United States Court of Appeals for the Federal Circuit

COSMOKEY SOLUTIONS GMBH & CO. KG,
Plaintiff-Appellant

v.

DUO SECURITY LLC, FKA DUO SECURITY, INC.,
Defendant-Appellee

2020-2043

Appeal from the United States District Court for the District of Delaware in No. 1:18-cv-01477-CFC, Judge Colm F. Connolly.

Decided: October 4, 2021

SCOTT THOMAS WEINGAERTNER, White & Case LLP, New York, NY, argued for plaintiff-appellant. Also represented by STEFAN MENTZER, GRACE WANG, MATTHEW ROBERT WISNIEFF.

MARK A. LEMLEY, Durie Tangri LLP, San Francisco, CA, argued for defendant-appellee. Also represented by BETHANY BENGFORT.

Before O'MALLEY, REYNA, and STOLL, *Circuit Judges*.

Opinion for the court filed by *Circuit Judge* STOLL.

Concurring opinion filed by *Circuit Judge* REYNA.

STOLL, *Circuit Judge*.

CosmoKey Solutions GmbH & Co. KG appeals the United States District Court for the District of Delaware's entry of judgment on the pleadings holding that the asserted claims of CosmoKey's U.S. Patent No. 9,246,903 are ineligible under 35 U.S.C. § 101. The district court held that the asserted claims are directed to abstract ideas and fail to provide an inventive concept. We conclude that the claims of the '903 patent are patent-eligible under *Alice* step two because they recite a specific improvement to a particular computer-implemented authentication technique. Accordingly, we reverse the decision of the district court.

BACKGROUND

I

The '903 patent is titled "Authentication Method" and purports to disclose an authentication method that is both low in complexity and high in security. The abstract describes a method of authenticating the identity of a user performing a transaction at a terminal (e.g., a computer), including activating an authentication function on the user's mobile device. '903 patent Abstract, col. 2 ll. 35–40.

The patent specification recognizes that when a user communicates with a remote transaction partner (e.g., a bank, a store, or a secured database) via a communication channel like the Internet, "it is important to assure that an individual that identifies itself as an authorized user is actually the person it alleges to be." *Id.* at col. 1 ll. 15–19. The specification also describes several conventional authentication methods involving a user's mobile phone. *Id.* at col. 1 ll. 30–46. The specification discloses that by using a user's mobile device for authentication, the prior art

confirms "that the person carrying the mobile device, e.g., a mobile telephone, is actually present at the location of the terminal from which the transaction has been requested." *Id.* at col. 1 ll. 47–50. "Thus, as long as the user is in control of his mobile device, the authentication method assures that no third party can fake the identification data of this user and perform any transactions in his place." *Id.* at col. 1 ll. 50–53.

The specification purports to improve on these conventional mobile phone authentication methods in that, according to the invention, the "authentication function is normally inactive and is activated by the user only preliminarily for the transaction, said response from the second communication channel includes the information that the authentication is active, and the authentication function is automatically deactivated." *Id.* at col. 1 ll. 58–63. The specification explains the advantages of this method as follows: "In this method, the complexity of the authentication function can be reduced significantly" because all that is required "from the authentication function is to permit the authentication device to detect whether or not this function is active[,]" and "the only activity that is required from the user for authentication purposes is to activate the authentication function [within] a suitable timing." *Id.* at col. 1 l. 64–col. 2 l. 3. The specification explains that there is a "predetermined time relation" in that "the authentication function is activated within a certain (preferably short) time window after the transmission of the user identification." *Id.* at col. 2 ll. 8–14. The specification also touts the enhanced security provided by this method:

> Since the authentication function is normally inactive, the authentication will almost certainly fail when a third party fraudulently identifies itself as the user in order to initiate a transaction. Then, the authentication would be successful only in the very unlikely event that the true user happens to activate the authentication function of his mobile

> device just in the right moment. Even in this unlikely case the fraud could be detected . . . . Thus, notwithstanding the low complexity, the method according to the invention offers a high level of security.

Id. at col. 2 ll. 15–32.

The specification thus explains that the claimed invention "provide[s] an authentication method that is easy to handle and can be carried out with mobile devices of low complexity." *Id.* at col. 1 ll. 54–56. The specification elaborates that "[i]t is a particular advantage of the invention that the mobile device does not have to have any specific hardware for capturing or outputting information." *Id.* at col. 2 ll. 44–46. According to the specification, the mobile device need only be capable of being activated for a certain period of time and connecting to a mobile network where it has an address that is linked to the identification data of the user. *Id.* at col. 2 ll. 46–50. Then, the authentication device must be "capable of checking whether the authentication function of the mobile device with the associated address is active." *Id.* at col. 2 ll. 50–54.

Thus, instead of requiring the user to input multiple authentication factors using multiple communication channels, the user's identity is verified by transmitting the user identification via a first communication channel and checking via a second communication channel that an authentication function is activated in the user's mobile device. *Id.* at col. 1 ll. 3–9. Checking for an activated authentication function replaces the manual entry of information for an authentication factor by the user. For example, the user may activate the authentication function by activating their mobile device, *id.* at col. 2 ll. 56–60, or by activating an application on a mobile device, *see id.* at col. 6 ll. 59–62.

Claim 1 is the sole independent claim of the '903 patent and recites:

> 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.

Id. at col. 10 ll. 39–60.

II

In September 2018, CosmoKey sued Duo Security, Inc.[1] for infringement of the '903 patent. In October 2019, Duo moved for judgment on the pleadings pursuant to Rule 12(c) of the Federal Rules of Civil Procedure, arguing that

---

[1] Duo Security LLC was known as Duo Security, Inc. at the time of filing.

all claims of the '903 patent are ineligible under 35 U.S.C. § 101 as the claims are directed to the abstract idea of authentication and do not recite any patent-eligible inventive concept. The district court granted Duo's motion on June 24, 2020. *Money & Data Protection Lizenz GmpH & Co. KG, v. Duo Security, Inc.*, 468 F. Supp. 3d 674 (D. Del. 2020) (*Judgment Op.*).[2]

At step one of the *Alice* two-step framework for determining patent eligibility, the district court agreed with Duo that the claims of the '903 patent "are directed to the abstract idea of authentication—that is, the verification of identity to permit access to transactions." *Id.* at 677; *see Alice Corp. v. CLS Bank Int'l*, 573 U.S. 208, 217 (2014). The district court reasoned that the "[']903 patent is not materially different from the patent at issue in *Prism Tech[nologies] LLC v. T-Mobile USA, Inc.*, 696 F. App'x 1014 (Fed. Cir. 2017)," where we determined that the patent claims were invalid because they were "directed to the abstract idea of 'providing restricted access to resources.'" *Judgment Op.*, 468 F. Supp. 3d at 677 (citation omitted). The district court determined that, "[g]iven the similarities between the abstract processes in the [']903 patent and the patent in *Prism*, I find that the claims at issue here are directed to the abstract idea of verifying identity to permit access to transactions." *Id.* at 678.

At *Alice* step two, the district court concluded that "the [']903 patent merely teaches generic computer functionality to perform the abstract concept of authentication; and it therefore fails *Alice*'s step two inquiry." *Id.* at 678. In so holding, the district court determined that the patent itself admits that "the detection of an authentication function's activity and the activation by users of an authentication

---

[2] CosmoKey was known as Money and Data Protection Lizenz GmbH & Co. KG at the time it filed its original complaint.

function within a pre-determined time relation were well-understood and routine, conventional activities previously known in the authentication technology field." *Id.* at 679 (citing '903 patent col. 1 ll. 15–53).

CosmoKey appeals the district court's judgment. We have jurisdiction under 28 U.S.C. § 1295(a)(1).

DISCUSSION

We apply regional circuit law when reviewing a district court's judgment on the pleadings. *Koninklijke KPN N.V. v. Gemalto M2M GmbH*, 942 F.3d 1143, 1149 (Fed. Cir. 2019). Applying Third Circuit law, we review the district court's grant of Duo's motion for judgment on the pleadings de novo, accepting as true all facts pleaded by CosmoKey and drawing all reasonable inferences in favor of CosmoKey. *Allstate Prop. & Cas. Ins. Co. v. Squires*, 667 F.3d 388, 390 (3d Cir. 2012).

Patent eligibility under § 101 is a question of law that may contain underlying questions of fact. *Interval Licensing LLC v. AOL, Inc.*, 896 F.3d 1335, 1342 (Fed. Cir. 2018) (citing *Berkheimer v. HP Inc.*, 881 F.3d 1360, 1365 (Fed. Cir. 2018)). We review a district court's ultimate conclusion on patent eligibility de novo. *Id.* We have held that "[p]atent eligibility can be determined on the pleadings under Rule 12(c) when there are no factual allegations that, when taken as true, prevent resolving the eligibility question as a matter of law." *Data Engine Techs. LLC v. Google LLC*, 906 F.3d 999, 1007 (Fed. Cir. 2018).

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. The Supreme Court established a two-step test for examining patent eligibility under § 101 in *Alice*. First, we "determine whether the claims at issue are directed to a patent-ineligible concept[,]" such as an abstract idea. *Alice*, 573 U.S. at 218. If so, we proceed to step

two and "consider the elements of each claim both individually and 'as an ordered combination' to determine whether the additional elements 'transform the nature of the claim' into a patent-eligible application." *Id.* (quoting *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 78–79 (2012)). Step two is "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*, 573 U.S. at 217–18 (alteration in original) (quoting *Mayo*, 566 U.S. at 72–73).

I

As the district court noted, this court has previously considered the eligibility of various claims generally directed to authentication and verification under § 101 and found those claims abstract. For example, in *Prism*, the case cited by the district court, 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." 696 F. App'x at 1017. Rather, the claims recited generic steps typical of any conventional process for restricting access, including such processes that predated computers. In particular, the claims recited "receiving" a user identity, "authenticating" the user identity, "authorizing" the user, and "permitting access" to the user. *Id.* at 1016. 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.* at 1017–18.

More recently, in *Universal Secure Registry LLC v. Apple, Inc.*, 10 F.4th 1342 (Fed. Cir. 2021), we held that the patent claims were directed to the abstract idea of combining multiple conventional authentication techniques for verifying the identity of a user to facilitate a financial transaction. The patent specifications disclosed that

biometric authentication, multi-factor authentication, and using multiple devices to authenticate were all conventional authentication techniques. The claims, then, were simply directed to combining these long-standing, well-known authentication techniques to achieve the expected result of increased security no greater than the sum of the security provided by each technique alone. Under *Alice* step two, we held that these claims did not recite an inventive concept because the combination of long-standing conventional methods of authentication yielded expected results of an additive increase in security, and nothing in the record suggested an additional technological improvement.

In contrast, we have held claims directed to specific verification methods that depart from earlier approaches and improve computer technology eligible under § 101. In *Ancora Technologies Inc. v. HTC America, Inc.*, we held that claims directed to storing a verification structure in computer memory were directed to a specific non-abstract computer-functionality improvement addressing the "vulnerability of license-authorization software to hacking." 908 F.3d 1343, 1348–49 (Fed. Cir. 2018). We explained that "[i]mproving security . . . can be a non-abstract computer-functionality improvement if done by a specific technique that departs from earlier approaches to solve a specific computer problem." *Id.* at 1349 (citing *Finjan, Inc. v. Blue Coat Sys., Inc.*, 879 F.3d 1299, 1304–05 (Fed. Cir. 2008)). We further explained the claims "yield[ed] a tangible technological benefit" in making the system less susceptible to hacking by altering how the verification is performed. *Id.* at 1350.

II

Under *Alice* step one, we consider "what the patent asserts to be the 'focus of the claimed advance over the prior art.'" *Solutran, Inc. v. Elavon, Inc.*, 931 F.3d 1161, 1168 (Fed. Cir. 2019) (quoting *Affinity Labs of Tex., LLC*

v. DIRECTV, LLC, 838 F.3d 1253, 1257 (Fed. Cir. 2016)). The district court held that the claims "are directed to the abstract idea of authentication—that is, the verification of identity to permit access to transactions." *Judgment Op.*, 468 F. Supp. 3d at 677. We are not convinced that this broad characterization of the focus of the claimed advance is correct. Rather, the claims and written description suggest that the focus of the claimed advance is activation of the authentication function, communication of the activation within a predetermined time, and automatic deactivation of the authentication function, such that the invention provides enhanced security and low complexity with minimal user input. The critical question then is whether this correct characterization of what the claims are directed to is either an abstract idea or a specific improvement in computer verification and authentication techniques. *Ancora*, 908 F.3d at 1347.

We need not answer this question, however, because even if we accept the district court's narrow characterization of the '903 patent claims, the claims satisfy *Alice* step two. *See Amdocs (Israel) Ltd. v. Openet Telecom, Inc.*, 841 F.3d 1288, 1303 (Fed. Cir. 2016) (explaining that "even if [the claim] were directed to an abstract idea under step one, the claim is eligible under step two").[3]

Turning then to *Alice* step two, we "consider the elements of each claim both individually and 'as an ordered combination' to determine whether the additional elements 'transform the nature of the claim' into a patent-eligible application." *Alice*, 573 U.S. at 217 (quoting *Mayo*, 566 U.S. at 77–78). In computer-implemented inventions, the

---

[3] Judge Reyna's concurrence challenges our approach of accepting the district court's analysis under *Alice* step one and resolving the case under *Alice* step two. Judge Reyna Concurrence at 1. We note that this very approach was followed in *Amdocs*, 841 F.3d at 1303.

computer must perform more than "well-understood, routine, conventional activities previously known to the industry." *Id.* at 223 (quoting *Mayo*, 566 U.S. at 73 (internal quotation marks and brackets omitted)). In addition, "[a]n inventive concept that transforms the abstract idea into a patent-eligible invention must be significantly more than the abstract idea itself, and cannot simply be an instruction to implement or apply the abstract idea on a computer." *BASCOM Glob. Internet Servs., Inc. v. AT&T Mobility LLC*, 827 F.3d 1341, 1349 (Fed. Cir. 2016) (citing *Alice*, 573 U.S. at 222–23).

The district court held that the '903 patent failed at step two because it "merely teaches generic computer functionality to perform the abstract concept of authentication[.]" *Judgment Op.*, 468 F. Supp. 3d at 678. The court recognized that the specification indicates that the "difference between [the] prior art methods and the claimed invention is that the [']903 patent's method 'can be carried out with mobile devices of low complexity' so that 'all that has to be required from the authentication device function is to detect whether or not this function is active'" and that "the only activity that is required from the user for authentication purposes is to activate the authentication function at a suitable timing for the transaction." *Id.* at 678–79 (quoting '903 patent col. 1 l. 55–col. 2 l. 3). But the court cited column 1, lines 15–53 of the specification as purportedly admitting that detection of activation of an authentication function's activity and the activation by users of an authentication function within a pre-determined time relation were "well-understood and routine, conventional activities previously known in the authentication technology field." *Judgment Op.*, 468 F. Supp. 3d at 679.

We disagree with the district court's analysis and conclusion. The '903 patent claims and specification recite a specific improvement to authentication that increases security, prevents unauthorized access by a third party, is easily implemented, and can advantageously be carried out

with mobile devices of low complexity. *See* '903 patent col. 2 ll. 15–32. Contrary to the district court's conclusion, the '903 patent discloses a technical solution to a security problem in networks and computers. While authentication of a user's identity using two communication channels and a mobile phone was known at the time of the invention, nothing in the specification or anywhere else in the record supports the district court's suggestion that the last four claim steps—including (1) "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"; (2) "ensuring that the authentication function is normally inactive and is activated by the user only preliminarily for the transaction"; followed by (3) "ensuring that said response from the second communication channel includes information that the authentication function is active"; and (4) "thereafter ensuring that the authentication function is automatically deactivated," *id.* at col. 10 ll. 45–55—are conventional.

The district court's reliance on column 1, lines 15–53 as allegedly admitting that these steps were routine or conventional is misplaced. While column 1, lines 30–46 describes three prior art references, none teach the recited claim steps. To the contrary, the specification describes the prior art references as disclosing: (1) sending a prompt to a user to confirm the transaction followed by the user's mobile device sending a confirmation signal; (2) using a user's mobile device for activating and deactivating a credit card; and (3) sending a token to the user's terminal from which a transaction has been requested followed by the user's mobile device capturing the image and sending it back to the authentication device via a second communication channel. *Id.* at col. 1 ll. 30–46. Read in context, the rest of the passage cited by the district court makes clear that the claimed steps were developed by the inventors, are not admitted

prior art, and yield certain advantages over the described prior art. The district court erred in its interpretation of this passage. This is particularly so given the procedural posture of Duo's motion for judgment under Rule 12(c), which requires the district court to draw all reasonable inferences in favor of CosmoKey. *Allstate*, 667 F.3d at 390.

Indeed, the patent specification describes how the particular arrangement of steps in claim 1 provides a technical improvement over conventional authentication methods. Specifically, the specification emphasizes the inventive nature of these steps, explaining that "the complexity of the authentication function can be reduced significantly" because "the only activity that is required from the user for authentication purposes is to activate the authentication function at a suitable timing for the transaction." *Id.* at col. 1 l. 64–col. 2 l. 3. Continuing, the specification explains that compared to the prior art and conventional multifactor authentication systems, the '903 patent performs user authentication with fewer resources, less user interaction, and simpler devices. *Id.* at col. 1 ll. 54–56 ("It is an object of the invention to provide an authentication method that is easy to handle and can be carried out with mobile devices of low complexity.").

Duo argues that using a second communication channel in a timing mechanism and an authentication function that is normally inactive, activated only preliminarily, and automatically deactivated is itself an abstract idea and thus cannot contribute to an inventive concept. Appellee's Br. 21. Duo asserts that these limitations "are far from concrete." *Id.* In addition, Duo cites *ChargePoint, Inc. v. SemaConnect, Inc.*, 920 F.3d 759, 764 (Fed. Cir. 2019), where our court held claims directed to network-controlled charging stations for electric vehicles abstract, including a dependent claim reciting a component "that can activate or deactivate charging at the connection." We disagree.

While prior cases can be helpful in analyzing eligibility, whether particular claim limitations are abstract or, as an ordered combination, involve an inventive concept that transforms the claim into patent eligible subject matter, must be decided on a case-by-case basis in light of the particular claim limitations, patent specification, and invention at issue. 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. '903 patent col. 2 ll. 15–32. We recognized in *Ancora* that improving computer or network security can constitute "a non-abstract computer-functionality improvement if done by a specific technique that departs from earlier approaches to solve a specific computer problem." 908 F.3d at 1349. Here, as the specification itself makes clear, the claims recite an inventive concept by requiring a specific set of ordered steps that go beyond the abstract idea identified by the district court and improve upon the prior art by providing a simple method that yields higher security.

CONCLUSION

For the reasons set forth above, we reverse the district court's judgment that the asserted claims of the '903 patent are ineligible under § 101.

REVERSED

United States Court of Appeals for the Federal Circuit

COSMOKEY SOLUTIONS GMBH & CO. KG,
Plaintiff-Appellant

v.

DUO SECURITY LLC, FKA DUO SECURITY, INC.,
Defendant-Appellee

2020-2043

Appeal from the United States District Court for the District of Delaware in No. 1:18-cv-01477-CFC, Judge Colm F. Connolly.

REYNA, *Circuit Judge,* concurring.

I concur with the majority decision to reverse the district court's judgment that the '903 Patent is patent ineligible under 35 U.S.C. § 101. I conclude that, under *Alice* step one, the subject claims are directed to patent-eligible subject matter.

I do not agree, however, with the majority's analysis or its application of law. In sum, the majority skips step one of the *Alice* inquiry and bases its decision on what it claims is step two. I believe this approach is extraordinary and contrary to Supreme Court precedent. It turns the *Alice* inquiry on its head.

Our case law, as governed by Supreme Court precedent, is clear: whether a patent satisfies the subject-matter eligibility requirement of § 101 involves a two-step inquiry. *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208, 217 (2014). I find nothing in *Alice* that provides for skipping the first step or for conflating the two steps into one. Nor does the majority cite any authority that specifically permits skipping step one.

The *Alice* inquiry should be viewed as a loose filter that prevents the patenting of abstract ideas, lest free thinking itself become a form of chattel. There should be no exclusivity to abstractness under the law. Of course, preemption is a primary underlying concern, but so are the concepts of inventiveness and innovation. To this end, step one serves several important purposes, chief among them being that a patent must lay bare that which is claimed. To echo Judge Rich's declaration: "[T]he name of the game is the claim." Giles S. Rich, *Extent of Protection and Interpretation of Claims—American Perspectives*, 21 Int'l Rev. of Indus. Prop. & Copyright L. 497, 499 (1990)). In terms of *Alice*, step one is about the claim.

At step one, we examine whether the claim is directed to patent-ineligible subject matter. Among other things, this examination permits us to distinguish between claims that recite mere concepts, functions or results (abstract ideas) from those that, through claimed limitations, chart the specific means for achieving such concepts, functions or results. *Ancora Techs., Inc. v. HTC Am., Inc.*, 908 F.3d 1343, 1347 (Fed. Cir. 2018). As a result, our case law has developed specific circumstances that help guide the question of abstraction. *See id.* at 1347–48 (collecting cases). For example, generally, if a claim is directed to a specific technological solution to a technological problem, it is not directed to an abstract idea. *See Enfish, LLC v. Microsoft Corp.*, 822 F.3d 1327, 1336 (Fed. Cir. 2016).

Our precedent is clear that once a claim is deemed not directed to an abstract idea, the *Alice* inquiry ends. We do not proceed to step two. *Core Wireless Licensing S.A.R.L. v. LG Elecs., Inc.*, 880 F.3d 1356, 1361 (Fed. Cir. 2018) ("If the claims are directed to a patent-eligible concept, the claims satisfy § 101 and we need not proceed to the second step."); *see also McRO, Inc. v. Bandai Namco Games Am., Inc.*, 837 F.3d 1299, 1312 (Fed. Cir. 2016). In other words, step two does not operate independently of step one. Step two comes into play only when a claim has been found to be directed to patent-ineligible subject matter. The "directed to" examination is only in step one, and not step two.

Step two is a lifeline. The step two inquiry recognizes that the claim has been struck down as ineligible. In simplistic terms, the question becomes whether there is any reason to save the claim on the basis of whether additional elements of the claim, considered individually and as an ordered combination, transform the nature of the claim into a patent-eligible application of the abstract idea. *Content Extraction & Transmission LLC v. Wells Fargo Bank, Nat'l Ass'n*, 776 F.3d 1343, 1347 (Fed. Cir. 2014) (citing *Alice*, 573 U.S. at 217).

Step two is rendered superfluous and unworkable without step one. Without the benefit of a step-one analysis, we are hobbled at step two in reasonably determining whether *additional elements transform* the *nature of the claim* into a patent-eligible application of the abstract idea. And by skipping step one, we create a risk that claims that are *not* directed to an abstract idea might be deemed to "fail" at step two.

Employing step one, I conclude that the claims at issue are directed to patent-eligible subject matter. I agree with my colleagues that "[t]he '903 Patent claims and specification recite *a specific improvement to authentication* that increases security, prevents unauthorized access by a third party, is easily implemented, and can advantageously be

carried out with mobile devices of low complexity." Majority Op. 11-12 (emphasis added). But this is a step-one rationale. *See Enfish*, 822 F.3d at 1336 ("[T]he 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 . . . or, instead, on a process that qualifies as an 'abstract idea' for which computers are invoked merely as a tool."); *McRO*, 837 F.3d at 1314 ("It is the incorporation of the claimed rules, not the use of the computer, that improved the existing technological process . . . ." (internal quotation marks omitted)).

We should not lose sight, as my colleagues have in this case, that the "question of abstraction is whether the claim is 'directed to' the abstract idea itself." *Data Engine Techs. LLC v. Google LLC*, 906 F.3d 999, 1011 (Fed. Cir. 2018).