

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS, LLC, AND JPMORGAN CHASE BANK, N.A.,
Petitioner,

v.

DYNAPASS IP HOLDINGS LLC,
Patent Owner.

IPR2023-00425¹
Patent 6,993,658 B1

Record of Oral Hearing
Held: April 16, 2024

Before KEVIN F. TURNER, LYNNE H. BROWNE, and
JASON M. REPKO, *Administrative Patent Judges*.

¹ JPMorgan Chase Bank N.A. was joined as a party to this proceeding via Motion for Joinder in IPR2023-01331.

APPEARANCES:

ON BEHALF OF THE PETITIONER:

TIMOTHY J. MURPHY, ESQUIRE
JORDAN M. ROSSEN, ESQUIRE
ALBERT HOW-YING LIOU, ESQUIRE
Unified Patents
4445 Willard Avenue, Suite 600
Chevy Chase, MD 20815
tj@unifiedpatents.com
(650) 999-0889

ON BEHALF OF THE PATENT OWNER:

JOHN WITTENZELLNER, ESQUIRE
Williams Simons & Landis PLLC
The Littlefield Building
601 Congress Ave., Suite 600
Austin, Texas 78701
johnw@wsltrial.com
(512) 543-1373

The above-entitled matter came on for hearing on April 16, 2024,
commencing at 1:00 p.m., via video teleconference.

P R O C E E D I N G S

- - - - -

JUDGE BROWNE: Good afternoon. We're here for oral argument in IPR2023-00425, which has been joined with IPR2023-01331. I am Judge Browne, and with me are Judges Turner and Repko. Before we begin, I have a few housekeeping items. As this is a video conference, we ask that you identify yourself before speaking. And if you are referring to a demonstrative, please state the number of the slide that you are referring to. We have copies of the demonstratives. There is a court reporter in attendance.

We request that counsel remain for a few minutes after arguments are submitted in case the court reporter has questions. Each party has 45 minutes of total argument time. Please indicate how much time you would like to reserve for rebuttal after making your appearance. We are on the record and we'll begin with appearances. Who is here for the petitioner?

MR. MURPHY: For Petitioner, Unified Patents, T.J. Murphy, and Jordan Rossen.

JUDGE BROWNE: Okay. And who will be presenting, or will both of you be presenting?

MR. MURPHY: I will be presenting.

JUDGE BROWNE: Thank you. And do you know how much time you would like to reserve for rebuttal?

MR. MURPHY: I would like to reserve 20 minutes for rebuttal.

JUDGE BROWNE: Thank you. All right. And who is here for Patent Owner? I think you are on mute.

1 MR. WITTENZELLNER: Good afternoon, Your Honor. John
2 Wittenzellner for Patent Owner.

3 JUDGE BROWNE: Great. And Mr. Wittenzellner, you will be
4 presenting?

5 MR. WITTENZELLNER: Correct.

6 JUDGE BROWNE: All right. And when you begin your portion
7 of the hearing, I will ask how much time you would like to reserve for
8 rebuttal.

9 MR. WITTENZELLNER: Thank you, Your Honor.

10 JUDGE BROWNE: We will make every effort to inform you
11 when your time is nearly up, but we also ask that you keep track of your
12 time. And that is everything I have at this point. We will begin with
13 Petitioner, and you can proceed when you're ready.

14 MR. LIOU: Your Honor, could I make an announcement? I am
15 Albert Liou, also for the joint Petitioner in proceedings (INDISCERNIBLE).

16 JUDGE BROWNE: Yes. Thank you, Mr. Liou. Is anyone else
17 here?

18 MR. LIOU: No, just me.

19 JUDGE BROWNE: Just you. Great. Thank you.

20 MR. MURPHY: Okay. Yes, my apologies, Albert. I was going to
21 mention that. May it please the board, T.J. Murphy for Petitioner Unified
22 Patents. With me today is Jordan Rossen, also, with Unified Patents. I'm
23 going to go ahead and share my screen with the demonstratives. Please let
24 me know if they're not visible.

25 Although Claims 1 through 3, and 5 and 6 were challenged today,

1 I'm going to focus on the claim limitations that are actually in dispute that
2 involve Claims 1 and 5. The '658 patent is directed to the well-known
3 concepts of user authentication and security. This is a very old problem, and
4 various solutions have been implemented over the years, including time-
5 based access, as well as using multiple channels to authenticate a user. The
6 claims of the '658 patent are merely directed to the authentication of users of
7 secure systems, and more particularly, to a system through which user
8 tokens are required for user authentication and supplied through personal
9 communication devices such as mobile telephones and pagers.

10 What is alleged to be novel in the claims is setting up a password
11 using a different connection than the connection eventually used by the
12 account holder. As will be discussed, this concept was well-known, as
13 demonstrated by Kew, Sormunen, as well as Veneklas and Jonsson.
14 Ground 1 is based on the combination of Veneklas and Jonsson. As shown
15 on slide 10, there are four limitations of Claim 5 that are in dispute.
16 Veneklas operates by having a user enter a password into a computer and
17 receiving a password, also described as a random code, over a different
18 channel. The user receives over a different channel, which the user receives
19 on a pager and enters into the computer to gain access.

20 Thus, Veneklas discloses the alleged point of novelty of using a
21 different communication channel in order to authenticate a user. Jonsson
22 operates by requesting authorization, which triggers the system to send a
23 challenge code, or token, to the user's device, which Jonsson describes as a
24 conventional cellular telephone or personal communication device, as shown
25 on slide 14. This challenge code is used with the user's input pin and a

1 response code, i.e., a new password is created, which is compared against an
2 expected response code.

3 Turning to slide 12, the Petition explains that there would have
4 been multiple reasons to combine the disclosures of Veneklas and Jonsson.
5 First, Veneklas discloses a transmission of two passwords, which are
6 authentication parameters that are secret, the password in the random code.
7 The combination eliminates the transmission of two secret passcodes.
8 Instead, proceeding under Jonsson's teaching, the user enters an
9 authentication request and receives a token, i.e., challenge code. This
10 challenge code is used with a pin that is entered by the user on the user's
11 device.

12 Thus, the user's pin is not transmitted anywhere, which removes
13 the risk of being intercepted. The challenge code and the pin are used by an
14 algorithm on the device to produce a response code, i.e., a transaction-
15 specific, unique password that is then compared to an expected response
16 code to gain access. Thus, dual transmission of the password is eliminated.

17 Second, the combination prevents unauthorized access by
18 preventing SIM swapping, which was a well-known method that
19 compromised security. In particular, an unauthorized party would contact
20 the user service provider and activate a new SIM card on a different device
21 in order to receive the user's authentication token. This would not work in
22 the combined system because simply swapping out a SIM card would not be
23 enough due to the stored algorithm on the user's device, which generates the
24 expected response code disclosed by Jonsson.

25 Thus, a potential hacker would need to be in possession of the

1 actual device and not merely a similar device with a swapped SIM card.
2 Third, Veneklasе discloses the use of algorithms in the security protocol. As
3 such, it would have been obvious for a POSITA to use another algorithm
4 such as the password-generating algorithm of Jonsson in the process. The
5 modification of Veneklasе with the teachings of Jonsson would simply be
6 using a well-known technique to improve a very similar device in the same
7 exact way.

8 Patent owner alleges that the proposed modification would
9 somehow destroy the intended purpose and principle operation of
10 Veneklasе. However, this is simply not the case. The modified system
11 would still achieve Veneklasе's goals of preventing unauthorized access.

12 Turning to slide 11, Veneklasе discloses that the key to the method
13 of operation is the use of a secret password highlighted in blue, a secret
14 random number highlighted in yellow, and a secret second channel. All of
15 these are still present in the modification with Jonsson. The secret password
16 is the pin or input security number of Jonsson, the secret random number is
17 the random code sent to the user device, and the secret second channel is not
18 modified in the combination and corresponds to Element 422 in Figure 6 of
19 Veneklasе.

20 Thus, the entire principle of operation is still intact, only modified
21 to add extra security. Patent Owner also alleges that the proposed
22 combination would be open to denial service attacks because the system of
23 Veneklasе uses a password to initiate the authentication process where the
24 combination would use an authentication request. As shown on slide 13,
25 Patent Owner's own evidence confirms that a denial service attack, as they

1 were known at the time of invention, where it attempts to overwhelm a
2 server with connection requests.

3 Such an attack is not based on whether the request includes a
4 password. Indeed, Exhibit 1019, shown on the right, is a patent that was
5 filed contemporaneously with the '658 patent, which further confirms that
6 knowledge of a password is not the basis for denial-of-service attack.
7 Rather, as known in 2000, it is merely an attempt to generate enough
8 requests to prevent access. Patent Owner did not offer any evidence or any
9 alternative definition for how this would have been understood as of the
10 earliest possible priority date. Thus, the denial-of-service argument just
11 simply doesn't hold any water.

12 Turning to slide 14, Jonsson expressly discloses that the capacity
13 for performing its algorithm exists in conventional devices, i.e., devices that
14 were known in 1995. As such, a POSITA would have expected that the
15 substantially off the shelf devices and readily available components of
16 Veneklasé would have been able to perform the algorithm in Jonsson.
17 Notably, substantially off the shelf indicates that modified occasions are
18 contemplated. Accordingly, Patent Owner's allegations that the combination
19 would not work because of alleged complex algorithms needed to perform
20 Jonsson's method would not be available on the device of Veneklasé is
21 contradicted by the disclosure of both references. Turning to slide 15.

22 JUDGE REPKO: Now, before you turn to slide 15, I have a
23 question about that.

24 MR. MURPHY: Sure.

25 JUDGE REPKO: So, would the pager of Veneklasé be capable of

1 performing Jonsson's algorithm? You mentioned that the SIM swapping
2 rationale requires the algorithm to be on the device. So, can that device be a
3 pager?

4 MR. MURPHY: Device, can it be a pager? The pager is an
5 exemplary device. It's not -- I don't think the disclosure is necessarily
6 limited to a pager.

7 JUDGE REPKO: So, I mean, I guess the -- you're pointing to the
8 general capabilities, you know, you're saying any device in 1996, so you're
9 saying that device -- any device in 1996 could be a pager? Is that -- do I
10 understand that you reading that particular teaching?

11 MR. MURPHY: Well, Chelsea was in 1995. However, when we
12 are evaluating the obviousness, it is at the time of the invention, which is
13 2000, which there had been substantial advances in those five years since the
14 dot com boom, and things changed very quickly. However, yes, our
15 position, based on the disclosure of both references, is that it would be able
16 to perform the method of Jonsson.

17 JUDGE REPKO: Are you saying that either reference expressly
18 teaches that, though? I guess I'm trying to really understand your position as
19 to what the prior art teaches. Does the prior art teach a pager capable of
20 performing the algorithms of Jonsson?

21 MR. MURPHY: Jonsson itself says that the -- the capacity for
22 performing the necessary calculations exist in conventional cellular through
23 telephones and personal communication units, which we would say does
24 include pagers.

25 JUDGE REPKO: Okay. Thank you.

1 MR. MURPHY: Yes. Turning to slide 15. This is where claim
2 construction comes up, in particular the parties disagree over the meaning of
3 activates access in response to the password -- activates access to the
4 account in response to the password. However, as we discussed in the reply,
5 it really isn't necessary to consider this claim because of the combination of
6 Veneklasen and Jonsson renders this limitation obvious under either
7 interpretation. In particular, the Petition identified the disclosure of Jonsson
8 where the response code is compared to an expected response code to allow
9 access.

10 Patent Owner alleges that the words, the creation of, should be
11 injected into the claim as highlighted in yellow. Nonetheless, the
12 combination meets this limitation even under this interpretation because
13 Jonsson discloses that access is activated in response to the creation of the
14 password, at least because the challenge code and the response code are
15 unique for each transaction. Thus, old passwords would not work. That is,
16 there is no access until a challenge code is generated, which creates an
17 expected response code, i.e., password. Thus, this limitation is met even
18 under Patent Owner's interpretation.

19 So now turning to Ground 2, slide 17 shows the contested
20 limitations of Claim 5. Slide 18, which are limitations 5.3 and 5.6. Slide 18
21 shows the contested limitations of Claim 1, limitation 1.3. Because the
22 combination is not in dispute in terms of motivation to combine, I will focus
23 mostly on the disclosure of Kew.

24 Turning to slide 19, Kew operates by the user requesting access at
25 a terminal. This results in code A being sent to the user's receiver unit by

1 the security server. The user enters the user identity code into the terminal
2 where the server utilizes a one-way algorithm to generate a new password,
3 code B, based on code A and the user ID, which corresponds to an identity
4 code. At this time, the security server sends a token, code A, to the
5 receiver's unit, the user's receiver unit. The user identity code corresponds to
6 the identity code stored in EPROM on the device.

7 The device uses the same algorithm used by the server to generate
8 code C, which is then compared with code B to allow it access. The Petition
9 treats the user ID and the identity code as being one and the same because
10 they are. The user ID corresponds to the identity code and is used by the
11 security server in combination with code A to generate the new password,
12 code B. In other words, there is no new password, code B, without entering
13 the user ID because the security server would not know which algorithm to
14 use. Thus, the new password is based on the user ID and token code A.

15 This limitation does not require a physical combination of the
16 passcode and token. Rather, that is the subject of Claim 2, which requires
17 concatenation, and is not challenged in this proceeding. All that is required
18 by the claim is that the password be based on the passcode and the token.
19 Because the password, code B, cannot be generated without the user ID, the
20 password is based on the user ID.

21 JUDGE REPKO: Before you move on, I have a question about
22 this figure. So, this is Figure 2. This is the second embodiment, correct, of
23 Kew, one of two embodiments?

24 MR. MURPHY: This figure does depict the second embodiment.
25 However, the highlighted portions at the bottom relate to the first

1 embodiment.

2 JUDGE REPKO: So, why highlight only the second embodiment?
3 Why not . . . is there some place in the first embodiment you could direct me
4 to that has a similar feature? Why take out the second embodiment here?
5 Show it on that slide?

6 MR. MURPHY: We just wanted a visual representation of the first
7 embodiment, and this is the best that Kew offered.

8 JUDGE REPKO: Okay. So, really, you're not pulling features --
9 you're not looking at the entire second embodiment, your rationale focuses
10 on the first embodiment. Is that correct?

11 MR. MURPHY: That is correct. That is set forth in the Petition
12 and the reply.

13 JUDGE REPKO: Okay. Thank you.

14 MR. MURPHY: Yes. Before we move on, it's worth to note that
15 we have only recently found out, because it was not served, that Patent
16 Owner has filed amended infringement contentions in one of the
17 corresponding District Court cases, in which we are not a party, which
18 alleged that infringement of the claim passcode limitation is met by the
19 password that the user uses for login or other information that is known to
20 the user, such as the username or in termination that references or is an alias
21 to the username.

22 So, the passcode, according to Patent Owner in a District Court,
23 only has to be a reference or an alias to a username. And that's in case 2:22-
24 cv-00212, document 154-2 at page 18. Patent Owner goes even further
25 alleging infringement under the doctrine of equivalents with a session ID

1 that corresponds to the username and is used for the same purpose of
2 authenticating a user. Although this was not presented in this case because it
3 was never served, it bears consideration how expansively Patent Owner
4 deems this limitation when asserting infringement. Turning to slide 21.

5 JUDGE TURNER: Counsel?

6 MR. MURPHY: Yes.

7 JUDGE TURNER: This is Judge Turner.

8 MR. MURPHY: Yes, Judge?

9 JUDGE TURNER: I guess the question is, I understand that this
10 wasn't served, but it's not part of the responsive record we have here. Why
11 should we allow arguments, you know, based on something that, you know,
12 it's not part of the record?

13 MR. MURPHY: Judge Turner, it's a good question. The problem
14 is being that we were not a party to the District Court litigation. So, we were
15 not aware that this argument was being made at all. And this is why there
16 are mandatory disclosures in place for parties when they are taking a
17 contrary position. There are many, many District Court cases associated
18 with this proceeding. And originally, these infringement contentions were
19 under seal.

20 In fact, we don't really usually see the infringement contentions at
21 all in District Court cases. The only reason this was made public was
22 apparently because Patent Owner sought to amend their infringement
23 contentions after a claim construction ruling. But we were not aware, we
24 were not made aware of it by Patent Owner, even though we would set forth
25 that they did have a duty to disclose this contrary position. So, it just bears

1 consideration that they are taking this expansive view of this claim
2 limitation.

3 JUDGE TURNER: I guess as a follow-up, I mean, can we give
4 this any weight given, you know, that there's nothing underlying this and all
5 we have is attorney argument? And if patent owner responds, again, it will
6 probably be just simply attorney argument, you know, that has no support in
7 the record. So, I guess I wanted to make sure we express a concern here for
8 both sides. You know, we can't restrict what you say, but, you know, it may
9 have very little weight. So, any response, please do.

10 MR. MURPHY: It is unfortunate that we were not given this
11 information until this late stage of the proceeding. However, this is a public
12 record that can be taken into consideration for what it's worth. It does seem
13 to directly contradict their position here. So that's why we thought we'd
14 bring it to your attention because it does seem relevant.

15 JUDGE TURNER: Thank you.

16 MR. MURPHY: Okay. Turning to slide 21. The system of Kew
17 activates access to the account in response to the password under Patent
18 Owner's interpretation. The creation of a new password, code B, activates
19 access because, put simply, access to the account must be activated in order
20 for the new password to work. In other words, account access is activated
21 when code B is generated, i.e., when access is requested. This is just how
22 this process of Kew works. There is no access until the new password is
23 generated, and the system awaits entry of code C for comparison to code B.

24 Turning to slide 22, Kew's system is grounded in the well-known
25 concept of time-bound access. It was a fundamental principle of

1 authorization techniques in secure access to limit the period of time that
2 passwords were valid. Petitioner's expert discusses this, as well as his
3 personal experience with this concept in Exhibit 1003 at paragraph 49.
4 Now, at this time, it's important to consider on slide 9 the level of skill in the
5 art. The Petition's set present level of skill in the art is at least an undergrad
6 degree in electrical and computer science, and two or more years of
7 experience in security. Now, this level of skill has not been contested or
8 really addressed, but it provides important context to disclosure of Kew.

9 Turning to slide 24, Kew discloses time-bound access in a few
10 ways. First, Kew discloses that Code C is only displayed to the user for a
11 predetermined length of time. But a POSITA would have understood this
12 argument, or this to be a time-bound access, such that Code C was no longer
13 viable upon the expiration of this predetermined length of time. And by
14 corollary, Code B would also be time-based. In addition, Kew states that
15 the receiver can only be enabled for a predetermined amount of period of
16 time to transform Code A to generate Code C.

17 Again, this tells a POSITA that there is a shelf life to Code A and
18 the generation of Code C. Kew also discloses that the user is alerted when
19 Code A is sent to the receiver unit. Finally, Kew discloses that the security
20 server prompts the user to enter Code C at the terminal, indicating that the
21 security server is waiting and expecting the entry of Code C to compare to
22 Code B. In other words, the security server knows when Code A was sent,
23 alerts the user that Code A has been sent, and expects Code C to be input
24 while still displayed on the receiver unit. When these time-bound protocols
25 are evaluated through the eyes of the POSITA, it is clear that Kew's security

1 server deactivates the account within a predetermined amount of time after
2 activating the account.

3 Slide 25 provides one example of how Kew's time-bound
4 disclosures would be combined and operate. This example uses five minutes
5 as the disclosed predetermined amount of time. The user would enter the
6 ID, the user ID to generate Code A, which is used with the user identity code
7 to generate Code B, which is the expected response code. This begins the
8 lifetime of Code B for the predetermined five-minute period. Code A is sent
9 to the receiver by the security server at the same time. It sends an alert
10 which begins the lifetime of Code A for the predetermined period of five
11 minutes. The user is alerted by the security server to enter his identification
12 code, second identification code.

13 In other words, a request for A has been made for access. You
14 have five minutes to get this done. The clock is ticking. You have to
15 enable your receiver to transform Code A or to use Code A to be
16 transformed to Code C. Then the user must enter Code C while it is
17 displayed during that same five-minute predetermined period. If the user
18 waits, Code A expires, and Code C is no longer able to be generated by the
19 receiver. If the user waits until Code C is not displayed, the five minutes is
20 up, then Code B is expired and access denied. Allowing Code B to remain
21 active after the predetermined period expires would be contrary to the goals
22 of achieving secure access as the password could simply be written down
23 and lost.

24 Since the server knows when it is sent Code A, alerts the user that
25 Code A has been sent and then prompts the user to enter Code C, a person of

1 ordinary skill in the art would understand that the server is deactivating
2 access after a certain amount of time.

3 JUDGE REPKO: So, in your question before, you said that you
4 were relying on the first embodiment. So, this part, where you have a
5 transform to Code C, this is in the first embodiment of Kew?

6 MR. MURPHY: That's my understanding.

7 JUDGE REPKO: I know on page two of Kew, they talk about
8 Code C, a transform Code C. And in the first embodiment, it looks like
9 there's accepting the input to Code C. It's on, I guess, on page one. And
10 then on page three of Kew, we have that time based. And I guess that's on
11 lines 14 through 23 on page 3 according to Kew's pagination. So, we're
12 saying that that paragraph that talks about a predetermined time period, that
13 applies to both embodiments, or just the first one or the second one?

14 MR. MURPHY: I would say that it would apply to both
15 embodiments, but it definitely applies to the first.

16 JUDGE REPKO: Okay. Thank you.

17 MR. MURPHY: Sure.

18 JUDGE BROWNE: Also, Mr. Murphy, you have about two and a
19 half minutes before you'll be cutting into your rebuttal time.

20 MR. MURPHY: Great. Thank you for that. I will turn to -- look,
21 Patent Owner has made arguments Kew's security server does not know
22 when Code C is no longer displayed. However, looking at slide 26, Kew
23 discloses a predetermined period as well as an alert to user device. Patent
24 Owner's arguments ignore Kew's disclosure of a prompt by the security
25 server. A POSITA would understand that security server's prompt is the

1 beginning of a limited time to enter Code C.

2 If there was no time limit for Code C or Code A, Kew's password
3 would be valid indefinitely, which would, when reading Kew as a whole,
4 defeat the entire purpose of Kew's time-bound access. Turning to Limitation
5 1.2 on slide 27, the Petition maps Sormunen's disclosure, the Request
6 Message 2, shown on the right in green, for the disclosure of communication
7 from the device to the security server. Patent Owner alleges that the system
8 of Kew has no way of identifying the terminal if the request is sent by the
9 device.

10 This is simply not the case as Kew specifically contemplates
11 communication from the device to the terminal, which is shown in blue on
12 slide 28. Thus, the device, modified by Sormunen, already has transmission
13 capability, and Kew expressly discloses that the device communicates with
14 the terminal or is capable of doing so. Accordingly, the modified Kew
15 Sormunen device would communicate with the terminal as needed. For this
16 reason, Patent Owner's alleged deficiencies, one, attempt to attack Kew
17 individually instead of a combination with Sormunen, and two, are refuted
18 by the disclosure of Kew. And if there are no further questions at this time, I
19 will reserve the remaining time for rebuttal.

20 JUDGE BROWNE: Thank you, Mr. Murphy. You were pretty
21 much exactly on time, so you'll have 20 minutes for rebuttal.

22 MR. MURPHY: Okay.

23 JUDGE BROWNE: Mr. Witten, how much time would you like to
24 reserve? I'm sorry, it's Wittenzellner, correct?

25 MR. WITTENZELLNER: Correct.

1 JUDGE BROWNE: My apologies.

2 MR. WITTENZELLNER: Not the first time, no problem. I would
3 like to reserve 35 minutes of my time, Your Honor.

4 JUDGE BROWNE: I believe that's more than half of your time
5 with 45 minutes being total. So, we normally don't allow that much for a
6 rebuttal. I could say we could give you 25.

7 MR. WITTENZELLNER: I'm sorry, 35 minutes for my argument,
8 and reserving 10.

9 JUDGE BROWNE: You have 35 minutes, and you want to
10 reserve 10.

11 MR. WITTENZELLNER: Got it.

12 JUDGE BROWNE: Thank you. That makes sense. And you can
13 begin when you're ready.

14 MR. WITTENZELLNER: Thank you. Good afternoon, Your
15 Honors. On behalf of Dynapass and my firm, we appreciate the opportunity
16 to be heard today. Before I go into the '685 patent, I'd like to address Judge
17 Turner's question about the infringement contentions and correct a number
18 of misrepresentations from my counterpart. To the first point, infringement
19 contentions are not sealed.

20 These infringement contentions were sitting on the public record
21 since December 4th at the earliest. Second, Mr. Liou is currently present as
22 he identified himself as a Co-Petitioner. He was actually at the hearing in
23 Marshall on December 15th when an argument was presented regarding
24 these infringement contentions. And I find it hard to believe that counsel for
25 Unified was not aware of them given that timing, and rather than attempt to

1 provide the infringement contentions to the Board to see in its
2 demonstratives, which would have surely raised an objection, they instead
3 tried to improperly introduce them to the record during this hearing, also
4 without providing the Board with the benefit of seeing the actual contentions
5 rather than counsel's representation of what they say.

6 So, it is our position that the contentions bear no weight on this
7 proceeding, even putting aside counsel's misrepresentation of what they
8 actually say. I'll pause there to see if there aren't any questions on that issue.

9 JUDGE TURNER: Sure. This is Judge Turner. Let me -- because
10 you're raising these issues, you know, in terms of function. As a Joint
11 Petitioner, Petitioner JPMorgan Chase, per our joining of these decisions,
12 would they have the ability to bring this before us in their capacity since
13 they're not the first Petitioner?

14 MR. WITTENZELLNER: My understanding is that they are
15 essentially second fiddle, Your Honor, in the proceedings. But certainly, if
16 they thought an argument was there, there's nothing preventing them with
17 communicating with primary counsel about the issue. And they were
18 certainly aware of it because he was in the courtroom with me arguing about
19 those contentions.

20 JUDGE TURNER: And I understand that. But I guess my -- more
21 to my question is, even if the secondary Petitioner knew of the information,
22 they, under the joinder, I don't think they could necessarily bring it to our
23 attention directly. Is that not correct?

24 MR. WITTENZELLNER: I believe that's correct, Your Honor.
25 Again, that they could bring it to the attention of primary counsel to bring it

1 to your attention.

2 JUDGE TURNER: No, I just wanted to make that clear because
3 you sort of implied that, you know, that counsel was there, and they know,
4 so that would bring the inference up that, of course, that they could raise it,
5 but I don't know that they could directly. But I appreciate the distinction
6 you're raising and I'll let you get back unless other members of the panel
7 have a question.

8 MR. WITTENZELLNER: Thank you, Your Honor. The claims
9 of the '658 patent are straightforward in and of themselves as far as the
10 language goes. And I think part of that also comes from the fact that the
11 technology has become ubiquitous. I use the claim technology this morning
12 while using online banking, and I would be surprised if others in this hearing
13 have not used it recently. It's one of the challenges that I face representing
14 Dynapass is ensuring that the validity of the '658 patent is assessed as of
15 March 6, 2000, not today, through hindsight based on the claims and the
16 familiarity of everyone with the technology.

17 I would like to start today with a limitation that cuts across both
18 grounds on both independent claims, and for Your Honors, I'm going to start
19 with Patent Owner's slide 5, demonstrative slide 5. In Claim 5, the relevant
20 limitation has been marked as 5.6, and it's written in the context of the
21 authentication module, which is in the upper righthand corner. And in that
22 context, the authentication module activates access to the account, and then
23 later deactivates it after a predetermined amount of time. Claim 1 has
24 similar limitation, although it's split in the claim language.

25 There's activation of access or activating access to the user account

1 on the first secure computer network. And then the final limitation is
2 deactivating access to the user account on the first secure computer network.
3 These are important limitations. The Patentee had filed two responses to
4 nine final office actions before the examiner issued a third final office action
5 on February 7, 2005. And these limitations about activating and
6 deactivating access to the user account were added into the independent
7 claims in an RCE dated May 12, 2005, and only after those additions was
8 the '658 patent allowed.

9 Your Honors, I'm going to slide 14 of Patent Owner's
10 demonstratives. So, the question is, what does the limitation mean? Using
11 Claim 5 as an example, the plain language of the claim requires that the
12 predetermined amount of time is the time between activation and
13 deactivation of access to the account. It's the authentication module that
14 activates the access to the account in response to the password, which comes
15 into existence only after it is created by the control module. On Patent
16 Owner's slide 14, we have an annotated version of Figure 6 of the '658
17 patent, which was also in our briefing.

18 And what we've done is taken the figure and illustrated how it
19 corresponds with the claim language. In red, that box depicts the steps that
20 correspond to activation. So, the authentication module according to the
21 claim language activates access to the account in response to the password.
22 The password has to exist before activation can occur. The green box
23 corresponds to the claimed predetermined amount of time. And then the
24 blue box corresponds to the period of time after the predetermined amount
25 of time has expired. And that is why the system is then deactivating the user

1 account through the database.

2 JUDGE REPKO: So, when is the amount of time determined in
3 this Figure 6? So, you said the green box represents the predetermined
4 amount of time. When is that amount of time determined?

5 MR. WITTENZELLNER: Your Honor, it's predetermined, so it
6 has to be determined before these mechanisms are put into place. And I
7 think that's actually one of the issues that we had with some of the other
8 interpretations that would allow the length of time to vary. So, for example,
9 if -- I believe one of the arguments put forth by Petitioner was that, well, the
10 predetermined amount of time does not have to correspond to the entirety
11 between activation and deactivation. If that's the case, that amount of time
12 can actually vary, and then it's our position that it's then no longer
13 predetermined.

14 And so, to answer your question, the amount of time for the
15 predetermined amount of time has to be set by the system before these
16 processes are determined. So, for example, it could be 10 minutes, which I
17 think is a very common value that we see in practice. And so, without
18 anchors on either side of when we're evaluating whether the system or
19 account access is deactivated after a predetermined amount of time, we
20 really have no way to determine whether that claim limitation is actually
21 disclosed in the prior art or from an infringement standpoint met.

22 JUDGE REPKO: So, before step 508, it's determined?

23 MR. WITTENZELLNER: At some point before, I think really it
24 would have to be at some point before the green box. So, it would have to
25 happen at or before 512 because our understanding of the claims is that once

1 you have the password created, that timer starts running. And so, if the
2 timer starts running, you have to know, well, when should, what's the end of
3 the timer, at which point my predetermined amount of time is expired and I
4 should be deactivating access to the account.

5 JUDGE REPKO: Are there any examples that would help me
6 understand when it's determined? Are there some examples at 512 before
7 508 in the specification?

8 MR. WITTENZELLNER: I don't think it tells you exactly when
9 that time frame has to be set is perhaps something like a system variable, but
10 it has to proceed or it has to come before the time period starts running so
11 that the system actually has it predetermined as opposed to just being a
12 period of time that's assessed.

13 JUDGE REPKO: So, I mean, any time before the time period
14 starts running sounds like it simply could be calculated after 512, after 510,
15 after 508, correct? It means determined, right? Is that how you determine it
16 to calculate it?

17 MR. WITTENZELLNER: No, the predetermined period of time is
18 just the interval. So, it'd be essentially setting a variable perhaps in the
19 software, say we're going to set the predetermined timeframe as 10 minutes.
20 Then really there's, I don't see any calculation with that. What I see there is
21 calculation subsequently once that activation of the access occurs, you're
22 then comparing the running timer against the predetermined amount of time
23 to determine whether or when to later deactivate.

24 JUDGE REPKO: So, predetermined means to you not calculated,
25 it must be read from a configuration file or, you know, set by the system at

1 some point?

2 MR. WITTENZELLNER: Correct, correct.

3 JUDGE REPKO: Okay. Is there any examples of that that I could
4 look at in the specification about whether it's calculated or, I mean, like you
5 said, it's probably read from a configuration file. Does it have that as an
6 example?

7 MR. WITTENZELLNER: Your Honor, I'm not aware of any
8 instances, certainly of it being shown as being a calculation, but I can get
9 back to you on your other question about whether it's a configuration that's
10 read out.

11 JUDGE REPKO: Okay. Thank you.

12 MR. WITTENZELLNER: You're welcome.

13 JUDGE REPKO: I have no further questions on that.

14 MR. WITTENZELLNER: Thank you. And so, I think we've
15 covered the one argument about how the predetermined amount of time does
16 not have to be necessarily tied to creation. Another argument that we've
17 seen is that the predetermined amount of time does not correspond to the
18 entire time between activation and deactivation of access, and that is our
19 position would essentially either read the limitation out or render it indefinite
20 because you no longer have an anchoring point on either end of the
21 predetermined amount of time to determine whether it has expired.

22 So, with that in mind, I'm moving to slide 15 of Patent Owner's
23 demonstratives, Your Honor. I'd like to talk about Veneklase and Jonsson,
24 which is Ground 1. Petitioner presented several different readings of this
25 claim limitation in the Petition, and we explained why those disclosures

1 were wrong on pages 35 through 37 of the Patent Owner response. And I'd
2 like to -- but then in reply, Petitioner pivoted to a new position, which we
3 identified in our sur-reply. I'd actually like to switch to Petitioner's
4 demonstratives at this point, slide 16.

5 On slide 16, and today I did not hear any of those other positions,
6 so it appears that Petitioner has abandoned them in favor of this new petition
7 that came in reply, or position that came in reply. Here Petitioner is focused
8 on the predetermined window identified in Veneklase, at column 8, lines 40
9 through 49, but the issue still remains. So, according to Petitioner, the
10 predetermined amount of time, as claimed, begins when the first password is
11 received, but that is not what the claims call for. The claims call for the
12 predetermined amount of time, or activation and deactivation to occur in
13 response to the password or creation of the password. Now, under in
14 Veneklase, the first password is received before what Petitioner is
15 identifying as the token is ever created or transmitted. So even if we take
16 everything else in Petitioner's new position at face value, it does not actually
17 read on the claim language, which requires that the predetermined amount of
18 time start after creation of the password.

19 And I think we can agree that at a minimum, even if we do have --
20 even if the Board does not accept our position that the beginning of the
21 predetermined amount of time has to start with creation of the password,
22 even if we allow for having some period of time between then, and we can
23 all agree that the password under the claim language must actually exist
24 before that predetermined amount of time can start. And in Veneklase, that
25 is actually not the case, because it's saying that the predetermined window of

1 time starts upon receipt of the first password, but not necessarily generation
2 of that other password or token.

3 Your Honors, I'd like to switch back to Patent Owners'
4 demonstratives, specifically slide 21. In this, I'm going to discuss the same
5 claim limitation, but now with respect to Ground 2 and the Kew reference.
6 And here we get even further from the claim language with Kew. Petitioner
7 alleges that the predetermined amount of time corresponds to when a code is
8 displayed on Kew's receiver unit, which would be the claimed personal
9 authentication device, not the authentication module as required by the
10 claim.

11 And so, under Petitioner's grounds, it would actually be a totally
12 separate device making this determination, not the authentication module.
13 And specifically, it's that their predetermined amount of time is based simply
14 on when Kew's handheld device is displaying the code. There's nothing that
15 they've been able to point to actually stating that Kew's, what they're calling
16 the authentication module, which will be physically located somewhere else,
17 is actually activating and deactivating access to the account. And we saw
18 this during counsel's presentation. There was reliance on the facts, and this
19 is slide 26 of Petitioner's claims, reliance on there being a prompt from the
20 security server. A prompt simply means that the security server is waiting
21 for input. MS-DOS had a prompt. Unix Terminal has a prompt. That does
22 not tell us that the security server itself with the alleged authentication
23 module is actually deactivating access to the account for that password
24 within the predetermined amount of time.

25 Your Honors, I'd like to now move to slide 12 of Petitioner's

1 demonstratives, where counsel touched on motivation to combine. Our
2 understanding of the motivations to combine set forth in the Petition were
3 twofold. First, according to Petitioner, a person of ordinary skill would have
4 been motivated to combine Veneklase and Jonsson to increase the security
5 of Veneklase.

6 Second, that combination would increase the efficiency of
7 Veneklase because you now have a single transaction as opposed to two. On
8 the first point, Veneklase itself tells us that it actually introduces these two
9 transactions, a first password, which causes the second password to be
10 transmitted. That is in the invention for the particular reason of increasing
11 security. And so, removing the first password would have been counter to
12 all of the teachings of Veneklase. From the efficiency standpoint, we
13 pointed out in our response that removing Veneklase's first password
14 transmission, so going from a two-step system to a one-step system, would
15 have rendered it inoperable.

16 The response was that there would have been a first step because
17 that would have been necessary to prompt Veneklase's system to send the
18 second password. The issue there then is that we're back to two transactions.
19 We're back to two transmissions from the user's device. And so, there is no
20 efficiency gain. You have these two interactions and these two
21 transmissions that have to occur for the system to actually operate.

22 On the topic of obviousness and the understanding of a person of
23 ordinary skill in the art, Petitioner's demonstrative slide 9, they presented the
24 argument that we have not applied the person of ordinary skill in the art in
25 this case or have not identified it. I think what's missing from Petitioner's

1 slide 9 is the fact that the Board adopted Petitioner's definition. So, in our
2 preliminary response, we indicated, yes, we are going to, or we do not
3 dispute the definition for purposes of the preliminary response.

4 The Board adopted that position or that definition on page 8 of the
5 institution decision, and we applied the definition adopted by the Board. At
6 no point did we say we were applying a different definition or we disagree
7 with it. And then as slide 9 from Petitioner also shows, in sur-reply we
8 further confirm that, that we have at all points throughout the proceeding
9 been operating off the same definition as the Board and Petitioner. Your
10 Honors, I'd like to go to Patent Owner's slides or slide 18.

11 JUDGE BROWNE: Before you move on, Mr. Wittenzellner, just
12 letting you know you got about four minutes before you cut into your
13 rebuttal time.

14 MR. WITTENZELLNER: Thank you, Your Honor. During my
15 counterpart's presentation, I believe he said that the identity code and the
16 user identification code in Kew are one and the same. He needed to say that
17 because the user identification code is not actually used as part of the
18 password in Kew. The fact is that the reference uses different words for
19 different things.

20 Finally, we heard discussion about whether or not the user
21 identification code is eventually known, or sorry identity code is eventually
22 known to the user and there is a substantial discussion about in the briefing,
23 as well as expert declarations, about what it means by the fact that that code
24 is actually stored in EPROM. And counsel today confirmed that that code
25 actually is stored in EPROM. We'll just submit that the fact that it is set up

1 in that way clearly shows that the code is not known to the user. It's
2 essentially burned into the device of Kew when it's acquired. And so, the
3 claim limitation is simply not met.

4 Your Honors, that's all I have for my response unless the Board has
5 any questions.

6 JUDGE BROWNE: Not seeing any questions, I can add two
7 minutes to your rebuttal time. And, Mr. Murphy, if you would begin your
8 rebuttal when you're ready.

9 MR. WITTENZELLNER: Thank you.

10 MR. MURPHY: Thank you, Your Honor. First, I just wanted to
11 point out that the joinder Petitioner was not joined until after the reply was
12 due. So, there was really no mechanism for any of this to be brought to the
13 Board's attention, which is precisely why the rules require a party to disclose
14 positions that are contrary to what they have said in the proceeding. Getting
15 to the disclosure of Veneklas, I would like to turn to slide -- the claim
16 construction of limitation 5.6, slide 7 of Petitioner's demonstratives. The
17 actual language of the claim reads, deactivates the account within a
18 predetermined amount of time after activating the account.

19 It does not require that the entire time period between activation of
20 the account and deactivation of the account make up the predetermined
21 period of time. That would read out the terms within and after. Therefore,
22 Veneklas, which is almost identical in disclosure to the '658 patent,
23 discloses that the -- this is at column 9, lines 61 to 64. This is the only
24 support we can find for this limitation.

25 And it says Veneklas's teaching is the scope of the -- it's identical

1 to the '658 patent, and this is also listed on page 43 and 44 of the Petition.
2 Figure 5, that the user can access the system by logging in using a token in
3 step 5.16, but if the token expires in step 5.18, the system deactivates the
4 user account in the user database. That's step 5.18 that the token has an
5 expiry time that the token expires. At step 5.20, upon expiration of the token
6 and the control module deactivates the account. That's it. And that's exactly
7 how Veneklasen operates as we set forth the Petition.

8 Regarding Kew and the user ID identification code, we've been
9 through that and why the user identification code in the password is based on
10 the user identification code. I believe Patent Owner's counsel said it could
11 not be used as part of the password. That is not what's claimed. It's claimed
12 to be based on Claim 2, again, refers to concatenation and does not -- is not
13 within the scope of the challenge.

14 Finally, I would also point to Claim 1 of Kew, which is
15 summarized -- or which is put down on slide 20 of Petitioner's
16 demonstratives. It doesn't require the identity code. In fact, it says that the
17 subjecting Code A to transformation characteristic of a transformation
18 algorithm identified by the input user identification code. So, the user
19 identification code is the user ID. In some cases, it can be used to point to
20 the identity code to find the right algorithm. It's not necessary. It's broader.
21 It's a broader disclosure. And even if it was only used to point to the user ID
22 in order to find the transformation code, it still would have to be entered, and
23 therefore, the password would be based on the user ID.

24 I don't think I have any more discussion unless there are any
25 questions based on what Patent Owner's counsel has brought up. I'm happy

1 to address those. Other than that, I thank you for your time, and I will yield
2 the rest of my time.

3 JUDGE BROWNE: So, before we proceed to Patent Owner's
4 rebuttal, it looks like we have an issue here regarding this evidence that's not
5 in the record. And we would like to know if you request additional briefing
6 on this issue, and I will ask -- I'd like to ask both parties about that.

7 MR. MURPHY: Petitioner wouldn't be opposed to additional
8 briefing necessarily. However, it is a public document that the Board can
9 take judicial notice of just to look at and see exactly what it says. I don't
10 believe I mischaracterized. One, it says that. I think I quoted exactly from
11 the claim construction that was -- or the infringement contentions that were
12 set forth by the Patent Owner. I will verify that and make sure that it's
13 correct in the record, but we would not necessarily be opposed. I would like
14 to just, for clarity and for accuracy, make sure that I have exactly the right --
15 oh, sorry. I am looking at the wrong document. But I want to make sure
16 that what I said was 100 percent accurate. And so let me find --

17 JUDGE BROWNE: So, I think that if we do authorize briefing,
18 that you could clarify it at that time. I'd like to turn to Mr. Wittenzellner.
19 What are your thoughts about additional briefing on this issue?

20 MR. WITTENZELLNER: Your Honor, it's our position that the
21 additional briefing would really be unnecessary. I think the infringement
22 contentions are of very limited relevance here. And I'm not sure what it
23 would actually impact with respect to the art that's been asserted here.

24 MR. MURPHY: Your Honor, if I may, if the Board does not see
25 fit to have additional briefing, I think it is incumbent on Patent Owner at a

1 minimum to make this part of the record in accordance with their obligations
2 under the rules.

3 JUDGE BROWNE: Okay. At this point, we're going to take this
4 under advisement to consider whether we're going to authorize additional
5 briefing or not. And Mr. Wittenzellner if you would like to continue with
6 your rebuttal.

7 MR. WITTENZELLNER: Thank you, Your Honor. I really only
8 have two points. The first is I would like to respond to the question from
9 Judge Repko specifically about the predetermined amount of time being a
10 value that's looked up. And column 8 of the '658 patent describes the user
11 token server starting at the top of column 8. And then specifically in lines
12 24 through 28 of column 8, it discusses other information that can be
13 associated with the user.

14 And I'll read it for the benefit of the Board. The other
15 supplemental user data may include one or more of colon, whether an
16 account is active, the expiration time of passwords, and the frequency with
17 which tokens may be automatically distributed. I believe specifically the
18 second item, the expiration time of passwords, corresponds to a
19 predetermined amount of time as being a value that is stored beforehand
20 before those steps where the token is actually generated and the new
21 password as a result is created.

22 The second point that I would like to address is my counterpart's
23 argument with respect to Petitioner's demonstratives, slide 7, on claim
24 construction, and I believe the argument was that Patent Owner's
25 interpretation of the claims would essentially read within and after out of the

1 claim language, but that's not correct. Simply put, the within just reads that
2 deactivation occurs when the predetermined amount of time expires, not
3 afterwards. Deactivation does not occur 10 minutes after the predetermined
4 amount of time, and after is consistent with what we've been putting forth
5 the whole time. The predetermined amount of time cannot happen until the
6 account is actually activated.

7 And that's all, Your Honor.

8 JUDGE BROWNE: Thank you. I'm going to take a moment to
9 confer with my fellow panelists. Okay, I don't think we have anything else.
10 The arguments are submitted.

11 (Whereupon the above-entitled matter went off the record at 2:04
12 p.m.)

PETITIONER:

Timothy Murphy
Jordan Rossen
UNIFIED PATENTS
tj@unifiedpatents.com
jordan@unifiedpatents.com

How-Ying Liou
Vishal Khatri
Matthew Johnson
Evan Tassis
JONES DAY
aliou@jonesday.com
vkhatr@jonesday.com
mwjohnson@jonesday.com
etassis@jonesday.com

PATENT OWNER:

John Wittenzellner
Todd E. Landis
Michael J. Fagan, Jr.
Mark McCarthy
WILLIAMS SIMONS & LANDIS PLLC
johnw@wsltrial.com
tlandis@akingump.com
mfagan@wsltrial.com
mmccarthy@wsltrial.com