

transmitting the account holder's response to the online account to satisfy the multi-factor authentication request.

2. The method of claim 1, further comprising the steps of: storing one or more of the account holder's endpoints for the online account in a data store associated with the online account; and

utilizing said one or more endpoints to permit the third-party to gain access to the online account, or information pertaining to the online account, without requiring a response by the account holder to any subsequent multi-factor authentication requests.

Use of the Abstract Idea From Step One Cannot Provide the Required Inventive Concept at Step Two



“It has been clear since *Alice* that a claimed invention’s **use of the ineligible concept to which it is directed cannot supply the inventive concept** that renders the invention ‘significantly more’ than that ineligible concept.”

“As a matter of law, **narrowing or reformulating an abstract idea does not add ‘significantly more’ to it.**”

BSG Tech LLC v. Buyseasons, Inc., 899 F.3d 1281, 1290, 1291 (Fed. Cir. 2018)

The Examiner's Unexplained Withdrawal of a Section 101 Rejection Is Not Binding On This Court

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Case 2:25-cv-00514-DAK-JCB Document 1-2 Filed 06/26/25 PageID.85 Page 29
of 113

Docket No.: 103771-500
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: Gary E. Zimmerman Docket No.: 103771-500
Application No.: 16/850,150 Art Unit: 3691
Filed: April 16, 2020 Examiner: Niquette, Robert R.
Conf. No. 1088
Title: SYSTEM AND METHOD FOR AUTOMATED OPTIMIZATION OF
FINANCIAL ASSETS

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicant hereby submits the following Arguments as an attachment to the concurrently filed Pre-Appeal Brief Request for Review Form (PTO/SB/33). A Notice of Appeal is being filed concurrently herewith.

ARGUMENTS

Applicant's claims recite a method for permitting a third-party entity to gain access, in a secure manner, to an online account held by an account holder, where such account is secured by a multi-factor authentication protocol. The present claims recite the use of an encrypted process that enables individual investors to manage, in a secure way, a multitude of bank accounts through a single interface. In doing so, users can obtain increased FDIC insurance coverage and earn higher returns. The present claims recite the use of an endpoint (i.e., phone number, email address) that is stored in a database and associated with the user's (e.g., account holder's) online account, wherein the endpoint is used to relay a multi-factor authentication code after the user's account login credentials have been verified. The user's credentials are encrypted using one or more processors to enhance the security protocols of the method recited in the independent claims. After the user's credentials have been verified, and at subsequent step, Applicant's claimed method then interacts with the endpoint to satisfy multi-factor authentication. In doing so, the method of the present claims can pass both prongs of a multi-factor authentication test,

This solution, disclosed by Applicant's claimed methods, can only be implemented using specialized computer hardware for several reasons: 1) a human call center could not serve this function, for no savvy bank customer would ever provide their unencrypted username/password combination necessary to access their bank account to another untrusted human -- in fact, doing so would violate the agreement that exists between a bank and its customers; 2) specialized computer systems are required to implement 256-bit bank-level encryption to protect these login credentials, which is the only known safe and trusted way to transmit and store such credentials; and 3) specialized computer hardware is necessary to power the headless browsers that are able to use logic to interpret bank websites and interact with their various messages, prompts, data input boxes, and action buttons. The claims of the present application are thus novel and inventive. Indeed, there being no prior art rejections, Applicant will address the rejection of all of the claims under 35 U.S.C. § 101 as being directed to a judicial exception without significantly more.

The Examiner's Unexplained Withdrawal of a Section 101 Rejection Is Not Binding On This Court



“The USPTO’s decision finding a patent eligible is **not binding on this court**. . . . Accordingly, courts regularly find patents ineligible under § 101 even though those patents had been previously examined and allowed by the USPTO.”

WhitServe LLC v. Dropbox, Inc., 2019 WL 3342949, at *7 (D. Del. July 25, 2019), *aff’d*, 854 F. App’x 367 (Fed. Cir. 2021)

Plaintiff's Conclusory Allegations Fail to Save the Claims



“[A] district court need not accept a patent owner’s conclusory allegations of inventiveness.”

IBM Corp. v. Zillow Grp., Inc., 50 F.4th 1371, 1379 (Fed. Cir. 2022)



“[A]ny allegation about inventiveness, wholly divorced from the claims or the specification does not defeat a motion to dismiss.”

Dropbox, Inc. v. Synchronoss Techs., Inc., 815 F. App’x 529, 538 (Fed. Cir. 2020)

Plaintiff Proposes No New Factual Allegations on Patent Eligibility



“The district court denied leave to amend as futile because it concluded that the new factual allegations in the [proposed amended complaint] did not save the asserted claims from ineligibility at the pleadings stage.”

Simio, LLC v. Flexsim Software Prods., Inc., 983 F.3d 1353, 1364 (Fed. Cir. 2020)

Plaintiff Proposes No New Factual Allegations on Patent Eligibility

D. If the Court Grants Defendant's Motion, Dismissal Should Be Without Prejudice

If the Court grants Defendant's motion to dismiss, then it should do so without prejudice and allow SAT to amend its complaint to include additional allegations showing the claims are directed to a technological solution. As Defendant explains in its motion, dismissal with prejudice is appropriate only if the intrinsic record "show[s] that the claim elements were well understood, routine, and conventional." Mot. 23–24. Defendant has not pointed to anything in the patent that shows the process described in the claims was well-understood, routine, or conventional. All Defendant offers are conclusory statements that each step in isolation is "routine." Mot. 4, 21. "Here, allowing [SAT] to file the proposed amended complaint, which alleges facts directed to the inventive concepts in its claimed invention, would not be futile." *Aatrix*, 882 F.3d at 1126. Indeed, Defendant has not asserted that any potential amendment would be futile. The Court should therefore provide SAT leave to amend its complaint if the Court grants Defendant's motion.