# United States Court of Appeals for the Federal Circuit

---

**UNIVERSAL SECURE REGISTRY LLC,**
*Plaintiff-Appellant*

**v.**

**APPLE INC., VISA INC., VISA U.S.A. INC.,**
*Defendants-Appellees*

---

2020-2044

---

Appeal from the United States District Court for the District of Delaware in No. 1:17-cv-00585-CFC-SRF, Judge Colm F. Connolly.

---

Decided: August 26, 2021

---

KATHLEEN M. SULLIVAN, Quinn Emanuel Urquhart & Sullivan, LLP, New York, NY, argued for plaintiff-appellant. Also represented by BRIAN MACK, KEVIN ALEXANDER SMITH, San Francisco, CA; TIGRAN GULEDJIAN, CHRISTOPHER MATHEWS, Los Angeles, CA.

MARK D. SELWYN, Wilmer Cutler Pickering Hale and Dorr LLP, Palo Alto, CA, argued for defendant-appellee Apple Inc. Also represented by LIV LEILA HERRIOT, THOMAS GREGORY SPRANKLING; MONICA GREWAL, Boston, MA.

STEFFEN NATHANAEL JOHNSON, Wilson, Sonsini, Goodrich & Rosati, PC, Washington, DC, argued for defendants-appellees Visa Inc., Visa U.S.A. Inc. Also represented by MATTHEW A. ARGENTI, JAMES C. YOON, Palo Alto, CA.

---

Before TARANTO, WALLACH,* and STOLL, *Circuit Judges*.

STOLL, *Circuit Judge*.

Universal Secure Registry LLC (USR) appeals the United States District Court for the District of Delaware's dismissal of certain patent infringement allegations against Apple Inc., Visa Inc., and Visa U.S.A. Inc. (collectively, "Apple") under Rule 12(b)(6) of the Federal Rules of Civil Procedure. The district court held all claims of four asserted patents owned by USR ineligible under 35 U.S.C. § 101. Because we conclude that all claims of the asserted patents are directed to an abstract idea and that the claims contain no additional elements that transform them into a patent-eligible application of the abstract idea, we affirm.

## BACKGROUND

### I

USR sued Apple for allegedly infringing all claims of U.S. Patent Nos. 8,856,539; 8,577,813; 9,100,826; and 9,530,137 (collectively, the "asserted patents"). The '137 patent is a continuation of the '826 patent. Although the patents are otherwise unrelated, they are directed to similar technology—securing electronic payment transactions. As USR explained in its opening brief, its patents "address the need for technology that allows consumers to conveniently make payment-card [e.g., credit card]

---

* Circuit Judge Evan J. Wallach assumed senior status on May 31, 2021.

transactions without a magnetic-stripe reader and with a high degree of security." Appellant's Br. 7. "For example, it allows a person to purchase goods without providing credit card information to the merchant, thereby preventing the credit card information from being stolen or used fraudulently." *Id.* at 9.

II

Apple moved to dismiss the complaint under Federal Rule of Civil Procedure 12(b)(6), arguing that the asserted patents claimed patent-ineligible subject matter under 35 U.S.C. § 101. The magistrate judge determined that all the representative claims are directed to a non-abstract idea. *Universal Secure Registry, LLC v. Apple Inc.*, No. 17-cv-00585, 2018 WL 4502062, at *8–11 (D. Del. Sept. 19, 2018). The magistrate judge explained that the '539 patent claims are "not directed to an abstract idea because 'the plain focus of the claims is on an improvement to computer functionality itself, not on economic or other tasks for which a computer is used in its ordinary capacity.'" *Id.* at *8 (quoting *Visual Memory LLC v. NVIDIA Corp.*, 867 F.3d 1253, 1258 (Fed. Cir. 2017)). Of particular importance to the magistrate judge was the conclusion that the claimed invention provided a more secure authentication system. *See id.* at *9.

The district court disagreed, concluding that the representative claims fail at both steps one and two of *Alice Corp. v. CLS Bank International*, 573 U.S. 208 (2014). *Universal Secure Registry LLC* (*USR*) *v. Apple Inc.*, 469 F. Supp. 3d 231, 236–37 (D. Del. 2020). The district court explained that the claimed invention was directed to the abstract idea of "the secure verification of a person's identity" and that the patents do not disclose an inventive concept—including an improvement in computer functionality—that transforms the abstract idea into a patent-eligible application. *Id.* Accordingly, the district court

granted Apple's motion to dismiss for failure to state a claim under Rule 12(b)(6). *Id.* at 240.

USR appeals. We have jurisdiction under 28 U.S.C. § 1295(a)(1).

## DISCUSSION

We apply regional circuit law when reviewing a district court's dismissal for failure to state a claim under Rule 12(b)(6). *XY, LLC v. Trans Ova Genetics, LC*, 968 F.3d 1323, 1329 (Fed. Cir. 2020). The Third Circuit reviews such dismissals de novo, accepting as true all factual allegations in the complaint and viewing those facts in the light most favorable to the non-moving party. *Klotz v. Celentano Stadtmauer & Walentowicz LLP*, 991 F.3d 458, 462 (3d Cir. 2021) (citing *Foglia v. Renal Ventures Mgmt., LLC*, 754 F.3d 153, 154 n.1 (3d Cir. 2014)).

Patent eligibility under § 101 is a question of law based on underlying facts, so we review a district court's ultimate conclusion on patent eligibility de novo. *Interval Licensing LLC v. AOL, Inc.*, 896 F.3d 1335, 1342 (Fed. Cir. 2018). We have held that patent eligibility can be determined at the Rule 12(b)(6) stage "when there are no factual allegations that, taken as true, prevent resolving the eligibility question as a matter of law." *Aatrix Software, Inc. v. Green Shades Software, Inc.*, 882 F.3d 1121, 1125 (Fed. Cir. 2018).

## I

Section 101 defines patent-eligible subject matter as "any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof." 35 U.S.C. § 101. Long-standing judicial exceptions, however, provide that laws of nature, natural phenomena, and abstract ideas are not eligible for patenting. *ChargePoint, Inc. v. SemaConnect, Inc.*, 920 F.3d 759, 765 (Fed. Cir. 2019) (citing *Alice*, 573 U.S. at 216).

The Supreme Court has articulated a two-step test for examining patent eligibility when a patent claim is alleged to involve one of these three types of subject matter. *See Alice*, 573 U.S. at 217–18. The first step of the *Alice* test requires a court to determine whether the claims at issue are directed to a patent-ineligible concept, such as an abstract idea. *Id.* at 218. "[T]he claims are considered in their entirety to ascertain whether their character as a whole is directed to excluded subject matter." *McRO, Inc. v. Bandai Namco Games Am. Inc.*, 837 F.3d 1299, 1312 (Fed. Cir. 2016) (quoting *Internet Pats. Corp. v. Active Network, Inc.*, 790 F.3d 1343, 1346 (Fed. Cir. 2015)). If the claims are directed to a patent-ineligible concept, the second step of the *Alice* test requires a court to "examine the elements of the claim to determine whether it contains an 'inventive concept' sufficient to 'transform' the claimed abstract idea into a patent-eligible application." *Alice*, 573 U.S. at 221 (quoting *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 72, 78–79 (2012)). This inventive concept must do more than simply recite "well-understood, routine, conventional activity." *Mayo*, 566 U.S. at 79–80.

In cases involving authentication technology, patent eligibility often turns on whether the claims provide sufficient specificity to constitute an improvement to computer functionality itself. For example, in *Secured Mail Solutions LLC v. Universal Wilde, Inc.*, we held that claims directed to using a marking (e.g., a conventional barcode) affixed to the outside of a mail object to communicate information about the mail object, including claims reciting a method for verifying the authenticity of the mail object, were abstract. 873 F.3d 905, 907, 910–11 (Fed. Cir. 2017). We explained that the claims were not directed to specific details of the barcode or of the equipment for generating and processing the barcode. *See id.* at 910. Nor was there a description of how the barcode was generated, or how that barcode was different from long-standing

identification practices. *See id.* At step two, we determined that there was no inventive concept that transformed the claimed abstract idea into a patent-eligible application of the abstract idea. *See id.* at 912. We explained that the claims recited well-known and conventional ways to verify an object using a barcode and to allow generic communication between a sender and recipient using generic computer technology, and that the patents themselves suggested that all the hardware used was conventional. *See id.*

In *Electronic Communication Technologies, LLC v. ShoppersChoice.com, LLC*, we drew a similar conclusion about claims focused on monitoring the location of a "mobile thing" and using authentication software to increase security. 958 F.3d 1178, 1181 (Fed. Cir. 2020). As to the authentication limitations—"namely, enabling a first party to input authentication information, storing the authentication information, and providing the authentication information along with the advance notice of arrival to help ensure the customer that the notice was initiated by an authorized source"—we determined that these limitations were themselves abstract and thus were not an inventive concept. *Id.* We pointed to the specification, which stated that the claimed "authentication information" could be essentially any information recognizable to the party being contacted. *Id.* We also noted that businesses have long been recording customer information that would qualify as authentication information as broadly defined in the specification. *See id.* at 1182.

Similarly, in *Solutran, Inc. v. Elavon, Inc.*, we held ineligible claims that recited a method for electronically processing checks, which included electronically verifying the accuracy of a transaction to avoid check fraud, because the claims were directed to a long-standing commercial practice of crediting a merchant's account as soon as possible. 931 F.3d 1161, 1163, 1167 (Fed. Cir. 2019). We recognized that the claims only recited conventional steps that were

not directed to an improvement to the way computers operate, noting that the patent specification explained that "verifying the accuracy of the transaction information . . . was already common." *Id.* at 1167. At step two, we rejected the argument that reordering these conventional steps constituted an inventive concept, and held that using a general-purpose computer and scanner to perform the conventional activities of transaction verification does not amount to an inventive concept. *Id.* at 1168–69.

Finally, in *Prism Technologies LLC v. T-Mobile USA, Inc.*, the claims broadly recited "receiving" identity data of a client computer, "authenticating" the identity of the data, "authorizing" the client computer, and "permitting access" to the client computer. 696 F. App'x 1014, 1016 (Fed. Cir. 2017). We held that the claims at issue were directed to the abstract idea of "providing restricted access to resources" because the claims did not cover a "concrete, specific solution." *Id.* at 1017. Rather, the claims merely recited generic steps typical of any conventional process for restricting access, including processes that predated computers. *Id.* At step two, we determined that the asserted claims recited conventional generic computer components employed in a customary manner such that they were insufficient to transform the abstract idea into a patent-eligible invention. *Id.*

## II

With this precedent in mind, we turn to the patent claims at issue in this case. We address each patent in turn.

### A

We first consider the claims of the '539 patent. The '539 patent is titled "Universal Secure Registry" and explains that most people carry multiple forms of identification to verify their identities and make purchases, '539 patent col. 1 ll. 53–67, but that they may not always

want to disclose their personal information during financial transactions, *id.* at col. 2 ll. 1–27. Thus, the '539 patent proposes "an identification system that will enable a person to be identified or verified . . . and/or authenticated without necessitating the provision of any personal information." *Id.* at col. 2 l. 64–col. 3 l. 1. The patent purports to accomplish this goal through use of a Universal Secure Registry or "USR system or database . . . [that] may take the place of multiple conventional forms of identification." *Id.* at col. 3 ll. 22–24. Access to the USR system may be gained through a user's electronic ID device, which may be a smart card, cell phone, pager, wristwatch, computer, personal digital assistant, key fob, or other commonly available electronic devices. *Id.* at col. 3 l. 64–col. 4 l. 4.

One embodiment of the invention facilitates purchasing goods or services without revealing personal financial information to a merchant. *See id.* at col. 11 l. 46–col. 12 l. 18. When a user initiates a purchase, the user enters a secret code in the user's electronic ID device to cause the ID device to generate a one-time code. *Id.* at col. 11 ll. 51–56. After the user presents the one-time code to the merchant, the merchant transmits the code, the store number, the amount of the purchase, and the time of receipt to the credit card company. *Id.* at col. 11 ll. 56–59. The credit card company then passes the code to the USR system, which determines if the code is valid and, "if valid, accesses the user's credit card information and transmits the appropriate credit card number to the credit card company." *Id.* at col. 11 ll. 59–65. The credit card company then checks the credit worthiness of the user and either "declines the card or debits the user's account in accordance with its standard transaction processing system." *Id.* at col. 12 ll. 6–9. "The credit card company then notifies the merchant of the result of the transaction." *Id.* at col. 12 ll. 9–11.

> Claim 22 is representative of the '539 patent claims at issue and states as follows:

> 22. A method for providing information to a provider to enable transactions between the provider and entities who have secure data stored in a secure registry in which each entity is identified by a time-varying multicharacter code, the method comprising:
>
> receiving a transaction request including at least the time-varying multicharacter code for an entity on whose behalf a transaction is to take place and an indication of the provider requesting the transaction;
>
> mapping the time-varying multicharacter code to an identity of the entity using the time-varying multicharacter code;
>
> determining compliance with any access restrictions for the provider to secure data of the entity for completing the transaction based at least in part on the indication of the provider and the time-varying multicharacter code of the transaction request;
>
> accessing information of the entity required to perform the transaction based on the determined compliance with any access restrictions for the provider, the information including account identifying information;
>
> providing the account identifying information to a third party without providing the account identifying information to the provider to enable or deny the transaction; and
>
> enabling or denying the provider to perform the transaction without the provider's knowledge of the account identifying information.

*Id.* at col. 20 ll. 4–31.

The district court held that claim 22 is not materially different from the claims at issue in *Prism*. As discussed above, in *Prism*, we determined that the claims were directed to the process of "(1) receiving identity data from a device with a request for access to resources; (2) confirming the authenticity of the identity data associated with that device; (3) determining whether the device identified is authorized to access the resources requested; and (4) if authorized, permitting access to the requested resources." *Prism*, 696 F. App'x at 1017. Here, the district court stated that claim 22 requires the following steps:

> (1) "receiving" a transaction request with a time-varying multicharacter code and "an indication of" the merchant requesting the transaction; (2) "mapping" the time-varying multicharacter code to the identity of the customer in question; (3) "determining" whether the merchant's access to the customer's secure data complies with any restrictions; (4) "accessing" the customer's account information; (5) "providing" the account identifying information to a third party without providing that information to the merchant; and (6) "enabling or denying" the merchant to perform the transaction without obtaining knowledge of the customer's identifying information.

*USR*, 469 F. Supp. 3d at 237. Based on the similarities between these steps and those in the claims at issue in *Prism*, the district court determined that claim 22 is directed to "the abstract idea of obtaining the secure verification of a user's identity to enable a transaction." *Id.*

While we see differences between claim 22 and the claims at issue in *Prism*, we agree with the district court that, like the claims at issue in *Prism*, claim 22 is directed to an abstract idea. 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 is used to access a database that indicates any restrictions on the user's transactions with the merchant and also 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. In our view, the claims "simply recite conventional actions in a generic way" (e.g., receiving a transaction request, verifying the identity of a customer and merchant, allowing a transaction) and "do not purport to improve any underlying technology." *Solutran*, 931 F.3d at 1168. Accordingly, the claims are directed to an abstract idea under *Alice* step one.

USR cites *Ancora Technologies, Inc. v. HTC America, Inc.*, to assert that the claims' recitation of a time-varying multicharacter code used in combination with additional intermediaries constitutes a specific technique that departs from earlier approaches to solve a specific computer problem. 908 F.3d 1343 (Fed. Cir. 2018). We are unpersuaded. In *Ancora*, the claimed invention identified a specific technique for addressing the vulnerability of license-authorization software to hacking in an unexpected way—by storing the software license record in the computer's BIOS memory. *Id.* at 1348–49. Using the BIOS memory to assist with software verification was unexpected because it had never previously been used in that way. *Id.* The claimed invention of the '539 patent, on the other hand, uses a combination of conventional components in a conventional way to achieve an expected result. *See, e.g.*, '539 patent col. 7 ll. 30–36 (disclosing a SecurID™ card or its equivalent as an example of a single use code generator). While we appreciate that the claims here are closer to the demarcation line between what is abstract and non-abstract than the claims in *Prism*, we 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.

Turning to *Alice* step two, the district court rejected USR's argument that the claim's recitations of (1) time-varying codes and (2) sending data to a third-party as opposed to the merchant each rise to the level of an inventive concept. *USR*, 469 F. Supp. 3d at 238. We agree. Regarding USR's first argument, the patent itself acknowledges that the claimed step of generating time-varying codes for authentication of a user is conventional and long-standing. '539 patent col. 8 ll. 17–35 (disclosing use of a "SecurID™ card available from RSA Security," which "retrieves a secret user code and/or time varying value from memory and obtains from the user a secret personal identification code").

And with regard to USR's second argument—that the step of bypassing the merchant's computer constitutes an inventive concept—USR cites *BASCOM Global Internet Services, Inc. v. AT&T Mobility LLC*, where we determined that claims directed to a method and system of filtering Internet content using the individual account association capability of some Internet Service Provider (ISP) servers were a "technical improvement over prior art ways of filtering such content." 827 F.3d 1341, 1350, 1352 (Fed. Cir. 2016). In that case, we reasoned that although "[f]iltering content on the Internet was already a known concept, . . . the patent describes how its particular arrangement of elements is a technical improvement over prior art ways of filtering such content." *Id.* at 1350. Unlike was the case in *BASCOM*, however, the Supreme Court has previously held the use of a third-party intermediary in a financial transaction to be an ineligible abstract idea. *Alice*, 573 U.S. at 219–20. In *Alice*, the claims involved "a method of exchanging financial obligations between two parties using a third-party intermediary to mitigate settlement risk." *Id.* at 219. Similarly, the claims here involve allowing a financial transaction between two parties using a third-party

intermediary to mitigate information security risks. Because sending data to a third-party as opposed to the merchant is itself an abstract idea, it cannot serve as an inventive concept. *BASCOM*, 827 F.3d at 1349 ("An inventive concept that transforms the abstract idea into a patent-eligible invention must be significantly more than the abstract idea itself . . . ." (citing *Alice*, 573 U.S. at 223–24)).

B

We next consider the claims of the '813 patent. The '813 patent is also titled "Universal Secure Registry" and the invention bears resemblance to that in the '539 patent. The '813 patent discloses combined use of a user device (e.g., cell phone), a point-of-sale (POS) device, and a universal secure registry to facilitate financial transactions. '813 patent col. 43 ll. 6–15. One embodiment of the claimed invention contemplates the user device communicating with a secure database in the secure registry, which stores account information, such as credit card and debit card account information, for multiple accounts. *Id.* at col. 44 ll. 39–53. This allows users to employ a single user device or cell phone to conduct financial transactions at a POS device using a plurality of different credit or debit accounts. *Id.* at col. 45 ll. 4–17.

Before the user device can access the secure registry, however, certain authentication processes must be completed. One embodiment contemplates first restricting access to the user device until the user has been authenticated using biometric input provided to the user device. *Id.* at col. 46 ll. 37–41. Next, the secure registry also requires that the user be authenticated before account information is accessed. *Id.* at col. 45 ll. 18–20. Some embodiments employ a multi-factor authentication process whereby encrypted authentication information is generated by the user device. *Id.* at col. 46 ll. 14–36. That is, the claimed invention can authenticate the user based on a combination of two or more of (1) "something the user

knows" (e.g., PIN number); (2) "something the user is" (e.g., a biometric measurement as detected by a biometric sensor); (3) "something that the user has" (e.g., cell phone serial number); and (4) an "account selected by the user for the current transaction" (e.g., the transaction for which the authentication is being completed). *Id.* at col. 45 l. 63–col. 46 l. 21. This encrypted authentication information is then communicated to the secure registry for authentication through the POS device and, if authentication is successful, the transaction and access to the user's account is permitted. *Id.* at col. 46 ll. 27–36.

Claim 1 of the '813 patent is representative:

> 1. An electronic ID device configured to allow a user to select any one of a plurality of accounts associated with the user to employ in a financial transaction, comprising:
>
> a biometric sensor configured to receive a biometric input provided by the user;
>
> a user interface configured to receive a user input including secret information known to the user and identifying information concerning an account selected by the user from the plurality of accounts;
>
> a communication interface configured to communicate with a secure registry;
>
> a processor coupled to the biometric sensor to receive information concerning the biometric input, the user interface and the communication interface, the processor being programmed to activate the electronic ID device based on successful authentication by the electronic ID device of at least one of the biometric input and the secret information, the processor also being programmed such that once the electronic ID device is activated the processor is configured to generate a non-predictable value and to generate encrypted authentication

> information from the non-predictable value, information associated with at least a portion of the biometric input, and the secret information, and to communicate the encrypted authentication information via the communication interface to the secure registry; and
>
> wherein the communication interface is configured to wirelessly transmit the encrypted authentication information to a point-of-sale (POS) device, and wherein the secure registry is configured to receive at least a portion of the encrypted authentication information from the POS device.

*Id.* at col. 51 l. 65–col. 52 l. 29.

The district court held that the claims are directed to the abstract idea of "collect[ing] and examin[ing] data to authenticate the user's identity." *USR*, 469 F. Supp. 3d at 239. We agree with the district court that the claims are directed to an abstract idea, not a technological solution to a technological problem, as USR asserts. In our view, the claims are directed to an electronic ID device that includes a biometric sensor, user interface, communication interface, and processor working together to (1) authenticate the user based on two factors—biometric information and secret information known to the user—and (2) generate encrypted authentication information to send to the secure registry through a point-of-sale device. There is no description in the patent of a specific technical solution by which the biometric information or the secret information is generated, or by which the authentication information is generated and transmitted. In our view, as with the '539 patent, the claims recite "conventional actions in a generic way"—e.g., authenticating a user using conventional tools and generating and transmitting that authentication—without "improv[ing] any underlying technology." *Solutran*, 931 F.3d at 1168. Accordingly, the claims are directed to an abstract idea under *Alice* step one.

USR asserts that the claims solve a problem in an existing technological process using a novel form of data the patent describes as "encrypted authentication information." Appellant's Br. 44. USR reasons that, like the claimed invention in *Finjan, Inc. v. Blue Coat Systems, Inc.*, 879 F.3d 1299 (Fed. Cir. 2018), this encrypted authentication information is a non-abstract improvement in computer functionality. Appellant's Br. 45. We are not persuaded. In *Finjan*, we determined that the claimed invention was not abstract because it claimed the use of a "behavior-based" virus scan that was able to identify and compile unique information about potentially hostile operations, while the traditional scan method was limited to recognizing the presence of previously identified viruses. 879 F.3d at 1304. Unlike in *Finjan*, the claimed "encrypted authentication data" here is merely a collection of conventional data combined in a conventional way that achieves only expected results. *See* '813 patent col. 46 ll. 21–27 ("For example, in one embodiment, encrypted authentication information is generated from a non-predictable value generated by the user device 352, identifying information for the selected user account 360, and at least one of the biometric information and secret information the user knows (for example, a PIN)."). We thus conclude that the claims are directed to the abstract idea of collecting and examining data to enable authentication.

Turning to *Alice* step two, the district court explained that the specification "describes the Electronic ID Device as 'any type of electronic device' capable of accessing a secure identification system database." *USR*, 469 F. Supp. 3d at 239 (citation omitted). The court added that the patent also "describes the device as consisting of well-known, generic components, including a computer processor." *Id.* at 239–40. Based on this, the court determined that the claims do not recite an inventive concept sufficient to transform the claimed abstract idea into a patent-eligible application.

We agree with the district court that the claims fail to recite an inventive concept that would transform the abstract idea into patentable subject matter. As we explained above, the "encrypted authentication data" is merely a combination of known authentication techniques that yields only expected results. For example, the '813 patent specification explains that a one-time non-predictable code can be generated by the "SecurID™ card available from RSA Security," as well as "other smart cards" or an algorithm programmed onto a processor. '813 patent col. 12 l. 45–col. 13 l. 5. The '813 patent specification also discloses that identifying information may include something as well-known as "a unique serial number" on a check. *Id.* at col. 17 ll. 26–29. Moreover, the specification explains that a user may be verified using "any combination of a memorized PIN number or code, biometric information such as a fingerprint, voice print, signature, iris or facial scan, or DNA analysis, or any other method of identifying the person possessing the device." *Id.* at col. 4 ll. 29–34; *see also id.* at col. 2 ll. 59–64 (disclosing that prior art uses "biometric sensors that sense one or more biometric feature[s]"). There is nothing in the specification suggesting, or any other factual basis for a plausible inference (as needed to avoid dismissal), that the claimed combination of these conventional authentication techniques achieves more than the expected sum of the security provided by each technique. *Cf. TecSec, Inc. v. Adobe Inc.*, 978 F.3d 1278, 1295–96 (Fed. Cir. 2020) (explaining that multilevel security using a combination of secure labeling with encryption constituted an inventive concept where the patent specification made clear that "the focus of the claimed advance is on improving . . . a data network used for broadcasting a file to a large audience" and the improvement was "an efficient way for the sender to permit different parts of the audience to see different parts of the file"). In other words, the combination of these long-standing conventional methods of authentication yields expected results of an additive increase in security. Moreover, as we have

previously explained, verifying the identity of a user to facilitate a transaction is a fundamental economic practice that has been performed at the point of sale well before the use of POS computers and Internet transactions. *See Elec. Commc'n Techs.*, 958 F.3d at 1182.

C

We next turn to the claims of the '826 patent. The '826 patent is entitled "Method and Apparatus for Secure Access Payment and Identification." The specification discloses a system for authenticating identities of users, including a first handheld device configured to transmit authentication information and a second device configured to receive the authentication information. '826 patent, Abstract. The first and second handheld devices are configured to wirelessly communicate with each other so that the entity associated with the first handheld device can communicate his or her identity to the entity associated with the second handheld device. *Id.* at col. 28 ll. 40–44. One embodiment of the claimed invention contemplates configuring the first handheld device so that the first entity cannot gain access to the first device without providing a PIN or biometric data (e.g., a fingerprint). *Id.* at col. 28 ll. 56–65. The second handheld device can be configured in the same manner for a second user, *id.* at col. 29 ll. 8–16, or not have a user at all, *id.* at col. 32 ll. 43–56.

Once at least the first user successfully authenticates their identity to the first handheld device, the first device may transmit a first wireless signal containing encrypted authentication information of the first user to the second device. *Id.* at col. 30 ll. 46–58. This encrypted authentication information may be generated from biometric information received from the first handheld device, and may include generating a non-predictable signal using that biometric information. *Id.* at col. 35 ll. 22–28. For example, the signal may include multiple fields, including a digital signature field (e.g., biometric data), further identifying

information (e.g., name, height, weight, eye color), and a one-time varying code field (e.g., a PKI encrypted one-time DES key). *Id.* at col. 31 l. 55–col. 32 l. 31. The second handheld device may then authenticate the first user by decrypting the authentication information and verifying the identity of the first user. *Id.* at col. 32 ll. 43–56.

Claim 10 is representative of the '826 patent claims at issue and states as follows:

> 10. A computer implemented method of authenticating an identity of a first entity, comprising acts of:
>
> authenticating, with a first handheld device, a user of the first handheld device as the first entity based on authentication information;
>
> retrieving or receiving first biometric information of the user of the first handheld device;
>
> determining a first authentication information from the first biometric information;
>
> receiving with a second device, the first authentication information of the first entity wirelessly transmitted from the first handheld device;
>
> retrieving or receiving respective second authentication information for the user of the first handheld device; and
>
> authenticating the identity of the first entity based upon the first authentication information and the second authentication information.

*Id.* at col. 45 ll. 30–47.

The district court held that the claims are "directed to the abstract idea of secured verification of a person's identity." *USR*, 469 F. Supp. 3d at 238. It reasoned that the method steps disclosed do not recite "a technological solution but instead disclose an authentication method that is

accomplished by retrieving and reviewing information, including biometric information, using a handheld device and a second device, to authenticate a user's identification." *Id.* at 238–39. Further, the district court explained that the specification does not disclose "a technological solution for obtaining, generating, or analyzing biometric information, which the patent defines generically as 'any . . . method of identifying the person possessing the device.'" *Id.* at 239 (alteration in original) (quoting '826 patent col. 4 ll. 27–32).

We agree with the district court that the claims are directed to an abstract idea. Specifically, the claims are directed to multi-factor authentication of a user's identity using two devices to enable a transaction. Although USR contends that the claims cover an innovative technological solution to address problems specific to prior authentication systems, it does not proffer a persuasive argument in support of that conclusion because the claims do not include sufficient specificity. *See* Appellant's Br. 50–51. Rather, the claims generically provide for the collection of biometric information to generate a first authentication information, and then authenticating a user using both the biometric-information-derived first authentication and a second authentication information. The specification even discloses that this information is conventional. *See* '826 patent col. 2 ll. 57–62 (disclosing that prior art devices use "biometric sensors that sense one or more biometric feature[s]"); *id.* at col. 1 ll. 49–53 (disclosing that prior art completes multi-factor authentication using "software located on a device being employed to access the secure computer network and on a server within the secure computer network"). There is no description of a specific technical solution by which the biometric information is generated, or by which the authentication information is transmitted. Because the claims broadly recite generic steps and results—as opposed to a specific solution to a technological problem—we hold that the claims are abstract under *Alice*

step one. *Solutran*, 931 F.3d at 1168 (holding claims to be directed to an abstract idea "where the claims simply recite[d] conventional actions in a generic way . . . and [did] not purport to improve any underlying technology").

Turning to *Alice* step two, the district court determined that the claims do not recite "any improvements to handheld or other devices or technological solutions that enable such devices and biometric information to be combined to authenticate a user's identity remotely." *USR*, 469 F. Supp. 3d at 239. Rather, the court explained, the claims are directed to "the routine use of biometric information, mobile devices, onetime variable tokens, and/or multiple devices to authenticate a person," which "is not inventive and does not make the claimed authentication method patentable under § 101." *Id.*

We agree with the district court's conclusion that the claims do not recite an inventive concept. Rather, the asserted claims recite well-known and conventional ways to perform authentication. *Secured Mail*, 873 F.3d at 912 (holding that the claims lacked an inventive concept where the claims recited only well-known and conventional ways to allow generic communication between a sender and recipient using generic computer technology). For example, the '826 patent explains that "the biometric information can be fingerprint information, a voiceprint, DNA codes of the first user, or any other biometric information known and used by those of skill in the art." '826 patent col. 33 ll. 22–25. The claims are likewise broad and nonspecific. Indeed, the claimed second authentication information could be anything from a social security number to a digital signature generated with a user's private PKI key. *See id.* at col. 31 l. 55–col. 32 l. 31. Thus, the claims do not recite a new authentication technique, but rather combine nonspecific, conventional authentication techniques in a noninventive way. There is nothing in the specification suggesting, or any other factual basis for a plausible inference (as needed to avoid dismissal), that the claimed

combination of these conventional authentication techniques achieves more than the expected sum of the security provided by each technique.

D

Finally, we consider the claims of the '137 patent. The '137 patent is a continuation of the '826 patent, and similarly discloses a system for authenticating identities of users, including a first handheld device configured to transmit authentication information and a second device configured to receive the authentication information. '137 patent, Abstract. The first and second wireless devices can include a user interface with a display and a biometric sensor, where the devices may be accessed by authenticating the user of the device using secret information (e.g., PIN number). *Id.* at col. 29 ll. 21–53.

As in the '826 patent, here an embodiment of the claimed invention contemplates the first device transmitting a first wireless signal containing encrypted authentication information of the first user to the second device. *Id.* at col. 31 ll. 19–57. This encrypted authentication information may be generated from biometric information received from the first device, and may include generating a non-predictable signal using that biometric information. *Id.* at col. 36 ll. 1–7. The second device may then authenticate the first user by decrypting the authentication information and verifying the identity of the first user. *Id.* at col. 33 ll. 20–34.

Claim 12 is a system claim and is representative of the '137 patent claims at issue:

> 12. A system for authenticating a user for enabling a transaction, the system comprising:
>
> a first device including:
>
> a biometric sensor configured to capture a first biometric information of the user;

> a first processor programmed to: 1) authenticate a user of the first device based on secret information, 2) retrieve or receive first biometric information of the user of the first device, 3) authenticate the user of the first device based on the first biometric, and 4) generate one or more signals including first authentication information, an indicator of biometric authentication of the user of the first device, and a time varying value; and
>
> a first wireless transceiver coupled to the first processor and programmed to wirelessly transmit the one or more signals to a second device for processing;
>
> wherein generating the one or more signals occurs responsive to valid authentication of the first biometric information; and
>
> wherein the first processor is further programmed to receive an enablement signal indicating an approved transaction from the second device, wherein the enablement signal is provided from the second device based on acceptance of the indicator of biometric authentication and use of the first authentication information and use of second authentication information to enable the transaction.

*Id.* at col. 46 l. 55–col. 47 l. 14.

The district court held that the claims are directed to the abstract idea of a "system for authenticating a user for enabling a transaction." *USR*, 469 F. Supp. 3d at 240 (quoting '137 patent col. 46 ll. 55–56). In reaching this conclusion, the court emphasized that the claims recite, and the specification discloses, generic well-known components—"a device, a biometric sensor, a processor, and a transceiver—performing routine functions—retrieving,

receiving, sending, authenticating—in a customary order." *Id.*

Although claim 12 of the '137 patent is more detailed than claim 10 of the '826 patent, we nonetheless agree with the district court that it too is directed to an abstract idea. Claim 12 is directed to multi-factor authentication of a user's identity using two devices to enable a transaction. In particular, the claim recites authenticating a user based on secret information, authenticating the user based on a first biometric information, and generating one or more signals including first authentication information, an indicator of biometric authentication of the user of the first device, and a time varying value to send to a second device, where that second device will then generate an enablement signal based on the biometric authentication, the first authentication information, and second authentication information.

Though we appreciate that claim 12 of the '137 patent includes limitations not found in claim 10 of the '826 patent, the claims still are not sufficiently specific. We have previously held claims abstract "where the claims simply recite conventional actions in a generic way" without purporting to improve the underlying technology. *Solutran*, 931 F.3d at 1168; *see also McRO*, 837 F.3d at 1314 (we look to whether the claims "focus on a specific means or method that improves the relevant technology or are instead directed to a result or effect that itself is the abstract idea and merely invoke generic processes and machinery" (citing *Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1326, 1336 (Fed. Cir. 2016))). This is true here. For example, claim 12 does not tell a person of ordinary skill what comprises the secret information, first authentication information, and second authentication information. While we recognize that some of the dependent claims provide more specificity on these aspects, what is claimed is still merely conventional. Indeed, the specification discloses that each authentication technique is conventional. *See* '137 patent col.

3 ll. 1–6 (disclosing that prior art devices use "biometric sensors that sense one or more biometric feature[s]"); *id.* at col. 1 ll. 60–64 (disclosing that prior art completes multi-factor authentication using "software located on a device being employed to access the secure computer network and on a server within the secure computer network"); *id.* at col. 4 ll. 42–46 (disclosing that biometric information may be any of a "fingerprint, voice print, signature, iris or facial scan, or DNA analysis"); *id.* at col. 32 ll. 31–58 (disclosing that the authentication information may include "name information, a badge number, an employee number, an e-mail address, a social security number, and the like," a "digital signature" using a user's "private PKI key," and a "one-time varying code" that "includes a random code as generated by the first wireless device"); *id.* at col. 1 l. 64–col. 2 l. 3 (disclosing that known authentication software included software installed on two separate devices).

USR's assertion that this claim is akin to the claim in *Finjan* is similarly unavailing. As we explained above, the claimed invention in *Finjan* employed a new kind of file enabling a computer system to do things it could not do before, namely "behavior-based" virus scans. 879 F.3d at 1304. Here, the claimed invention merely combines conventional authentication techniques—first authentication information, a biometric authentication indicator, and a time-varying value—to achieve an expected cumulative higher degree of authentication integrity. Without some unexpected result or improvement, the claimed idea of using three or more conventional authentication techniques to achieve a higher degree of security is abstract. Likewise, as claimed in this patent, the idea of using two devices for authentication using these multiple conventional techniques is also abstract. For all these reasons, the claims are directed to an abstract idea rather than a technological solution to a technical problem.

Turning to step two, the district court determined that claim 12 "lacks the inventive concept necessary to convert

the claimed system into patentable subject matter." *USR*, 469 F. Supp. 3d at 240. On appeal, USR asserts that the use of a time-varying value, a biometric authentication indicator, and authentication information that can be sent from the first device to the second device form an inventive concept. Appellant's Br. 41. We disagree. As we explained above, the specification makes clear that each of these devices and functions is conventional. *See supra* at 24–25. Further, we conclude that adding them all together is itself directed to the conventional idea of multi-factor authentication. USR further asserts that authenticating a user at two locations constitutes an inventive concept because it is locating the authentication functionality at a specific, unconventional location within the network. Appellant's Br. 41 (citing *BASCOM*, 827 F.3d at 1350). Unlike the claims in *BASCOM*, however, the specification suggests that the claims here only recite a conventional location for the authentication functionality. *See* '137 patent col. 1 ll. 60–64 (disclosing that prior art completes multi-factor authentication using "software located on a device being employed to access the secure computer network and on a server within the secure computer network"). Thus, nothing in the claims is directed to a new authentication technique; rather, the claims are directed to combining longstanding, known authentication techniques to yield expected additory amounts of security. There is nothing in the specification suggesting, or any other factual basis for a plausible inference (as needed to avoid dismissal), that the combination of these conventional authentication techniques results in an unexpected improvement beyond the expected sum of the security benefits of each individual authentication technique.

## CONCLUSION

We have considered USR's remaining arguments and find them unpersuasive. For the foregoing reasons, we

affirm the district court's decision to dismiss, as the asserted patents claim unpatentable subject matter.

**AFFIRMED**