

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MASTERCARD INCORPORATED AND
MASTERCARD INTERNATIONAL INCORPORATED,

Petitioner,
v.

OV LOOP, INC.,

Patent Owner.

IPR2023-01289
Patent 10,032,171 B2

Record of Oral Hearing
Held: December 13, 2024

Before LYNNE H. BROWNE, JAMES A. TARTAL and
BRENT M. DOUGAL, Administrative Patent Judges.

IPR2023-01289
Patent 10,032,171 B2

APPEARANCES:

ON BEHALF OF THE PETITIONER:

ELIOT D. WILLIAMS, ESQUIRE
JENNIFER TEMVESTA, ESQUIRE
Baker Botts, LLP
700 K Street, N.W.
Washington, D.C. 20001-5692
(202) 639-7700

ON BEHALF OF THE PATENT OWNER:

SETH LINDNER, ESQUIRE
BRETT COOPER, ESQUIRE
ROBERT A. AUCHTER, ESQUIRE
BC Law Group, P.C.
200 Madison Avenue, 24th Floor
New York, New York 10016 
(212) 951-0100

The above-entitled matter came on for hearing on Friday, December 13, 2024, commencing at 1:00 p.m. ET, via video conference.

PROCEEDINGS

1 - - - - -

2 JUDGE TARTAL: Good afternoon. We are meeting for oral
3 arguments in IPR2023-01289, MasterCard, Incorporated and MasterCard
4 International, Incorporated, the Petitioner, v. OV Loop, Incorporated, the
5 Patent Owner, concerning patentability challenges of claims in U.S. patent
6 number 10,032,171 B2, which we will refer to as the '171 patent. I am
7 Judge Tartal and also appearing is Judge Browne and Judge Dougal.

8 We will begin with appearances for both parties for those who will be
9 arguing today. If anyone else is attending remotely with you today but will
10 not be speaking, please identify them as well. We'll start with appearances
11 for Petitioner.

12 MR. WILLIAMS: Thank you, Your Honor, good afternoon. This is
13 Eliot Williams for Petitioner MasterCard. I believe we have back-up
14 counsel Thomas Natsume on the public line and I will be handling the
15 presentation today.

16 JUDGE TARTAL: Yes, welcome, counsel.

17 And who do we have for Patent Owner? You may be muted, counsel
18 for Patent Owner.

19 MR. LINDNER: My apologies. The audio when Petitioner was
20 speaking just there broke up for me significantly. Was that an issue just for
21 me or was that an issue for others as well?

22 JUDGE TARTAL: I think I was able to hear him clearly. We can try
23 again and see if you have an issue again. Would you like to -- okay. Let's
24 just do the appearance for Patent Owner first and then we'll address whether
25 you're able to hear.

1 MR. LINDNER: Sure. This is Seth Lindner with BC Law Group for
2 Patent Owner OV Loop, Inc. Also attending today but not presenting is
3 Spencer Hosie with Hosie Rice, also on behalf of the Patent Owner but not
4 presenting today.

5 JUDGE TARTAL: Okay. Thank you, counsel, and we could hear
6 you clearly.

7 If counsel for Petitioner could introduce himself again and we'll just
8 confirm whether counsel for Patent Owner is having any issues hearing you,
9 that would be helpful.

10 MR. WILLIAMS: Yeah, sure, okay, Your Honor. This is Eliot
11 Williams counsel for Petitioner MasterCard. How are you hearing me?

12 JUDGE TARTAL: And Patent Owner, was that better?

13 MR. LINDNER: That was, yes.

14 JUDGE TARTAL: Okay. If there is at any point in time an issue
15 with any of the technical connections, please interrupt and let us know. That
16 would be the one interruption that we would appreciate hearing from some
17 kind of indication of.

18 We'll begin with a few introductory remarks before starting the
19 argument. We set forth the procedures for today's argument in our hearing
20 order, Paper 32 in this case. Each party has 60 minutes total time to argue
21 their case. The Petitioner will open the argument and may reserve rebuttal
22 time which may not exceed more than half of Petitioner's total argument
23 time.

24 Patent Owner will then respond to Petitioner's arguments and may
25 reserve surrebuttal time, also to not exceed more than half of Patent Owner's
26 total argument time. Please remember that your arguments should be

1 limited to only arguments previously presented in your briefs. Please make
2 it clear which challenges and claims you are addressing at all times.

3 Please refrain from interrupting opposing counsel with objections.
4 We ask that the parties instead hold any objections regarding your party's
5 arguments until it is their time to speak. To ensure the transcript of this
6 hearing is clear we ask you to identify yourself just before speaking, to
7 speak directly into the microphone, and to identify specific slide numbers,
8 numbering and figures, and any other pertinent identifying information when
9 referring to demonstratives. Also please mute yourself when not speaking.

10 If you encounter any technical difficulties, please let us know
11 immediately. Also, we note that this proceeding includes public access. Our
12 understanding is that no confidential information is at issue in today's
13 arguments. Petitioner, is that also your understanding?

14 MR. WILLIAMS: That is correct, Your Honor.

15 JUDGE TARTAL: And Patent Owner, can you also confirm that
16 you're not aware of any confidential information at issue today?

17 MR. LINDNER: Yes, I confirm, Your Honor.

18 JUDGE TARTAL: Thank you, counsel. I will maintain a clock and
19 will try to provide each party time warnings as you near the end of your
20 allotted opening argument time and near the end of any reserved rebuttal
21 time, but it would be helpful for the parties to also track their time
22 accordingly.

23 Petitioner, do you wish to reserve any rebuttal time, and if so, how
24 much out of the 60 minutes of total argument time?

25 MR. WILLIAMS: Yes, Your Honor. If you could let me know when
26 I have 10 minutes remaining, I'd like to try to reserve that for rebuttal.

1 JUDGE TARTAL: Okay, thank you, counsel. We will let you know
2 after 50 minutes or when 50 minutes is approaching. All right. You may
3 begin your arguments when ready, Petitioner.

4 MR. WILLIAMS: Okay, great. I'm going to try to share my slides as
5 well. Let me just see if this works. And if you can let me know if you see
6 those demonstratives, Your Honor?

7 JUDGE TARTAL: Your demonstratives are on the screen. We can
8 see those. We also have copies that we have access to --

9 MR. WILLIAMS: Great.

10 JUDGE TARTAL: -- on our computers.

11 MR. WILLIAMS: Great. Okay, super. Let me start my clock here
12 to keep track of myself. Okay. Thank you, Your Honor. So, the issues in
13 this case I think are technically not difficult to understand, but the payment
14 card industry does use some specialized jargon so I'm going to beg the
15 Board's indulgence for a few minutes here just to, kind of, give you an
16 overview of the card acceptance process and the terms that are, sort of, used
17 to describe that process. I think it will be helpful when we get into the actual
18 disputed issues in just a few moments.

19 With that said, what I have on this screen now, it should be page 16 of
20 the petition that shows just an overview of, kind of, the payment system.
21 This is the payment system as it has existed since at least the 1960s. This is
22 an interchange system so the way the payment works here is at the bottom of
23 the screen you'll see there's a card holder and the card holder wants to do a
24 transaction with a merchant who's labeled here as a card acceptor. And so at
25 the time of the transaction what would happen is the card holder would hand
26 the card over to the card acceptor.

1 Now starting, again, going back even pre-electronic funds transfer
2 what would happen here is, you know, the card would be embossed with a
3 card number that was called a PAN, or primary account number, and, you
4 know, historically that PAN would be captured onto a paper transaction
5 record usually using an imprinter machine where the embossed card
6 numbers would be carbon copied onto a slip of paper that would also record
7 the merchant information and the amount of the transaction.

8 Now, that slip of paper would then actually at some point be sent to
9 the acquirer, which is how these banks started to be called acquirer banks
10 because they would acquire these slips, and they would pay the merchant for
11 the slips and then they would settle the transaction with the card holder's
12 issuer who would eventually send a bill to the card.

13 The PAN that we're talking about there still exists today, as I'm sure
14 you know. And you'll see on slide 41 of our demonstratives it's just a very
15 high level picture of what's going on in that PAN. There's two pieces of
16 information that are going to be listed in the PAN. The one is the issuer
17 identification number IIN, also sometimes called the bank identification
18 number, or BIN, and those are the first few digits. The exact number has
19 changed over time but it's always been the case. The first few digits are
20 going to tell you which bank issued the credit card and then the rest of the
21 digits can give you the actual account number of the user. And there's often
22 a check digit or two at the end to just make sure that information got
23 captured correctly.

24 Now by the 1980s, we started to transition over to an electronic
25 version of this system and there we continue to maintain this PAN idea of an
26 account number and issuer number, sort of, encoded into one piece of

1 information.

2 And it continued to be embossed on the card but we also put it into a
3 magnetic stripe. And actually there were two versions of the magnetic
4 stripe, track one, track two were the two most common versions that could
5 be encoded onto the mag stripe. And that terminology of track data that
6 includes this PAN number has carried over to today and into smartcards.

7 And, in fact, I think we have slide 55. I'll show you here an excerpt of
8 one of the EMV specifications that shows you that this track two equivalent
9 data is still present and it has in it the primary account number. So, these are
10 ideas that have gone back, obviously, a very long time and those terms
11 continue to be used today.

12 Now, the other advancement that happened around this time is people
13 began to transition to smartcards. So, instead of just having a static
14 magnetic stripe encoded on the back of the card we could actually have a
15 card that could do some calculations and that have memory in them. And
16 that technology was used, as you see on slide 4, to further improve fraud
17 protections in the payment system.

18 So, on slide 4 you'll see an excerpt from a textbook from the early
19 1980s laying out this idea of a message authentication code, and it describes
20 it pretty clearly. It's essentially a cryptographically generated number using
21 an encryption algorithm, here DES. And DES at the time would have used a
22 secret key to make it work and you would use this DES algorithm and your
23 secret key to create a cryptogram over some input information. And the
24 cryptogram that came out of that process was called the message
25 authentication code.

1 That secret key could be shared by both the smartcard itself, so the
2 card holder's card had the secret key on it but the issuer also could keep a
3 copy of the secret key and therefore when the issuer got the financial
4 transaction that came across the network it could recompute that MAC using
5 that secret key and verify that the transaction information that was present to
6 the card at the time of the transaction matches what the issuer got. And as
7 described in this textbook it was known, you know, no one without the
8 secret key could generate that correct MAC and so therefore you could
9 protect the transaction from fraud. There's no one who could introduce a
10 spurious message into this network without knowing that that secret key.

11 Okay. That concept I just described is also, you know, talked about in
12 the RADU textbook, which we have at slide 60. I'll just show you that
13 quickly here. As you'll see here, it's describing in the bottom left box and
14 carrying over to the right box on the slide, just showing you what the issuer
15 then would be doing at the time of the transaction, which is receiving the
16 authorization message.

17 Here, as you see, the cryptogram has this identifier ARQC. I'll talk
18 more about that in just a minute, but that's just a MAC. It's a message
19 authentication code. And that message authentication code then, as
20 explained in RADU, gets recomputed using the information that was input
21 into the message authentication code calculation process by the card at the
22 time of the transaction.

23 JUDGE TARTAL: Counsel, can I just interrupt you briefly --

24 MR. WILLIAMS: Yeah, sure.

1 JUDGE TARTAL: -- to confirm since Patent Owner's video -- I think
2 he shut that off potentially -- Patent Owner, can you just confirm that you're
3 able to hear clearly?

4 MR. LINDNER: I am, Your Honor, and if you'd prefer me to have
5 the video on I can do that. I just didn't want to be --

6 JUDGE TARTAL: It's up to you. Sorry to interrupt. It's fine if you
7 want the video off while you're not speaking. I just wanted to confirm that
8 we didn't lose you. So, if you'd like to leave it off that's fine.

9 Sorry, Petitioner, you can proceed.

10 MR. WILLIAMS: Sure, okay. So, that idea of the message
11 authentication code and its authentication by the issuer is, again, you know,
12 well-known in several textbooks that long predate what's going on here. As
13 I indicated, as shown on slide 5 here, the idea of the message authentication
14 code gets several different names in the art. And this is an excerpt from the
15 '171 patent itself which, you know, concedes that and describes the various
16 names that that has.

17 And the various names you see listed there on the left-hand side are
18 CVC3, which is associated with MasterCard PayPass, dCVV, which is
19 associated with VISA's version of a contactless transaction. Then there is
20 the AC, TC, AAC, ARQC and those are all names describing a cryptogram
21 that can be generated in accordance with the EMV specifications. They all
22 have slightly different use cases, but they're all message authentication codes
23 and they all received these, sort of, acronyms.

24 And so, you know, unfortunately, you know, you'll see floating
25 around in both the prior art and the briefs these various terms and they're all

1 categories of this message authentication code, which is just -- essentially it's
2 a digital signature using a single shared key over some input information.

3 Okay. Now, the '171 patent does, sort of, start from this premise that
4 these are prior art systems and, you know, you see here we've got some
5 excerpts from the patent that they're showing things that I'll get to in a
6 moment, you'll see these come directly from pre-existing specifications in
7 the field. But it starts with this idea and it builds on it.

8 And the idea that Patent Owner was pursuing is, I think, reflected well
9 on slide 7, which reflects some parts of the file history. In a nutshell, what
10 the '171 patent is about is taking this idea of how smartcards are calculating
11 cryptograms to do message authentication and porting that over to a
12 cellphone, you know, keeping in mind that the cellphone does have the
13 ability to communicate with a contactless terminal and communicate using
14 near field communication just like smartcards that were existing at the time.

15 It didn't have, or generally they didn't necessarily have, secure
16 elements that were available to be used for this purpose. There are some
17 phones that did and there became business issues associated with that and so
18 that's why the payment industry folks looked to solutions that didn't require
19 any kind of secure element on the phone. And the idea that the '171
20 inventors had was to allow the phone to calculate these cryptograms but
21 instead of using this shared secret key, what the idea was instead is that a
22 server would send a temporary secret key to the phone and essentially it's a
23 key that would change for every transaction.

24 So, every transaction the phone would go off and contact the server,
25 get a new key, and it would use that key when it came time to actually do a

1 transaction. That, in a nutshell, was what the inventor thought was the
2 invention. There's sort of two problems with that from our point of view.

3 So, the first is this idea of a key that changes each time itself was not
4 new. That was already known in the art. And so from slide 8 you'll see here
5 what that idea -- that idea of a temporary cryptogram key is just what EMV
6 was calling at the time a session key. And it's essentially the same thing,
7 that there would be, sort of, a derivation key that was shared between the
8 issuer and the card, but for every transaction the card would calculate a new
9 key based on some data that changed each time.

10 And the way that was implemented in practice was something called an
11 application transaction counter, which you see here. And it's just a counter
12 that the smartcard maintains and changes every time it does a transaction
13 and it uses that new piece of information to calculate a new key, which is
14 then used to prepare the cryptogram, so that's the idea of the session key.
15 So, the idea of a session key that was, you know, temporary was not new.

16 So, what that leaves was just the idea of doing this on a cellphone and
17 getting the new key from a server. And as we'll talk about now in great
18 detail, as shown in slide 9, that idea was also in the prior art. And, in fact,
19 both MasterCard and VISA filed patents on the same day for this idea, and
20 that's the Collinge and Fiske patents.

21 The Collinge patents is, sort of, shown on the left. As you'll see there,
22 there's in the blue box there's your cellphone. It's got the data it's going to
23 need to calculate a cryptogram when it communicates with the point of sale
24 terminal, which is shown to the right. And it gets that data from a server
25 shown at the bottom of the screen.

1 Fiske works very similarly except Fiske uses the more traditional
2 EMV session key language that I talked about earlier and just makes clear
3 that a session key would be calculated by a server and sent to the phone for
4 each transaction.

5 Okay. So, that is my overview. Now, let me just point out, sort of,
6 one, sort of, overarching issue I think that comes out in the papers is that it
7 seems like Patent Owner's main --

8 MR. LINDNER: Counsel -- Eliot, I apologize for interrupting, but
9 I've had a couple of audio issues during that intro part there and it only lasts
10 for about five seconds each time but everything does go silent for me for a
11 moment. So, Your Honor, would it be okay -- I know there's a backup audio
12 line. I'm wondering if maybe that would be better. It seems like the video
13 comes through okay, but maybe it would be better for me to connect -- to
14 dial in through the telephone versus relying on the Webex audio?

15 JUDGE TARTAL: That would be fine with us. Would you -- we can
16 hear very clearly and it would be helpful to see you during your
17 presentation, so we can pause for a moment. Would it be possible for you to
18 try to establish an audio line in addition to maintaining your video
19 connection?

20 MR. LINDNER: Yeah, I would keep the video on.

21 JUDGE TARTAL: Right, okay.

22 MR. LINDNER: I think when I speak we'll have to see which way
23 works better. I don't want to get two audio streams coming through at the
24 same time --

25 JUDGE TARTAL: Right.

1 MR. LINDNER: -- but I think if I mute the Webex and I speak to my
2 phone I think it would work okay that way.

3 JUDGE TARTAL: Do you have the information for the audio line?

4 MR. LINDNER: I do, yes.

5 JUDGE TARTAL: Okay. We'll just pause for a brief moment here
6 and everyone should stay online and let us know if you have the audio
7 connection through the phone.

8 MR. LINDNER: Okay, thank you.

9 JUDGE TARTAL: Counsel, I'm sorry. It would be helpful if you just
10 stayed on the record for the time being just so that we have -- this should
11 only be a brief pause.

12 MR. WILLIAMS: While we're waiting, Your Honor, could you just
13 let me know how much time you have recorded there?

14 JUDGE TARTAL: Sure. I have you as having used, I believe, about
15 12 and a half minutes.

16 MR. LINDNER: Okay. I'm seeing now that I'm connected to the
17 meeting via audio.

18 JUDGE TARTAL: And we can hear you. We've lost your -- I
19 believe we've lost your video feed for the time being.

20 MR. WILLIAMS: I'm seeing it his video, Your Honor.

21 JUDGE TARTAL: Yeah, maybe it's just on the screen.

22 MR. LINDNER: Okay. Can you see my video now?

23 JUDGE TARTAL: I can also, yes. Thank you.

24 Petitioner, do you want to say something?

25 MR. WILLIAMS: Yeah. Yes. Are you able to hear me now? Is this
26 any better or same?

1 JUDGE TARTAL: For Patent Owner --

2 MR. LINDNER: Yeah. No. It sounds fine, just a little bit low and
3 staticky but no problem as far as hearing.

4 JUDGE TARTAL: Okay, great.

5 Counsel for Petitioner, you can proceed, and as I said I believe I have
6 you having used about 12 1/2 minutes.

7 And for Patent Owner, please interrupt again if there's an issue with
8 the audio.

9 Petitioner, you can proceed.

10 MR. WILLIAMS: Okay, thank you, Your Honor. All right. My
11 back-up counsel said I might have misspoken a moment ago when I said that
12 the card would calculate a key each time. It's just I guess I should back up
13 and make that clear.

14 And so the way this was working for EMV for the typical smartcard
15 transaction is the card would calculate a session key for each transaction.
16 When we moved to the idea that's in Collinge and Fiske here, that session
17 key would be calculated off the card. It would be calculated in the, you
18 know, in the cloud by the server and that key would be sent to the card and
19 then the card would just hold the key until it was ready to do the next
20 transaction.

21 So with that said, let me now, sort of, flip over to what I think the key
22 disputed issues are. And some of them in the main have to do with this issue
23 of how much of this background knowledge would a person of skill in the
24 art brought to bear when reading the Collinge and Fiske disclosures. And,
25 you know, that is an important legal issue in the case.

1 And so as we show on slide, whoops, sorry, as we show on slide 11,
2 we've got some case law here from on this case from a prior PTAB decision.
3 And we will turn to the Federal Circuit view of this in a second, but it's, sort
4 of, well-established now that, you know, when reading the prior art it is
5 appropriate to consider the background knowledge available to the person of
6 skill in the art, including specifications that were, sort of, important for
7 commercial and implementation purposes. And, you know, in our view
8 that's exactly what is going on here.

9 If we turn to slide 12 you'll see a couple of the Federal Circuit's cases
10 that address this issue pointing out, consistent with the Supreme Court, you
11 know, case law that what has to happen when doing an obviousness analysis
12 or any analysis of prior art is that that art be read in the context of taking into
13 account the background knowledge that a person of ordinary skill in the art
14 would have in reading the references.

15 And so in this case it's clear, including from the patent itself, that the
16 person of ordinary skill in the art, this is slide 13, that the person of ordinary
17 skill in the art would have been familiar with these payment specifications,
18 including both MasterCard PayPass and EMV. And MasterCard PayPass
19 we can talk more about this if the Board has questions, but essentially this is
20 just an implementation of the EMV. It's MasterCard's approach to doing
21 EMV on these types of smartcards.

22 And then the idea of the Collinge patent is to take that PayPass
23 magstripe specification and apply it to this application running on a phone
24 and doing it exactly in that way. And so that's why there are many
25 references in Collinge to PayPass. There's many references in Fiske to

1 EMV. Both of them are describing using these ideas to implement this
2 standardized payment system or, you know, payment transaction.

3 And so because of that it's important that the person of skill in the art,
4 you know, be familiar with EMV and PayPass when reading the references.
5 And again, the same is true of the '171 patent itself, which makes clear that,
6 you know, the details of interrogation, which is one of the claim elements,
7 are found in the specifications, the exact ones that we put in evidence for the
8 Board.

9 JUDGE DOUGAL: Counsel, this is Judge Dougal. So with, for
10 example, the EMV documents, there are I believe 11 exhibits that you put in
11 that you define as the EMV, and it's something like 2,000 plus pages. You
12 know, and you're looking at particulars of this implementation, so I guess
13 explain to me why familiarity with the fact these exist and maybe some of
14 the general procedures behind them and looking at particular pages and
15 specific procedures, you know, on a document that spans 2,000, at least
16 2,000 plus pages, why would someone, you know, with two years out of
17 school have intimate familiarity with this level of detail?

18 MR. WILLIAMS: Well, I mean, they would perhaps not have
19 intimate familiarity with every page and that's not what we're contending,
20 but they would have intimate familiarity with the ideas that I just articulated
21 as background knowledge, right? That these smartcards exist, that they do
22 message authentication code computations. That's the entire point of the
23 smartcard, right?

24 So, we're not necessarily saying you have to know every bit and byte
25 and exactly how these things get formatted, right? The point is that when
26 these patent applications like Collinge and Fiske talk about, for instance,

1 authenticating the cryptogram, right, they say you authenticate the
2 cryptogram using standard methods. The art doesn't explain to you that that
3 means that you calculate a message authentication code using the session
4 key because those ideas are so fundamental, right, that every person reading
5 this patent or every person from this patent is meant, you know, is meant to
6 be reading the patent, every one of those people are going to know that
7 information. They're going to know that's what a session -- they're going to
8 know what a session key is. They're going to know exactly how it's used to
9 calculate a cryptogram. They're going to know that the issuer is going to use
10 that exact same process to authenticate the cryptogram. That's the point of
11 us citing these documents, right?

12 And so, you know, we point to exactly -- in the briefs we point exactly
13 where on those documents these ideas are found, but those are the
14 fundamental ideas of payment systems that have been the fundamental ideas
15 of payment systems, you know, since the advent of smartcards starting in the
16 1970s.

17 Just to, sort of, drive that point home that, you know, EMV is
18 important, you know, it's cited 47 times in the '171 patent, right, or PayPass I
19 guess I should say, which is Mastercard's implementation of the EMV.
20 Forty-seven times the '171 patent tells you that, hey, what we're doing here
21 is a PayPass transaction, so it stands to reason that you would probably want
22 to know something about what the PayPass transaction -- how it works, what
23 it does. And you would have consulted the PayPass step to find that out.
24 That's the point of, you know, that we're making in the papers, I think.

25 And this is not a subtle point. As you can see on slide 15 if we start
26 here, what was going on in the '171 patent is literal copying of the PayPass

1 specification, right? There's really no argument that that's not what's going
2 on here. We compared sections of the '171 patent for the PayPass magstripe
3 specification for you here starting on slide 15. The same thing is true on
4 slide 16 and it goes on. We have several. I'm not going to go through all of
5 them here, but in literally every single hexadecimal byte that shows up in the
6 PayPass magstripe specification as an example transaction shows up in the
7 '171 patent.

8 So, it's clear that what was going on here is the Patent Owner was
9 taking the PayPass magstripe specification and saying let's just do this thing
10 exactly as it is on a card instead of taking -- but instead of doing it on a card
11 we're going to do it on a phone and supply, you know, a one-time use key to
12 calculate this CVC cryptogram from the server, right? And so, it's important
13 then to understand the patent that you know how the PayPass transaction
14 works, what it did, and, you know, what is the advance that they're making.
15 It's the same advance that MasterCard itself made in the Collinge patent that
16 was filed, you know, earlier than the '171 patent's priority date.

17 JUDGE TARTAL: Counsel, this is Judge Tartal, and I don't
18 necessarily have a specific question but just for context in terms of your
19 arguments, it would be helpful to have you, where it's relevant to your
20 argument --

21 MR. WILLIAMS: Sure.

22 JUDGE TARTAL: -- differentiate between Collinge and sorry, I'm
23 blanking on the second primary reference -- Fiske. And I know in the
24 institution decision, for example, on Fiske there was an issue over
25 Petitioner's assertion that this could be incorporated by reference, all of these
26 standards, and we had, kind of, addressed that in the institution decision

1 saying that it wasn't an incorporation by reference because it lacked the
2 necessary terminology to do so. And it seemed like there was somewhat of a
3 switch of argument in the reply that it went from incorporation by reference
4 to this idea of background knowledge.

5 In broader context I think our concern is there's a difference between
6 using a reference that isn't relied upon in the petition to fill necessary
7 disclosure and to show how the asserted art meets a claim limitation as
8 opposed to using references that weren't relied upon as background, general
9 background knowledge. So, you know, clearly, there are instances in which
10 the knowledge of a person of ordinary skill in the art is relevant to
11 understanding the references being asserted themselves. That's distinct from
12 relying on background knowledge to fill a missing limitation.

13 So, I guess my question is, can you in your arguments going forward
14 differentiate between what is being relied on in Collinge versus what's being
15 relied on in the grounds based on Fiske? Is there a material difference in
16 terms of what you're contending would have been known to a person of
17 ordinary skill in the art, particularly in the context of any missing limitations
18 from the reference itself being asserted?

19 And not to overburden you, but to the extent you have any comments
20 on how the Federal Circuit views it, that would be helpful to understand as
21 well. And in that, I'm referring to how the case law views a difference
22 between using an unidentified reference to fill a missing limitation versus
23 using, you know, an unidentified reference, and by unidentified, I mean not
24 relied upon specifically in the ground, just to fill in a better understanding of
25 what a person of ordinary skill in the art would have known from the
26 reference itself.

1 MR. WILLIAMS: Yeah, okay. I'm going to get to the claim. I'm
2 going to get to all those particular disputes, so I think it would be easiest to
3 do that in the context of those particular disputes.

4 In general, my comment in response to that would be, you know, the
5 petition articulates both anticipation and obviousness and we think the
6 references do both. We concede, because we don't argue this in reply, that
7 Fiske does not literally incorporate the EMV specifications, so that's true.

8 We do continue to argue, as we did in the petition, that, you know, it's
9 clear that the point of Fiske is to implement an EMV transaction with no
10 modifications to the infrastructure and, you know, that would be important
11 to understanding how Fiske works because Fiske tells you here I'm doing an
12 EMV transaction. I don't want you to have to make any changes to the
13 infrastructure, meaning the point of sale terminal that's sitting there ready to
14 do an EMV transaction should be able to do the transaction using a phone
15 implementing my idea, right? And the same is true in Collinge, which
16 makes clear it's meant to implement a PayPass transaction without changing
17 the payment infrastructure.

18 So, I will point to where we're using EMV in particular to supply
19 some details to explain, like, when Collinge talks about, you know, standard
20 authentication process he doesn't say I literally will recompute the message
21 authentication code at the issuer, but that's the kind of thing that we're
22 pointing to the background knowledge for to understand that that's what he
23 means and everyone of skill in the art reading Collinge would know that's
24 what he means. That's how we're using the reference. It's not to supply a
25 missing limitation. It's to explain how he's talking, right?

1 He's talking -- he's saying just do a standard authentication. Everyone
2 knows what this is. I don't need to explain to you how to do that. That's the
3 kind of thing that you would read directly out of -- know from the prior art
4 and not just EMV but the textbook I just showed you. So, but I'll get to all
5 that and just one second.

6 I should just pause since you've raised incorporation by reference just
7 to mention an issue with respect to the Collinge provisionals because we do
8 rely on the Collinge provisional for certain disclosures, and they're shown on
9 slide 30. That's because the Collinge publication itself explicitly
10 incorporates by reference the Collinge provisional and the case law makes
11 clear that, you know, the language used here to incorporate that provisional
12 is more than sufficient to make the provisional now part of the Collinge
13 disclosure and which we can rely on.

14 But let me move to the disputed issues then. So, Claim 1 is shown
15 here on slide 33. Now, this is a long claim. It does seem intentionally
16 obtuse, but with the possible exception of element 1E3, which we'll talk
17 about, this is really just reciting textbook contactless transaction steps. The
18 differences are that the MAC is calculated using the session key that comes
19 from a server rather than on the device, right? That's the only change. The
20 only thing that is even potentially new here is that. But again, that new
21 feature is the entire point of both Collinge and Fiske, right, both the
22 MasterCard and the VISA patents.

23 On that 1.E3 I'll mention here, has to do with when the phone sends
24 the authentication data over to the point of sale terminal. There is this
25 ambiguity in the claim, which we point out in the petition, as to whether the
26 response coming from the phone has to include both the cryptogram and the

1 account identifier or whether you could send two responses that collectively
2 have that information, as we you pointed out the petition. Either or it doesn't
3 matter because, well, I mean, Fiske teaches both directly and Collinge would
4 be obvious to do it either way. One way is the VISA way. One way is the
5 MasterCard way. So Collinge written on the MasterCard way obviously
6 doesn't include both the cryptogram and the PAN in the response. It sends
7 that over two separate command responses whereas VISA does it in one
8 command response.

9 So this is what this is, you know -- what's going on here is he's
10 claiming it. You know, we think the way this is claimed is the VISA way
11 where you do it in one response. That's the most logical reading of that, but
12 even if that were true it would be obvious to have Collinge do it the VISA
13 way because then you could have this Collinge technology be used for VISA
14 transaction. So, it's not -- there's no rocket science here. There's nothing
15 inventive about them.

16 Okay. Let me get into the dispute on request. So, you know,
17 essentially, as we argue in the petition, the gist, this is at Petitioner page 46,
18 we say it would have been obvious to implement Collinge and, you know,
19 and there are places in the petition where we do this. And so you can see
20 them where we say the obvious. This is really, kind of, trying to address
21 your question, Judge Tartal in particular.

22 We have places where we say it would be obvious to implement
23 Collinge in this particular manner because this is the standard way of doing
24 things in EMV land and it would've been predictable and that it would
25 ensure that your system is compatible with the EMV infrastructure. So, we

1 do try to point those particular things out but let me start with the first
2 dispute which is request that we see in slide 34.

3 We show that in Collinge what happens is that the phone makes a
4 request to the server. The phone is in the left box, sort of, left middle box
5 and it makes a request check in that blue outlined area and then there's a
6 yellow outline blocks inside of it that shows the actual request going to the
7 server for your next set of data. And, you know, there's a dispute about
8 whether this is done via a push or a pull request or is it clear from Collinge
9 whether, you know, which way this is happening. Slide 35 shows that at
10 least the claims of Collinge make clear that these are pull requests that are,
11 sort of, initiated by the phone. They're not coming -- it's not just the server
12 pinging the phone with, hey, here's some new keys if you -- here's a new key
13 if you want it. This is a request that's actually made by the phone.

14 In the petition we point that out. We say at page 42 of the petition for
15 this element that, "a person of skill in the art would have found it obvious to
16 configure Collinge's application to make a request either together with
17 transmitting a CAP token or separately." And then we go on to explain the
18 CAP token business.

19 So, the way the Collinge actually does this is it authenticates to the
20 server using this cap token saying, hey, this is, you know, this is my phone.
21 Here's the account information. I'm who I say I am. Please send me a key.
22 If that CAP token is validated then the key gets sent. Okay. So, you know,
23 Patent Owner seems to argue that, well, that's not a request. It's just a CAP
24 token verification.

25 Our point is that, well, by doing that you are making the request. It's
26 just that the request starts with a CAP token but it's clear that the reason

1 you're sending the CAP token is to get the data. So, it's still in our view a
2 request.

3 I don't have really much more to say about this request element. I'm
4 going to go to the associated with dispute next. This is on slide 39. Okay.

5 Here the issue is that the session key, the cryptogram that's going to be
6 used to calculate the MAC -- sorry, the key that's going to be used to
7 calculate the MAC has to be associated with an account. This argument
8 based as we saw it in the Patent Owner response was essentially premised on
9 the argument that the key is only associated with the account if the account
10 number could be recovered from the key. It seems like that argument is
11 being abandoned now by Patent Owner, but in any event, let me just go on to
12 show how, in fact, Collinge's key is associated with the account.

13 So in Collinge, this session key is called KSun, or KSun. I may
14 sometimes use that terminology. And Collinge tells you how that KSun is
15 associated with the account. First, it's generated in response to this request
16 we just talked about so that's, you know, that's one way to meet the claim
17 element. The second is that based on an application-specific counter, this
18 ATC we talked about, that is specific to the account, right, the count is
19 maintaining a counter of how many times it's used -- it's done a transaction
20 and so that is tied to the account.

21 But then third and perhaps the most important is that the key itself is
22 computed based on the actual account number, and so you see that at the
23 bottom of slide 40 where this derivation key called KDun is calculated based
24 on the PAN which is, you know, we just talked about the account number.
25 The PAN then becomes this thing that they call Y. So, Y is essentially the
26 PAN. And then as you see at the bottom of the slide, a new key is created

1 using a DES algorithm so you actually calculate a cryptogram itself and that
2 becomes the key.

3 So the DES key, the KDun, uses the PAN as an input and then that
4 KDun is the key that's actually used to calculate KSun. Okay? So, that's
5 how in our view you get that element satisfied in Collinge. Okay?

6 Moving on to couple of claim elements that are shown here on slide
7 44, so this has to do with, you know, whether the responses that get sent
8 back are APDUs. So, slide 44 shows, as explained in the petition, you
9 know, we argue that this would be obvious, right, because Collinge --
10 although Collinge talks about responses going back and forth he doesn't say
11 they're APDUs. The point is, APDUs is how everyone of ordinary skill in
12 the art knows that smartcards communicate via APDUs. That's just how
13 they work.

14 And that's confirmed as you see on slide 46. On the left side there you
15 see the excerpt from the RADU textbook. This is just a very basic payment
16 industry textbook literally, literally a textbook knowledge that anyone of
17 ordinary skill in the art would have, which explains, you know, hey, how do
18 smartcards do these commands and responses? They do them with APDUs.
19 That's just the thing that we call them. So, there's nothing inventive about
20 making these responses in ADPU. Although Collinge doesn't necessarily
21 use that word our point is here is that everyone would understand that is
22 what he's talking about.

23 And, in fact, trying to do a smartcard transaction without APDUs
24 would make it not comply, you know, with the EMV transaction. You'd
25 have to invent a whole new set of payment infrastructure in order to accept
26 your card.

1 Okay. Let me move on to the next element which has to do with
2 cryptogram generation, which is, I think, slide 48. Okay. I'm not -- you
3 know, it might be easier to respond to rebuttal to what Patent Owner's
4 argument is here but just to be clear, Collinge explicitly discloses how the
5 cryptogram is generated. You'll see here it's generated using this KSun,
6 right, and so T is the cryptogram. It will -- well, T is what is going to
7 become the cryptogram and in Collinge it's called CVC3 track one or two.
8 And that's, again, that's just the PayPass terminology for a cryptogram,
9 CVC3.

10 So, he explains exactly how it how it works. So, here he doesn't say
11 that when you calculate that cryptogram and send it back it doesn't include
12 the secret key that was used to generate the cryptogram, as we point out in
13 the petition. Of course, everyone would know that's how you calculate
14 cryptograms. You don't -- once you calculate a cryptogram you would not
15 send the secret key along. That would defeat the whole point of the
16 cryptogram as we talked about at the outset.

17 The whole point of the MAC is so that someone without the secret
18 key can't inject a spurious message. So, if you were to make your secret key
19 available every time you did a transaction you would defeat the entire
20 purpose of the cryptogram generation. But in any event, it's also the case
21 that when you do a DES cryptogram that, you know, it's the output does not
22 include the key and so we have an example of that in the petition from the
23 Rada paper, that's Exhibit 1039 showing an actual calculation of how you
24 would do DES. It shows the key, which is on the left side here and then it
25 shows what the output of the cryptogram is, which is on the right side. And
26 as you will see by inspection, the key is not in the cryptogram.

1 Okay. Moving on into the dispute about whether the ADPU includes
2 both the cryptogram and the account. And this is the dispute having to do
3 with this claim construction issue. I've pointed out that the claim is written
4 in this somewhat ambiguous way. Is it claiming the VISA way where you
5 put both of those things together in one ADPU response or the MasterCard
6 way where you split it up? And we argue in the petition quite explicitly why
7 it would have been obvious to implement Collinge in the VISA EMV way
8 because then you could use that same technology to do essentially a VISA
9 transaction. So, there we were explicit and relying on an obviousness
10 analysis and we explained why Collinge would have turned to VISA to, you
11 know, the VISA approach to do that.

12 Okay. Let me move on next to some of the dependent claims then.
13 So, okay, by the way, that does end Claim 1. And so you've seen
14 everywhere where there's any potential, you know, an element that might be
15 missing in Collinge and, in our view, none of those elements are missing.
16 It's just that the way Collinge talks about them is using the language that a
17 person of skill in the art, you know, would have understood. So, there's
18 nothing that we think actually is missing with the possible exception of that
19 one claim element that if interpreted, you know, to mean the VISA approach
20 then, you know, you would have to make a modification to Collinge.

21 Okay. Turning to slide 57, I'll talk about Claim 10, for a moment.
22 Here this has to do with what the remote computer is doing so we've mapped
23 in the petition all the elements of Claim 1 and Claim 10 and where those
24 things are performed. They're all performed in that bottom blue box of
25 Collinge and so this is, in our view, the remote computer system. And, you
26 know, as we point out in reply, these things are connected. There's a

1 connection between them so they're clearly working together as a system.
2 That, in our view, is sufficient to satisfy this claim.

3 The other thing that's potentially here, again not explicitly stated in
4 Collinge, has to do with the way that that cryptogram is actually
5 authenticated at the user, at the issuer. He says, and we're showing it here on
6 slide 60, what Collinge actually says is that, you know, "How you would
7 validate the CVC3 will be apparent to persons having skill in the relevant
8 art." And so, again, here's an example where we point to things that were
9 well-known in the art, like, how you do issuer authentication of a
10 cryptogram, shown in the Radu textbook.

11 Okay. Let me just move on in the interest of time to Claim 8. So,
12 Claim 8, essentially what's going on in Claim 8 is it's talking about the
13 mirror image of element 1.A of the claim. So, in 1.A of the claim what's
14 happening is the phone is reaching out to the server for the next key, right?

15 Claim 8 just describes what the server does when that happens, which
16 is it prepares a key and then when it gets the request it sends the key with the
17 account identifier to the mobile device that's making the request. So, it's
18 essentially just a mirror image of that aspect of Claim 1.A, which Claim 1.A
19 is obviously addressed in our Claim 1 analysis where we point out that
20 Collinge discloses, "Payment credentials corresponding to the payment
21 account may be stored in this remote SE," which is the secure element that's
22 in the cloud on that server for provisioning to the mobile device. And we
23 point out, you know, we cite, you know -- and the evidence we cite there
24 shows various things from Collinge that teach that, including the fact that in
25 Collinge the payment credentials would include a PAN, right?

1 So, the point is Collinge, you know, perhaps Collinge doesn't
2 explicitly say that every time I respond to the phone with a key I send the
3 account number. What it says is I send the credentials and other places in
4 Collinge the credentials are explained to include the PAN, including at
5 paragraph 10 of Collinge, which is cited at page 26 of the petition.

6 And then again on paragraph 61 you'll see paragraph 9 of Collinge,
7 which talks about, you know, needing to receive all necessary payment
8 credentials. And here, again, this is where we may be relying to some extent
9 on the knowledge of a person of skill in the art that the necessary payment
10 credentials would include the PAN because when you go to make a payment
11 you have to have the account number, right ? The whole system would fail
12 if you didn't have an account number in the actual message that's getting
13 conveyed to the point of sale system because you don't know what account
14 not to debit and what account is trying to make this payment.

15 Okay. There are some arguments about Claim 4 and some of the
16 some of the related claims shown here on slide 63 that, you know, various
17 aspects of what's described in Claim 1 have to be done in compliance with
18 the card specification. You know, here Collinge is specific that this is a
19 PayPass transaction so that is more than sufficient to satisfy that.

20 Okay. In terms of Claim 6, which talks about use of triple DES, or
21 3DES, you know, that's well-known, but it's also shown here on slide 64. I
22 mean, Collinge basically says use triple 3DES.

23 And then lastly with respect to Collinge talking about Claim 16, so
24 Claim 16 has to do with the issuer master key. And as we've previously
25 shown, we've talked about this on slide 40, that when Collinge's server
26 calculates the KSun it does it starting at the bottom here with this KDun,

1 which is based on this thing called IMK, which is the issuer master key. So,
2 there's an issue of master key that's used to generate the KDun for the
3 payment card and then KDun is used to generate the particular KSun, the
4 temporary key based on the transaction counter.

5 So with that, Your Honor, I've, sort of, finished my presentation on
6 Collinge and I'm going to turn now to Fiske.

7 JUDGE TARTAL: Thank you, counsel, and I have you at about 42
8 minutes and so --

9 MR. WILLIAMS: Okay, super. I think Fiske is much more
10 straightforward in any event because, as I indicated, that potential ambiguity
11 in the claim about whether you do it the VISA way or the MasterCard way is
12 eliminated in Fiske, which is a VISA patent. So, Fiske particularly, you
13 know, talks about doing these transactions with both the PAN and the
14 cryptogram at the same time in a single transaction. So, it's -- if anything it's
15 just a cleaner version of the Collinge argument.

16 So, just in the interest of time I'll start at slide 79 real quick. So, there
17 was an argument in the Patent Owner response that somehow Fiske is not
18 compatible with a VISA transaction. Of course, this is a VISA patent and it
19 specifically talks about doing an EMV transaction, so obviously what's
20 being discussed here is an EMV VISA transaction. That should be clear on
21 the face of Fiske.

22 Again, Patent Owner makes some of the same arguments that it did
23 about the key being, you know -- it not being clear from Fiske that the key
24 itself is not included in the cryptogram that's calculated. But again, you
25 know, for all the same reasons everyone of skill in the art knows you don't

1 send the key with the cryptogram. It would defeat the whole purpose of the
2 cryptogram.

3 Again, with respect to APDUs, again here, you know, I believe Fiske
4 doesn't use the word ADPU to talk about communicating between the card
5 and the point of sale terminal, but again, you know, everyone knows that
6 that's exactly how these transactions are done. They're done via ADPU so,
7 again, you know, here what we're relying on is just the knowledge of a
8 person of skill in the art of how smartcards work. They know that they
9 communicate via ADPU. That's just a basic principle of operation of these
10 things and so there's nothing inventive about sending these things as
11 APDUs.

12 Okay. Let me move to -- and, you know, for the most part those are
13 the arguments that they make with respect to Claim 1 of Fiske. So, let me
14 move to the dependent claims starting with Claim 8. And again, with
15 respect to Claim 8, this is, as we talked about with Collinge, Claim 8 is
16 really just the mirror image of Claim 1 where you are going to prepare the
17 key at the issuer or the remote secure element in the server and you're going
18 to send that key to the phone every time it needs a new one.

19 You know, Collinge talks about that expressly. This is slide 68. Let
20 me turn back to that. Yeah, okay. So, Collinge talks about how, you know,
21 these payment applications are provisioned. The card needs to have all the
22 information to conduct a transaction and that is provisioned from the server,
23 and then Collinge makes -- sorry, this is Fiske -- and then Fiske makes clear
24 that when the transaction is -- when the device is being used to make a
25 transaction the device is going to send all the records that are identified in
26 the, this is called the AFL in the card.

1 It's basically a list of things that you have to include when you're
2 communicating with a terminal. And one of those things Collinge makes
3 clear is the print to PAN. So, you know, we know that the payment
4 application, the data it needs is the PAN and the one-time use key and that
5 that is provided by the issuer.

6 Okay. I'll move to Claim 10. So, Claim 10, what Collinge -- what
7 Fiske, I'm sorry, what Fiske talks about is shown on slide 71. Again, Claim
8 10 is, sort of, the authorization side going out at the issuer once the
9 transaction is going on. What Fiske says is, "The issuer examines the
10 ARQC to make a decision on whether to authorize a transaction."

11 You know, he doesn't say that you recompute the ARQC using the
12 inputs but, you know, our point, you know, the point we make in the papers
13 is that, yes, he doesn't say that because everyone that's skilled in the art
14 already knows that. That's the RADU textbook which everyone knew for,
15 you know, since smartcards were invented is the whole point of the
16 smartcard. It's doing the cryptogram and then the issuer can recompute the
17 cryptogram to authorize the transaction.

18 So, when a person of ordinary skill in the art reads that the issuer
19 examines the ARQC, what they understand that means is they look at the
20 ARQC and then they recalculate it to decide whether to authorize the
21 transaction. You know, do they do they match or not? And if they do then
22 you can authorize the transaction. If they don't then you've got some
23 spurious message and you would reject it.

24 Okay. Claim 11 talks about the unpredictable number. So, as we
25 point out in the petition, you know, what Fiske is talking about is
26 implementing an EMV transaction as we point out here at slide 73. You

1 know, a person of skill in the art would know that the cryptogram, the MAC
2 that's going on in an EMV transaction, is going to be based on an
3 unpredictable number from the terminal. That's shown here on the left side
4 of the screen.

5 This is not a -- again, this is not a, sort of, subtlety that someone
6 would need to spend years and years reading EMV documents to
7 understand. Everyone knows. Everyone of skill in the art knows, as shown
8 by the Radu textbook on the right as well, that these ARQCs, these
9 cryptograms, are generated using an unpredictable number. And the point of
10 this is that, you know, you have a terminal generator and unpredictable
11 number so that if someone was trying to use the card to precompute a
12 transaction it would fail because they wouldn't know what the unpredictable
13 number was going to come -- was going to be from the card. It would only
14 happen at the time of the transaction.

15 Okay. Turning to Claim 13, you know, this claim has to do with the
16 fact that authorization is going to include values from the transaction and for
17 the same reasons we just talked about, as shown already on slide 73, that it
18 was well-known that, you know, the authorization needs notice from the
19 transaction. The whole point of an authorization is to authorize the data in
20 the transaction message. That's, sort of, textbook knowledge that a person of
21 skill in the art would have understood when reading Fiske. There's no
22 reason to force him to say that. That's clearly what he's talking about in
23 doing the ARQC validation.

24 Okay. Lastly, with respect to Claim 4 and those other claims that just
25 say that the interrogation performs in accordance with the card specification
26 or other things that try to claim the idea of doing this in a standardized way,

1 I mean, as we pointed out, Fiske is obviously directed to authorizing an
2 EMV transaction.

3 So, that's really all I had to cover so unless the Board has questions,
4 I'd like to reserve the remaining time for rebuttal.

5 JUDGE TARTAL: Okay. Thank you, counsel. I have you at just
6 under 50 minutes so we'll be in the vicinity of 10 and 10 and a half, 11
7 minutes for your rebuttal portion.

8 Unless any of the other members of the panel have questions at this
9 time? And hearing none, we are going to go off the record and take a brief
10 break to give Patent Owner an opportunity to get ready for his portion of the
11 presentation. I have it as 2:00 right now and so we will look to resume at
12 about 2:07. Let's say 2:08, somewhere just a little before 2:10, seven, eight
13 minutes and we'll confirm once we resume that everybody is back online.

14 So, we can go off the record at this point in time.

15 (Whereupon the proceeding went off the record at 2:01 p.m. and back
16 on the record at 2:09 p.m.)

17 JUDGE TARTAL: Thank you. We are back on the record and will
18 confirm that we have everyone that was available on the call. Can counsel
19 for Petitioner confirm that you can hear us and see us and are present?

20 MR. WILLIAMS: Yes, Your Honor. I'm here and can see and hear
21 you.

22 JUDGE TARTAL: And you are?

23 MR. WILLIAMS: Oh, good point. Counsel -- this is Eliot Williams,
24 counsel for Petitioner.

25 JUDGE TARTAL: Okay, thank you, counsel.

1 And, Patent Owner, are you ready to proceed with your argument and
2 able to hear and see everyone? And is there an amount of time that you'd
3 like to reserve of the total time of 60 minutes for your surrebuttal?

4 MR. LINDNER: Thanks, Your Honor. Again, this is Seth Lindner
5 for Patent Owner. I can hear and see everyone, and I would like to reserve
6 15 minutes for the surrebuttal.

7 JUDGE TARTAL: Okay, counsel. That will correspond to starting
8 off with 45 minutes. I will try to give you a head's up when you reach
9 around 40 minutes, and we just ask that you try to keep track of the time
10 also. And you can begin when you are ready. Thank you.

11 MR. LINDNER: Thank you, Your Honors, and good afternoon to
12 everyone again. I think counsel for Petitioner, kind of, explained in
13 overview of how these systems work and so I'm not going to rehash that, but
14 I do want to answer one question which is the one that when I started getting
15 into these I thought to myself, because Petitioner has talked a lot about how
16 really this is all just done in EMV and there's not much new in the patent.

17 And so, the question I asked myself was, well, what's really different
18 here? And I think the point that I want to emphasize is that the EMV
19 specifications that they've pointed to and all this prior textbook information
20 is contemplating the scenario where you have a physical -- a card that
21 wouldn't be interacting with a remote system, right? When you take your
22 card out to make a purchase your card doesn't go and talk to the Bank of
23 America to get any information. Whatever it needs there is already on the
24 card when the card is made.

25 And so, when you move that now to a mobile device or a smartphone,
26 one of the fundamental, you know, important questions is, okay, now if

1 we're not doing it that way where the card is -- or where the card -- the
2 phone isn't made by the bank, right, it's made by someone else, how is it that
3 we're going to be communicating? What information is going to be sent
4 from one place to the other? And obviously there's, you know, in these kind
5 of transactions the security matters a whole lot, but what's that interaction
6 going to look like now that the card doesn't have the built-in information that
7 it would need to conduct a transaction? And so, that's one of the things that
8 makes it different and why when we look at the claims the claims are quite
9 detailed in terms of what information gets sent from one player in the system
10 to the others and how does that get sent.

11 So, Your Honors, do you have a preference of whether I share my
12 slides or just talk through them by slide number? I can do it either way.

13 JUDGE TARTAL: This is Judge Tartal. I find it helpful if you're
14 able to share your slides. It makes it quicker for us to move along with you
15 when you're referring to a particular location. But as I mentioned before, we
16 also have copies in front of us so I defer to your choice as to what you're
17 more comfortable with.

18 MR. LINDNER: Okay. It looks like the permissions are -- it says,
19 "You might have to restart Webex." I apologize for that. So I'm not going
20 to do it that way. I'll refer to those slide numbers and hopefully that'll be
21 easy enough to follow along. So --

22 JUDGE TARTAL: Okay. That works well, counsel, thank you.

23 MR. LINDNER: -- what I'm going to do, I will jump around just a
24 little bit because I think it makes sense to handle these probably in a
25 different order than I originally organized them. Where I wanted to start
26 was with the grounds three and four. That's for the Fiske reference. And I'm

1 going to start with Claim 8 and then we'll move on to Claim 10 for Fiske.
2 I'll do the same thing then for Collinge.

3 So, the slide I'll start with is 23 for introducing this limitation of
4 Claim 8. So, we're looking at a step. Claim 8, the preamble was at a remote
5 computer system so now we're looking not at the mobile device but we're
6 looking at the remote system. And so if we go to slide 24, what I've shown
7 on the left, the top left corner, is what Petitioner said about this limitation.

8 So, we can see here that it doesn't make an independent analysis of the
9 of claim. It just simply refers back to prior discussions of Claim 1 and in
10 particular the limitation that we're addressing here regarding sending the
11 account identifier to a mobile device. That's in 8A, and you can just see in
12 the petition that it just cites to sections 1.B and 1.C. So, that's two sections
13 dealing with those limitations of Claim 1.

14 So, when we look at those two sections, and I've put in what I think
15 are the relevant portions of those two sections on the right of this slide, we
16 can see that what they say there because, of course, Claim 1 is not directed
17 to what is received by the remote computer system. It's directed to what's
18 happening at the mobile device. We can see that what 1.B says is that,
19 "single use keys, such as the ICC session key, are what they mean by data
20 associated with the account." And in 1.C what we see again is that the user
21 device receives from the remote servers the first set of data, and they say
22 that's an ICC session key.

23 So, first of all, we're talking about a session key which is not the
24 account identifier. It's not the payment, right? So that doesn't help us with
25 this claim limitation that recites receiving, or sorry, sending the account
26 identifier.

1 And the other point I would make is that for this limitation there's no
2 allegation that the limitation would be obvious, right? The obviousness --
3 there's nothing in Claim 8 in the petition that says it would be obvious, right,
4 so that section.

5 Now, what you will find if you read through Claim 1, the cited
6 portions, they're saying that these limitations of Claim 1 are obvious. The
7 claim date recites different steps and so they haven't alleged in the petition
8 that that was obvious or, of course, given any reason why those limitations
9 would have been obvious.

10 If we go to slide 25 --

11 JUDGE TARTAL: Counsel just to --

12 MR. LINDNER: -- here's --

13 JUDGE TARTAL: Counsel, this is Judge Tartal, just to clarify on
14 your discussion, Claim 8 depends from Claim 1, correct?

15 MR. LINDNER: Yes.

16 JUDGE TARTAL: And so is it your understanding that when
17 Petitioner refers back to analysis under 1.B and 1.C that it's asserting
18 limitation 8A is obvious for the same reasons as what they argue in 1.B or
19 1.C? Or are you suggesting something different?

20 MR. LINDNER: I'm not suggesting -- no, I don't think that's what it meant
21 at all and if you look at -- and I would encourage the Board -- I didn't put the
22 entirety of those sections here. I think what I put on the screen in slide 24
23 are the portions that are really the only ones even potentially relevant to this
24 limitation of 8A. And Petitioner there says that it renders obvious this
25 element. And what it talks about is single use payment keys that are being
26 received, right?

1 So, the obvious -- there's no way that the obviousness argument that's
2 made here could relate to something else being received when they haven't
3 even said that that something else is here in their discussion of Claim 1
4 which, of course, doesn't recite, even though there are some parallels, Claim
5 1 doesn't recite that the device receives this account identifier. It's not
6 recited in Claim 1. That only shows up when we look at Claim 8.

7 So, I think to answer your question, yes. Saying that Claim 1 is
8 obvious doesn't show that the new limitations that aren't in Claim 1 that are
9 part of Claim 8 that those would be obvious or, of course, provide any
10 reasons why they would be obvious.

11 So moving to slide 25, I'm just showing here on the left what
12 Petitioner said in reply. And what they say there, and I think what counsel
13 said again today, was that the key point is that there's this digital credential
14 data and in the reply they say, and I've underlined it here on the top left of
15 slide 25, that the petition expressly notes that, "Fiske involves receiving
16 digital credential data required for authorizing -- or for authorization,
17 including primary account number, PAN, from the remote server." So, they
18 quoted some language there that looks like it comes from the petition.

19 If we look at the petition at what was actually said, it comes from
20 pages 66 and 67 and I've included it here on the right. What those pages say
21 is that the card will return digital credential data and that returning is to the
22 POS terminal so it's a totally different -- I just put a graphic here on the
23 bottom there. They're pointing to in the petition information sent from the
24 card to the card reader, the POS, in response to a read record command. So,
25 that's an interaction between the card and the card reader. That has nothing

1 to do with what would be sent from the remote server to the card, right? So,
2 they just point at something different.

3 And in the reply I'm surprised they said that the petition expressly
4 notes this because what the petition expressly notes is a different interaction
5 between two different devices than what are claimed in Claim 8. So, on
6 slide 26 it, sort of, shows the rest of this, what they say in their reply, and on
7 the left I've just shown, kind of, their rationale. And what that says is that
8 the PAN would be included with the cryptogram by the card when
9 requesting payment authorization.

10 So, we have the same problem here. They're saying that the card is
11 going to include the PAN when it's requesting authorization. That's
12 information sent from the card to the POS, again, like I talked about on the
13 last slide. That's not saying that the remote system is going to send the
14 account identifier to the card. It's just you have the different steps in the
15 process in a different interaction.

16 We can see the same thing in what they cite in the portions of the
17 petition here that are cited in reply. So at slide -- or pardon me -- page 50 of
18 the petition it showed that -- it says that, "The card may return a cryptogram
19 as well as track two equivalent data." That again, the card is returning that
20 information. That's not saying that the card received it or that it was sent
21 from the remote system.

22 Slide -- or pardon me -- page 72 of the petition, 73, talked about the
23 same thing that the mobile device is returning an application cryptogram
24 response to it in response to GENERATE AC Commands. So again, what
25 that is describing is an interaction between the card and the POS. It doesn't
26 have anything to do with what was sent to the card from the remote system.

1 So, really they've identified, kind of, the wrong interaction and it doesn't
2 really describe that the remote system would send that information to the
3 card.

4 Now, the other problem with this is, of course, I showed on slide 24
5 what the entirety of their response was for Claim 8 and it was just C1.B and
6 1.C of the petition. So, there was no obviousness argument made. Now,
7 they make an obviousness argument and today counsel for Petitioner seemed
8 to make only the obviousness argument, which is that it would be obvious to
9 send this account identifier so that the card knows which account it's
10 supposed to make a transaction on behalf of. That wasn't in the petition.

11 And the Federal Circuit is clear that if you don't make the obviousness
12 argument in the petition at all, and certainly if you don't explain it, that you
13 can't do it in reply. The POR certainly didn't say that here's some reasons
14 why your obviousness arguments failed because there wasn't an obviousness
15 argument. So, Petitioner should have put it in the petition in the first place
16 and the reply is then also problematic because it's not responsive to anything
17 that's in the POR. You'll see here, you know, on the left of slide 27 that
18 they're not citing to the petition when this argument was made. They're not
19 citing to the POR to dispute something. They're just making a new
20 argument as to why it would be obvious.

21 The other thing I'll point out here, and I think Petitioner, sort of, gave
22 this short shrift in their presentation, but they're not pointing here and
23 saying, well, the EMV did this and everybody knew it from textbook
24 knowledge. There isn't a citation in any of this discussion of Claim 8 that
25 says, well, this would have been done because everybody knew that you had
26 to do it this way because EMV did it this way.

1 It isn't part of what EMV is doing. It's not cited that way and that's
2 because, like I said at the beginning, this idea of what gets sent from the
3 remote system to the card isn't part of EMV because EMV is not operating
4 in that scheme where the card needs to receive something from the remote
5 system in order to conduct a transaction.

6 So, I think that's number one. It's inappropriate for them to even
7 include that theory, and number two, the theory itself is flawed. Even if it
8 had been included in the petition, the idea that, well, Petitioner says, well, if
9 there were multiple accounts then you would need to know which key -- or
10 pardon me, -- you need to know which account the particular key is coming
11 from.

12 But Fiske doesn't mention multiple accounts and, in fact, what Fiske
13 says is that payment keys, and I'm showing on slide 28 here in Column 12
14 and 11 of Fiske, it says that, "Payment keys are what's used to activate the
15 application and associated with an account," which, of course, makes sense
16 that you would have an application on a device. In order to get that up and
17 running you have to enter credentials. You have to make sure that you've
18 got everything linked before you can start using it for payments.

19 So, Fiske said you use payment keys to make that connection. It
20 doesn't say that you use an account identifier. It certainly doesn't say that
21 the payment keys are the PAN. And Petitioner hasn't made that allegation
22 that any of those things would apply. So, even if they could make this
23 argument, sort of, belatedly that, well, it would be obvious to do this even
24 though it wasn't presented that way in the petition, their reasoning doesn't
25 even make sense here because Fiske doesn't say that this is what's done. In

1 fact, it shows a different way to, sort of, make that connection between the
2 application and which account is available to make purchases for.

3 Okay. So, let me move on now to click -- I'm sorry. Did you have a
4 question, Your Honor?

5 JUDGE TARTAL: Yes, this is Judge Tartal. I just wanted to, kind
6 of, clarify what my understanding is of the issue that you're raising. Clearly,
7 the petition includes an obviousness challenge to Claim 8 based on Fiske.
8 So, I gather you're not trying to argue that there is no obviousness
9 challenges, sort of, in the petition directed to Claim 8.

10 What I understand you to be saying is that the arguments Petitioner is
11 making, particularly on reply, go beyond the arguments made in the petition
12 and so are improper as reply arguments because, in your view, the petition
13 failed to sufficiently set forth how this limitation for Claim 8 would have
14 been obvious here for the asserted art. And to the extent Petitioner is now
15 making new arguments in the reply, they're improper. And is that a correct
16 characterization of what you're saying?

17 MR. LINDNER: Yeah, I think, Your Honor, you said that. Clearly,
18 they've made an obviousness argument for Claim 8, and I'm not sure if I got
19 the words quite right. I think there's certainly, if we look at, like, the
20 statutory bases for the petition it says, you know, "Claim 8 would be obvious
21 in light of that knowledge of a person of skill." So yeah, that's there.

22 As to whether there was any argument whatsoever about why Claim
23 8's particular limitations would have been obvious, that's where I'd say no.
24 There wasn't any argument there at all. So, simply saying at the top level
25 Claim 8 is obvious, that doesn't provide enough disclosure as to, well, which
26 elements are obvious? Why are those elements obvious? What's the

1 reasoning for it? What are you relying upon? So, that's where they haven't
2 met their burden and given Patent Owner any opportunity to address those,
3 you know, through expert testimony meeting because it came all in the
4 reply.

5 JUDGE TARTAL: Okay. thank you, counsel.

6 MR. LINDNER: All right. So, I'm going to move on to Claim 10 in
7 grounds three and four for Fiske, and I'll start on slide 30. So, the first
8 limitation, what we call 10A in the petition and in the papers, is a step that's,
9 again, at the remote computer system and this step recites what's received at
10 the remote computer system. And one of the things that's received, or two
11 things, are a response cryptogram and the account identifier.

12 And so what I've shown here on slide 30 is the entirety of what
13 Petitioner says in the petition for this limitation. And this is it. This
14 sentence is all of what they say. So, what they say is that, you know, "In
15 response to receiving the application cryptogram the terminal identifies the
16 type of cryptogram sent and forwards the ARQC," and I cut out some words
17 there just for brevity. And this is it.

18 So, the claim says you have to receive a response cryptogram and you
19 have to receive an account identifier. What they pointed to in the petition
20 was just the ARQC. That's the alleged cryptogram. This whole allegation
21 here is silent as to whether an account identifier is received.

22 They haven't said that Claim 10A is obvious. They haven't said, well,
23 we talked about this somewhere else in the petition. It's just that they
24 believe that here, so this is plainly deficient, as we pointed out on pages 53
25 to 55 of the Patent Owner response.

1 Now on slide 31, I'm showing what they say in the reply. So there
2 they say that the Petitioner explains that, "The device receives all the data
3 necessary to perform a transaction including the PAN." Okay, so here's the
4 problem again. What they're saying in reply is talking about -- they're
5 alleging that the device receives everything it needs and that that includes
6 the PAN.

7 But the claim is not talking about what the device received. The claim
8 is talking about what's received at the remote computer system, so this
9 statement here about what the device received it just doesn't get them there.

10 The other thing I'll point out, they say at the beginning of this on slide
11 31, page 24 of the reply, they say that, "Patent Owner ignored the analysis of
12 this element incorporated in the analysis of Claim 1." So, I want to just
13 pause there. And as we pointed out in the surreply, we've looked at on slide
14 30 -- I showed the entirety of their section. It doesn't refer back to Claim 1
15 so they're just trying to, sort of, put that in later.

16 If we look at other portions of the petition, and we saw one earlier
17 today where they said see section such and such regarding Claim 1, right?
18 They did that explicitly in a bunch of places. For Claim 10 for Fiske they
19 didn't do so at all. So, I don't think it's reasonable for them to make this
20 statement that, well, you have to go back into Claim 1 and there you'll find
21 this limitation because they didn't refer back to it. And it's different.

22 Again, Claim 1 doesn't recite this step. It doesn't recite what's
23 received by the remote computer system. It's talking about the steps
24 performed by the mobile device. And by the way, just for context, there's no
25 allegation anywhere that the mobile device -- if the remote computer system
26 were to get a cryptogram even, it doesn't come from the mobile device,

1 right? It will come in an authorization request that comes from the POS
2 terminal. So, we're quite far from what the claims were recite here.

3 Okay. So, let me move to slide 33 and we're talking about here
4 another limitation for Claim 10. This is 10B. And in this one the claim
5 recites, "At the remote computer system determining a current non-
6 permanent cryptographic key associated with the account using the account
7 identifier." Okay. So again, what happens here is it's, kind of, remarkable
8 when we look at the petition and the reply and how far and away it is from
9 actually showing what is needed. The petition says, and this is in the top of
10 slide 33 in the top left corner. What I've included here is the entirety of what
11 the petition says. It says, "Fiske discloses that the user," pardon me, "the
12 issuer may identify which session key was used to generate the ARQC." So,
13 the testing key that's not the account identifier. That's the alleged non-
14 permanent cryptographic key.

15 And as to which one was used to generate the ARQC, the ARQC is
16 the alleged cryptogram so nothing in 10B says one word about the account
17 identifier, right, that's being used to determine a non-permanent
18 cryptographic key. There's also no obviousness argument here. Petitioner
19 doesn't make one for this limitation.

20 Okay. So on reply, what Petitioner says is he essentially repeats, and
21 I've included it on the bottom left here of slide 33, essentially petitioner
22 repeats the statement quoted from Fiske above about the session key and the
23 ARQC and then they say that Figure 7 showed the issuer examining the
24 received ARQC and then they say this. Oh, this claim element requires
25 nothing more. But the claim isn't reciting examining a cryptogram. It's not

1 reciting that you identify a session key just by itself. It says you have to
2 determine a non-permanent cryptographic key using the account identifier.

3 Now, what Petitioner said, and this was -- let me refer to their slide
4 number on this one, so but what Petitioner showed in their slide 59, this is
5 Petitioner's demonstrative, they say that you don't -- oh pardon me. I'm
6 looking at Collinge now. Let me come back to that in a moment. So I'll get
7 through Fiske first.

8 So, what happens here in the reply is they just say, well, Fiske shows
9 that you figure out which session key was used and that's all the claim
10 requires. The claim recites more than that. You have to use the account
11 identifier to figure out or to determine the non-permanent cryptographic key
12 and there's simply no disclosure of that or even an allegation that that's what
13 was done in the petition or in the reply. So, it's just ignored.

14 Okay. So, what we've talked about is Claim 8 and Claim 10 as to
15 Fiske, and I want to move now over to the same claims for the Collinge
16 reference. And we'll see that in large measure we have exactly the same
17 problems. So, this would be slide 17 of Patent Owner's demonstratives.
18 We'll look at what's happened in the -- what the petition says as to this
19 limitation.

20 So again, this is sending the account identifier to the mobile device.
21 So again here, Petitioner just presents Claim 8 in the petition as various
22 citations to other sections of the petition. So, we went through this in the
23 POR in detail on pages 37 to 39 each of these sections that are being cited to,
24 and what we see, similar to what we saw from Fiske, is that the sections that
25 are being cited to, for example in 1.B. which is shown on slide 17, 1.B
26 discusses what the mobile application is going to request. That's a request

1 that relates to a mobile application making a request. It doesn't show what's
2 sent from the remote system to the mobile application so that's essentially
3 irrelevant here.

4 In 1.C what we see is that they say Collinge discloses that the mobile
5 payment application receives an encrypted payload and payment credentials
6 and that that payload includes a single use key. So again, that's the alleged
7 non-permanent cryptographic key that would be received, right, but the
8 claim says that you're receiving the account identifier, which they said is the
9 PAN. That's not the cryptographic key or -- yeah, that's not the
10 cryptographic key or the single use key that they identify in 1.C.

11 So, we can then look at the other two parts of the petition that they
12 cite to and what they talk about in 1.A3 on slide 18 in the petition is that
13 "payment credentials can be stored in the remote system, remote-SE and for
14 provision to the mobile device," and that those are "returned in an encrypted
15 payload."

16 So, if we look at -- on the previous slide we looked at that encrypted
17 payload and what they've said about that is that it includes a single use key.
18 It doesn't say that the encrypted payload includes the primary account for
19 any other account identifier. It includes a single use key.

20 So then we have the other -- the last remaining part of the petition that
21 they cite to describes, again on slide 18, that "the mobile device sends
22 payment credential data to the POS terminal." So again, we're talking about
23 this different aspect. We're talking about mobile device to card reader, not
24 something sent from the remote system to the mobile device. And so it's
25 simply not here in Collinge's either, just like it was for Fiske. It's also not in
26 the EMV standard because, as I mentioned, EMV doesn't have this step of

1 having to send anything to the card which was, you know, at that point
2 envisioned as a physical card.

3 JUDGE TARTAL: Counsel, this is Judge Tartal. When you have a
4 moment, I don't want to interrupt what you want to cover in the immediate
5 term, but I believe in the response, Patent Owner disputed whether Collinge
6 was prior art. And I don't think you have any slides on that issue, but I
7 wanted to at least ask you if you are still maintaining that argument and if
8 you can briefly explain what the argument is that you were asserting in there
9 in regards to the prior art status of Collinge.

10 MR. LINDNER: Sure. Let me finish one more slide here on this
11 point and I'll turn to that briefly. So, on slide 19, again, I'm showing what
12 Petitioner says in reply as to this point for Claim 8. And what they say is
13 that effectively again, they're, sort of, quoting from the petition saying that,
14 you know, Collinge discloses that all the necessary payment credentials are
15 received including the account information and the PAN. But just like they
16 did for Fiske, what they are quoting from the petition is actually a section
17 1.A2 on page 38 of the petition. That section is describing that the card will
18 return this information including the PAN to the POS so it's not what's
19 coming to the card from the remote system. It's what's going from the card
20 to the POS. So, the petition never made the allegation because Collinge
21 doesn't show that this information, this account identifier for the PAN, is
22 sent from the remote system to the card.

23 As to the obviousness argument that they made here on -- I have it on
24 slide 20 -- where they say that static payment credentials, which is in
25 paragraph 9 of Collinge, that those would be understood by a person of skill
26 to include the account number. That argument is brand new in the reply. It

1 is entirely speculation by counsel. There's no expert citation. They don't
2 cite to anything in the record at all. It's simply an argument by counsel that
3 this is how a person of skill would have understood the term static payment
4 credentials in Collinge.

5 That term is used in Collinge, but we have no analysis by Petitioner as
6 to why a person of skill would understand it. And it's not, as I mentioned,
7 it's not even an expert opinion. It's just an opinion by counsel. So, if that
8 were the argument they wanted to make, which I don't think is supported
9 anyway, it should have been in the petition where we could have then
10 addressed it and said, okay, well, why are you interpreting static payment
11 credentials this way, you know, have expert testimony on it. But we don't
12 have any of that because it came only in the reply.

13 Okay. So, let me get to the question about Collinge as prior art, and
14 I've got slide 38 which gets to this issue a bit. So, it appears that Petitioner
15 focuses on whether or not Collinge properly incorporated by using the right
16 words, the provisionals. And that's not really the question here. Patent
17 Owner isn't just giving Collinge by saying I incorporate this in its entirety,
18 that that incorporation wasn't the right way that you do an incorporation.

19 The problem is that in this instance what we're talking about is a
20 particular set of rules for an IPR where Collinge itself, which was filed after
21 the priority date of the '171 patent, is using the provisional to predate the
22 '171 priority date. And the court has laid out through Dynamic Drinkware
23 and a few other cases, sort of, when is it that you're allowed to do that?

24 And the requirements are that number one you have to have support in
25 that provisional for the claims, and number two, that the subject matter that
26 you're relying on has to be carried forward from the provisional into the non-

1 provisional. Those are the circumstances where it's allowed to do this, kind
2 of, weird -- you're using a reference that isn't prior art, where the provisional
3 and not prior art. It's not a printed publication so it couldn't normally be
4 used, so why can we use those disclosures? Only when those disclosures --
5 there has to be a one-to-one match.

6 You can use -- you obviously can't use disclosures that only appeared
7 in the non-provisional for the first time. You also can't use disclosures that
8 appear only in the provisional and don't get carried forward into the non-
9 provisional.

10 And I think Petitioner, counsel for Petitioner, said today that the law is
11 clear on this but I've searched high and low and the closest case that I found
12 was the one that was cited in the POR relating to this Sequenom decision
13 where the Board actually looked at a situation similar to this and interpreted
14 the Federal Circuit's Yamaguchi decision to say that "the patent defeating
15 disclosures in a provisional must also be found in a document applicable as
16 prior art under 102 E." That is either a patent or a printed publication.

17 So, it's saying you have to find the disclosures that are in the
18 provisional in now the published application, and in this instance that
19 provisional was incorporated by reference. And I have it here on slide 38.
20 The entire contents are incorporated by reference for all purposes, right? So,
21 it's the same situation as what Patent Owner did here with Collinge -- or
22 pardon me -- Petitioner is trying to do with Collinge. You have a non-
23 provisional application. It incorporates by reference in its entirety a
24 provisional, and what the Board said was that you still need to show that the
25 disclosures in the provisional are in the published application in order to use
26 it this way. And that's not what Petitioner did here. There's numerous

1 disclosures and it's mentioned throughout the POR where the Collinge
2 provisional is the only place that these disclosures exist. If you look at the 4
3 corners of Collinge you don't find these disclosures.

4 And that's relevant, as it turns out, I won't go through them all in
5 detail here, but for example for limitation 1.A3 where they talked about a
6 pull request, that comes only from the Collinge provisional not from
7 Collinge. In limitation 1.C where they talked about how a cryptogram is
8 calculated, that comes only from the provisional and it's not carried forward
9 into Collinge. 1.E2, again, it's only, pardon me, it's only in the provisional.

10 JUDGE TARTAL: Just to verify, counsel, this is Judge --

11 MR. LINDNER: The other -- go ahead.

12 JUDGE TARTAL: -- sorry to interrupt. This is Judge Tartal. So, as I
13 understand what you're arguing is that when you say it's not carried forward
14 you mean although it's incorporated by reference it isn't expressly set forth.

15 MR. LINDNER: That's right.

16 JUDGE TARTAL: And so you're suggesting that by merely
17 incorporating by reference, that's not. for purposes of relying on it as prior
18 art, sufficient to carry the disclosure forward to the non-provisional
19 application.

20 MR. LINDNER: That's our position, Your Honor. And like I said,
21 the closest case that anyone has found is the one that I mentioned with the
22 PTAB where they said, look, even though you have a reference that is
23 incorporating by reference, right, you have a publication or a pre-publication
24 that's incorporated by reference to this provisional, you still have to show
25 that the elements are present there. So, that would indicate that
26 incorporating by reference in this circumstance in the PTAB where you have

1 to have a patent-oriented publication, that that would be -- you have to look
2 to what's actually in the body of Collinge itself, not just, you know, a little
3 blanket statement on incorporation by reference.

4 Okay. So, I wanted to now talk about Claim, and I think I have only a
5 couple of minutes left here, I'm going to go and talk about Claim 10. And I
6 think the best place to start there would be slide 13 of Patent Owner's
7 demonstratives. So, what slide 13, sorry, let's go to slide 14. So, what the
8 petition said, this is relating to determining a non-permanent key using the
9 account identifier.

10 So, the petition says that, "retrieving the KSun value is what would be
11 equivalent to determining the key." So, that's what the petition says,
12 retrieving.

13 And if you look at the Collinge provisional it also says retrieving. It
14 says using the ATC the issuer is able to retrieve the KSun value." Now, in
15 the reply they change it and they moved from the word retrieving to the
16 word recalculating. And I've shown that on the bottom right of slide 14. So,
17 when we pointed it out in the POR we said, well, the ATC is what's used to
18 retrieve it. That's what the provisional says. That's not the account
19 identifier. You're supposed to use the account identifier.

20 So then they changed it and they said, well, no. It's recalculated,
21 right? And today they went even further. They just abandoned the retrieve
22 entirely and said because the non-permanent key is in the first instance
23 calculated using the PAN, now when you retrieve it you must use the PAN.
24 But the problem is that doesn't make any sense.

25 First of all, it's not in the petition. Second of all, what the Collinge
26 provisional says is that you're retrieving that key. There's no need to

1 recalculate it because even in Claim 1 the key was already calculated. It's
2 what was sent to the device and then the device sends the cryptogram
3 allegedly back to the POS, and then it gets back to the remote system, right?
4 The remote system has the key already. It's the one that -- it's the system
5 that would have created the key. So, Petitioner's argument that somehow
6 because keys come from PAN that you must use the key to determine the
7 non-permanent cryptographic key is just completely incorrect.

8 And even, like I said, the provisional itself says that you're retrieving
9 it. It's there. You simply need to look it up, which is what the '171 patent
10 shows. Figure 26 is an example. There's a table. The PAN is there. The
11 temporary key is there and you use the account identifier to look it up.
12 That's not what Collinge says is done. It says it uses the ACC to do that.

13 So, the argument about the PAN being involved because it was part of
14 when the key was originally created, that's not what's used in this
15 determining step and it's not what the petition even alleged to have used in
16 this step.

17 Okay. The last point I want to make is about, and I think I've gone
18 right to the end of my 45 minutes, but I'm going to, if Your Honor is
19 allowing, I'd like, to use a few more minutes and save the remainder for
20 surrebuttal. I wanted to talk about Claim 10 in a different way, which is
21 what did Petitioner identify as their remote computer system?

22 So, I've gone through this in some detail on slides 5 through 12, and
23 I'm going to go through it pretty quickly here, but let's start with slide 7.
24 They pointed to their remote system SE in Collinge as the remote computer
25 system. That was clear in the petition, pages 38 to 39 that I've shown. They
26 refer to it by number, remote computer or remote-SE system, and

1 remote/cloud system. And those are both pointing to the gray box in the
2 lower left corner of Collinge's Figure 7.

3 That is the system that they point to. When asked during his
4 deposition if that's what he was relying on, Petitioner's expert confirmed,
5 yes. It's that gray box in the lower left corner. That's the remote system.

6 So, when we look at Claim 10 what we see is that Petitioner now
7 points to different components within Collinge for the same -- or for the
8 alleged functionality from Claim 10, right? And so I've shown it here on the
9 slide. I won't go through all of this but effectively they've pointed to -- I'm
10 sorry, slide 9 -- they've pointed to these different portions of Collinge. And
11 it implicates several different components, an acquiring processing server,
12 an acquirer, a payment network, issuer processing server 308. So, all of
13 these things are what they rely on in Claim 10.

14 And so on slide 10 I've just shown here the red box is what they've
15 said for Claim 1. The green arrows are indicating components that they
16 expressly relied on for limitations of Claim 10. Those are outside of the red
17 box, so they're clearly pointing to for Claim 10 something different. And
18 now we get to the reply, and in the reply they introduced for the first time
19 this blue box that I have shown on slide 11.

20 And so the problem here, and just the POR goes to this in detail, but
21 there's a bunch of problems with this. One of them is this blue box. They
22 never said this with their remote computer system.

23 Second problem is they are relying on components outside of what
24 they now say is the new remote computer system, right, the blue box.
25 They're pointing to components outside of that for elements of Claim 10.
26 So, even if the box had originally been in the petition, which it wasn't,

1 they're identifying components outside of that to perform the limitations that
2 are supposed to be performed at the remote computer system. So, it doesn't
3 work for that reason and it's inconsistent with what they said in the petition.

4 The other problem is, and Petitioner said this today, they said -- and
5 so I've highlighted on slide 12, I've highlighted here that the blue box
6 components are expressly stated to share a connection 178 there between.
7 And so I've shown that in the figure here on slide 12.

8 Today what Petitioner said was these are clearly working together as a
9 system. So, I'll say that's a new argument that they're working together as a
10 system because it wasn't made in any of the papers. So, I'll just put in my
11 objection now to that new argument. And we did address this in the surreply
12 because I thought maybe they were trying to do this. If Petitioner wanted to
13 argue that these two systems were together one system and say that these are
14 one remote computer system, that argument has to go into the petition so
15 that we have an opportunity to question their expert about, well, why do you
16 say these are a remote computer system as opposed to being separate
17 systems?

18 Both the Collinge and the Collinge provisional refer to them as
19 different systems. One is a cloud system. The other is an issuer system. So,
20 the fact that there's an error between them suggests there's maybe some
21 communication between the two, but there are communications between
22 each of the different components that are shown in these figures like on slide
23 12 in Figure 7, right? There's communications happening all over. It doesn't
24 mean that that system is operating as a remote computer system.

1 So, not only is this argument late, it is also entirely unsupported and,
2 like I said Petitioner, is trying to, sort of, beef it up today and I don't think
3 that's appropriate if it's not in the papers.

4 JUDGE TARTAL: Okay, counsel, you're at 51 minutes or so if you
5 want to reserve any time.

6 MR. LINDNER: Okay, thank you. I think I will stop there and I will
7 reserve the remainder of my time.

8 JUDGE TARTAL: Okay, counsel, thank you. That will leave you in
9 the vicinity of nine minutes for the surrebuttal.

10 We will return to counsel for Petitioner. If you're prepared at this
11 point you can proceed with your reply arguments. I have 11 minutes on the
12 clock, give or take, for your reply. And you may be muted, counsel.

13 MR. WILLIAMS: Thank you. Yeah, give me one moment. I'm just
14 trying to share these slides again.

15 JUDGE TARTAL: If you want to do it, again, counsel, if you have
16 any response to the comments that Patent Owner made in regard to the prior
17 art status of Collinge, that might be helpful just to check that issue off --

18 MR. WILLIAMS: Sure.

19 JUDGE TARTAL: -- if you care to address it first.

20 MR. WILLIAMS: Happy to. Let me go to slide 30. You see slide
21 30, correct, Your Honor?

22 JUDGE TARTAL: Yes, we do.

23 MR. WILLIAMS: Okay, great. So, as we point out there, the
24 argument in the petition is that the Collinge publication incorporates
25 material from the provisional and the case law we have on the screen there
26 in the two -- on the left side shows that that type of incorporation by

1 reference is completely consistent with the Federal Circuit precedent that,
2 you know, if you don't have -- carrying forward doesn't mean you literally
3 have to verbatim copy things in. You can incorporate them by reference.
4 And that's what Collinge did.

5 In the Comcast case we had a very, almost identical fact pattern and
6 the PTAB have had no problem finding that the provisional was prior art
7 since it was incorporated by reference in the published patent. So, that's
8 really all I have on that issue unless you had questions about it, Your Honor.
9 I think it is very straightforward.

10 JUDGE TARTAL: No. I just wanted to make sure that you had the
11 opportunity to address the arguments and help us clarify on the record what
12 the parties' positions are, so that's fine.

13 MR. WILLIAMS: Okay, thank you. Okay, just returning to, sort of,
14 the merits arguments and so Patent Owner started with Fiske so I guess I
15 will start there. With respect to Claim 8, the issue that Patent Owner is
16 pointing to is the question of what does Fiske provision to the card. And the
17 point we make in the petition, this is, you know, really with respect to both
18 Fiske and Collinge, is that because the PAN is required as part of the
19 payment credential during the point of sale transaction that it must be
20 provided from the issuer or at the very least it's obvious to provide that from
21 the issuer because it needs to get onto the card in some way.

22 We know what's on the card from both Fiske, I mean, Fiske and
23 Collinge both make clear that the PAN is on the card application that's
24 running on the device because what's happening is it's an emulated card,
25 obviously, running on the mobile phone. So, you need to get the PAN in
26 there somehow. It's necessary for every transaction. You have to put PAN

1 into the transaction data somehow and it's got to come from the device, and
2 both Collinge and Fiske make clear it's in the device.

3 And so the point we make in the petition is pointing to the fact that,
4 look, this is necessary data and the other thing Collinge and Fiske say is that
5 this remote server is the thing that provisions all the credential -- all the
6 necessary credentials onto the phone. So in both cases the point is that, you
7 know, a person of ordinary skill in the art would have understood from
8 reading Fiske and Collinge that that's what's going on. The PAN is getting
9 provisioned onto the device with the other credentials.

10 Now, you know, it's true in the petition we focus mostly on
11 provisioning of the session key because that, in our view, was the, sort of,
12 only thing that was even plausibly new in this patent, but that does not mean
13 that we were disregarding the other elements. They were addressed and we
14 point out in reply exactly how. So -- and the disclosures of the references
15 are, I think, very solid.

16 So, look, with respect to Fiske you can see on slide 68 some of the
17 disclosures that we point to in the petition for this provisioning, which is,
18 you know, Collinge at -- sorry. This is Fiske we're talking about at Column
19 11, Line 34 discussing how the device is provisioned with the payment
20 application and that then when the card is used it would send the PAN. So,
21 this was, sort of, the point of how we articulated this combination for Claim
22 10, sorry, for Claim 8 in the petition and in reply.

23 And now it's also true in reply we provided some additional
24 motivation for that combination, so Patent Owner talked about that and, you
25 know, it's true we did explain and provide additional motivations why you
26 would have provided the account number with the session keys during every

1 provisioning including so that the device if it had multiple accounts on it
2 would know which key was associated with which account. But that in no
3 way was reflective of a failure of the petition. It was just really responding
4 to Patent Owner's argument in response and giving some additional
5 motivation for the argument to be set forth in the petition.

6 Let me turn to Fiske, Claim 10. So, this -- remember Claim 10 here
7 relies -- relates to this question of what is the data that's getting sent to the
8 issuer during authentication. And we have a whole analysis of obviousness
9 in the petition for both references based on these two different constructions
10 that directly address this issue.

11 Remember the question is, okay, when the device is talking to the
12 terminal does it send the PAN and the cryptogram in one message or in two
13 messages? But the point is both of those things are getting sent into the
14 point of sale terminal and it was obvious to do it in either the ways that
15 Claim 1 may be covering. So, that analysis was directly relevant to Claim
16 10, which has to do with now receiving that data from the point of sale
17 terminal.

18 So, you know, during the transaction it goes into the point of sale
19 terminal. Then it gets passed to the network eventually landing at the issuer
20 where the issuer then needs to do the reconstruction of the message
21 authentication code. So, yeah, it would certainly receive the PAN. That's
22 definitely provided. We showed how it's provided to the point of sale
23 terminal. We've explained how a person of ordinary skill in the art knows
24 that the whole point -- I mean, you can't even route this transaction in the
25 first place without receiving the PAN. And the issuer in order to do
26 processing needs to know the account number that it's processing on. So, I

1 think that is laid out in more than sufficient detail in the petition and the
2 reply as to how Fiske is using the PAN during authorization to make clear,
3 yep, it definitely receives it and it's using it to look up the account so that the
4 authorization can go forward, as every person of the ordinary skill in the art
5 would have known.

6 Okay. Let me turn to Collinge. The arguments are very similar, I
7 think, with respect to Collinge just looking at the arguments Patent Owner
8 was addressing. Again, as we lay out in the petition starting at page 26, we
9 explain how in Collinge this remote system has to generate the payment
10 credentials. It includes the single use key again. You know, we're never
11 restricting ourselves to the single use key. We did call it out in particular
12 because we did think that was, sort of, the only, again, plausibly new feature
13 here but, you know, it generates all of the payment credentials. That is laid
14 out in the petition.

15 Collinge talks about for instance, you know, the petition references
16 Collinge at paragraph 48 and talking about the provisioning. When you read
17 paragraph 48 of Collinge you'll see that it explains that the payment
18 credentials included on the card, you know, would include the magstripe
19 payment credentials, the M-chip payment credentials, and again, going back
20 to my comment at the outset of my presentation earlier, a person of skill in
21 the art reading this patent when they see M-chip payment credentials they
22 know what that is, right? They know that that includes the PAN and
23 therefore it's clear that Collinge is provisioning the PAN as well as the key
24 to the device during those --

25 JUDGE DOUGAL: Counsel?

26 MR. WILLIAMS: Yes.

1 JUDGE DOUGAL: This is Judge Dougal. You know, here you refer
2 to the petition at page 26, which is the disclosure of Collinge of your
3 discussion generally of the disclosure. So, are we supposed to take your
4 ground and then read other parts like your general disclosure and match up
5 the claim limitations? Or do you point back in the petition to this
6 discussion, earlier discussion as to how these elements interact or are we just
7 supposed to -- I guess I'm not sure that you really put Patent Owner on
8 notice about how you identified, how Collinge teaches these elements.

9 Is it enough if you put it in the general disclosure or discussion of
10 what the prior art teaches or do you have to, you know, in the claim element
11 identify it? Or is this just a preliminary discussion and you're going to get
12 into, you know, where you identify it in the discussion of claim elements in
13 the petition?

14 MR. WILLIAMS: Yeah. So, yeah, a couple of questions there. I
15 mean, I think first of all, yes, the petition should be read as a whole to
16 understand, you know, what disclosures the Petitioner is pointing to. With
17 respect to the particular mapping that we're pointing to for provisioning a
18 device with these keys, we did point at paragraph page 38 where we analyze
19 element 183 of the petition. And we do talk again about how Collinge
20 discloses payment credentials are stored in the remote-SE and are
21 provisioned to the device.

22 So, we specifically mapped the payment credentials in quotes to that
23 element and I do think, you know, in terms of understanding what those
24 credentials are I'd have to read those from the perspective of a person of
25 ordinary skill in the art. And a person of ordinary skill in the art would

1 understand those credentials include the PAN as we, sort of, talked about in
2 the background section of the petition.

3 So again, the background section explains that, you know, what's
4 going on here and, sort of, summarizes the reference that explains how this
5 remote server is the thing that's generating the credentials and sending them
6 to the phone and it cites to this particular paragraph that makes clear PAN is
7 one of those things. So yeah, I think we did expressly map this element to
8 payment credentials from the device and we explained what that is, so I do
9 think the petition is more than sufficient to answer the question you're
10 asking, which is, you know, where do we actually map the elements. It's in
11 the claim analysis, but you have to read the analysis together with, kind of,
12 the background understanding of what this reference is including how a
13 person of ordinary skill in the art would have approached it.

14 Okay. And --

15 JUDGE TARTAL: Counsel, you're at about 11 minutes so if you
16 have some concluding comments that would be --

17 MR. WILLIAMS: Yeah. I just wanted to address the issue with
18 respect to the remote computer system thing that was mentioned at the end
19 of Patent Owner's presentation which is, you know, our petition maps the
20 claim functions to various aspects of that Figure 7 in the Collinge
21 provisional. And we've been consistent in identifying where those functions
22 are performed. And as our expert pointed out, you can see from slide 58
23 that, you know, the word system does not imply that everything has to
24 happen in a single computer. It could be a collection of computers and that's
25 what's mapped in the petition.

1 I'll also say I would encourage the Board to go back and read that
2 cross-examination testimony because I think you'll see that the questions that
3 were being asked about specifically the remote SE, those all related only to
4 the functions performed in Claim 1 that had to do with preparing the key and
5 not the stuff that's in Line 10 relating to authenticating the transaction once
6 it's been conducted.

7 So, unless the Board had any other questions I will rest.

8 JUDGE TARTAL: Okay. Thank you, counsel. I don't see any
9 additional questions from members of the panel, so we appreciate your
10 arguments and answering our questions.

11 We will turn now to counsel for Patent Owner, and I believe you have
12 nine, we'll say 10 minutes for your surreply. Counsel, you can begin when
13 you're ready.

14 MR. LINDNER: Thank you, Your Honor. Okay. So I want to -- I'll
15 start with Claim 8. Counsel for Petitioner said that the PAN must be
16 provided to the mobile device in some way and so it seems like their
17 argument is that, well, if the mobile device needs to have the PAN in order
18 to conduct a transaction that although the art doesn't say so we're going to
19 read in this idea that you would send the PAN every time you're going to
20 send a key because the PAN has to be there for some reason to make a
21 transaction. So, let's just send it every time.

22 And, I mean, that's one way to do it, right, but the art doesn't say that
23 you do it that way. And, in fact, as I talked about earlier, Collinge and Fiske
24 describe that there's a setup process that happens before you try to make a
25 purchase, right, that would already link the mobile application to the
26 account, right? So, as a part of that transaction where you're getting a key to

1 say that, well, you have to send the PAN, it's required, and therefore send it
2 every time it just doesn't make sense.

3 Petitioner's discussion of how the reference in Fiske and Collinge
4 describe sending all the necessary credentials, that phrase "all the necessary
5 credentials," that's not in Fiske and Collinge. Of course, the device will
6 have to have everything that it needs, but it doesn't have to come every time
7 from the remote system.

8 So, the other thing I'll point out here is that just because the device
9 sends the PAN to the POS, which that's mostly what they focused on, that
10 both the device sends it so it must be there, that doesn't tell you where it
11 came from. So, there's a bunch of other payment credentials, for example,
12 the amount of money that's being charged or the currency or other things
13 that are part of what the device would send in order to get authorization.
14 Those didn't come from the remote system, right, and certainly not with the
15 remote system at the time the remote system sent the key.

16 So, what Petitioner has done is just identified one way that it could
17 have been done, alleges that that was an obvious way to do it, sort of, in
18 reply, and hasn't provided a reason why that's the way that the prior art
19 actually operated.

20 Okay. Now, I want to talk about Claim 10 and what I want to point
21 out here is that what counsel for Petitioner said for Claim 10, which relates
22 to how the key -- pardon me -- whether the cryptographic key at the remote
23 system is determined using an account identifier. I pointed out that they
24 made the argument today that you have to regenerate the key. What counsel
25 said just now was that you're going to use the PAN to look up the account,
26 which is how I described what happens in the '171 patent.

1 But the argument in the reply was that, and in their slides, was that
2 you have to take the account number and recalculate the key. And just now
3 counsel for Petitioner said not you're going to recalculate the key. You're
4 going to look up the key using the account number. I would urge the Board
5 to look at the papers and see if there's any evidence at all that the account
6 number is used by the references to look up the account or to look up the
7 cryptographic key.

8 The references are specific. They say to use the application
9 transaction counter, ATC, in order to retrieve the KSun data you have in
10 Collinge, right? So, counsel for Petitioner today is saying just now that you
11 use the PAN to look it up. That's a new argument. I guess I'll object to it as
12 a new argument because it doesn't say that. And even in their
13 demonstratives today they presented it as using the PAN to recalculate. So,
14 neither of those things is done, so that's really incorrect.

15 The other thing I'll point out is that Petitioner made, kind of, an
16 incredible argument they made today, which is that the reason that the
17 petition lacks the detail to say where these elements are disclosed and, you
18 know, you can't find them and let you go back and look at the background
19 discussions of what it means to be -- what payment credentials mean,
20 counsel for Petitioner said, well, we thought the key was really the only new
21 feature so we didn't describe the rest of it.

22 And I just think that's a failure of the petition to provide the specificity
23 that's required by saying you have to go look elsewhere. And I would also
24 say that, as I mentioned, simply throwing the umbrella of payment
25 credentials up and saying, well, we talked about payment credentials so
26 therefore all of them get sent from the remote system to the mobile device, it

1 just doesn't make sense. There's a different set of information. The mobile
2 device is receiving something from the remote system. You know, the
3 claims say the cryptographic key in Claim 1. Claim 10 says you have to also
4 have the account identifier, and then a different set of information is sent
5 from the device to the POS terminal, right? You're not just sending the same
6 thing. The whole point of a transaction is that you're going to send different
7 information.

8 So, for them to rely on, well, the mobile device is going to send the
9 PAN so therefore it must have received the PAN from the remote system, it
10 just doesn't make any sense. These are two different interactions and clearly
11 this wouldn't work if all you're doing is sending the same information in a
12 loop, right? The information gets processed. It gets changed. And so
13 there's no reason why the PAN would have to be sent for every transaction.

14 And if that were what they wanted to say, then the petition should
15 have said so instead of just focusing on the cryptographic key being sent. It
16 should have said here's our argument and then we could have responded to
17 it.

18 I think I have three minutes left, which is unusual for me. I usually
19 take up every last moment, but if there aren't any questions, I have left
20 myself some space to answer them.

21 JUDGE TARTAL: Thank you, counsel, and turning to the rest of the
22 panel? I don't have any additional questions. I --

23 MR. LINDNER: Could I make one other comment? Sorry. I had it
24 in my notes and I forgot to do it.

25 JUDGE TARTAL: Yes, of course.

1 MR. LINDNER: Okay, thank you. I did want to comment on the
2 case that Petitioner said was relevant to the -- gosh, where did I write it
3 down? I'm sorry. I can't find it in my -- oh, Comcast. They pointed to the
4 Comcast case. And I think counsel for Petitioner said it's the same fact
5 pattern as we have here. It is not. And this is in the surreply on Page 3. In
6 Comcast the published application was prior art to the challenged patent.
7 Okay. They weren't using the provisional to get behind the challenged
8 patent so that's a totally different scenario here. It doesn't implicate
9 Dynamic Drinkware. It doesn't implicate. It's the published application was
10 itself already prior art, so it's not that case, as I pointed out in the surreply,
11 that case is not on point for the issue that we have here.

12 JUDGE DOUGAL: Counsel, this is Judge Dougal. Looking at your
13 *Sequenom* case, IPR2014-00337, it looks like there that the reference that
14 was at issue was just a provisional that we, the Board, found that was
15 improper. What is it, U.S.C. 315, I think, that specifies that IPR proceedings
16 are limited to patents and published publications. We determined that by
17 relying solely on a provisional it didn't fit within any patent or a print
18 publication. So, I'm not really sure how that case applies to the facts here
19 where Petitioner is relying on a patent that incorporates by reference an
20 earlier provisional.

21 MR. LINDNER: Thank you, Your Honor, and that's a good point and
22 you're correct that in that instance the Petitioner relied on the provisional and
23 the Board's response was that you couldn't use it by itself. The language that
24 the Board used to describe it as to why that wouldn't work did, you know,
25 like I said, it did note that you have to show that the disclosures in the

1 provisional are also in a published application, like as I mentioned, that
2 published application did incorporate by reference.

3 So, you know, there isn't a case that's closer to the facts that we have
4 here. That was the closest one that either side, I think, gave and in that one
5 it does say even though it's incorporated by a reference, the case does say
6 that you have to show that it's, you know, you have to show that it's in the
7 published application. So, I agree, Your Honor, it's not 100 percent on
8 point, but -- and I wish there were another one. I was shocked not to find
9 one but this is the closest that we have and it does make that indication that
10 you have to show that the disclosures are actually in the published
11 application.

12 JUDGE DOUGAL: Thank you.

13 JUDGE TARTAL: Okay, thank you, counsel. I think there are no
14 additional questions from the panel so I believe that will conclude our oral
15 arguments for today. We thank counsel for both parties for appearing and
16 for answering our questions. We'll take this case under advisement and
17 issue our decision in due course. We are off the record.

18 (Whereupon, the proceedings at 3:27 p.m. were concluded.)

IPR2023-01289
Patent 10,032,171 B2

PETITIONER:

Eliot D. Williams
Jennifer Tempesta
Baker Botts L.L.P
eliot.williams@bakerbotts.com
jennifer.tempesta@bakerbotts.com

PATENT OWNER:

Seth Lindner
Brett Cooper
Robert A. Auchter
BC Law Group, P.C.
slindner@bc-lawgroup.com
bcooper@bc-lawgroup.com
robert@auchterlaw.com