Trials@uspto.gov
571-272-7822

Paper No. 30
Entered: June 2, 2025

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

VISA, INC.,
Petitioner,

v.

CORTEX MCP, INC.,
Patent Owner.

IPR2024-00486 (Patent 9,251,531 B2)
IPR2024-00488 (Patent 9,954,854 B22)
IPR2024-00489 (Patent 10,749,859 B2)
IPR2024-00490 (Patent 11,329,973 B2)

Record Of Oral Hearing
Held: May 6, 2025

Before SHEILA F. McSHANE, KARA L. SZPONDOWSKI, and RUSSELL E. CASS, *Administrative Patent Judges*.

APPEARANCES:

ON BEHALF OF THE PETITIONER:

MATTHEW ARGENTI, ESQ.
of: Wilson Sonsini Goodrich & Rosati
650 Page Mill Road
Palo Alto, CA 94304-1050
(650) 493-9300
margenti@wsgr.com

ON BEHALF OF THE PATENT OWNER:

DOUGLAS WILSON, ESQ.
Armond Wilson LLP
13785 Research Boulevard, Suite 125
Austin, Texas 78750
(949) 932-0778
doug.wilson@armondwilson.com

The above-entitled matter came on for hearing Tuesday, May 6, 2025, commencing at 11:00 a.m. MDT, at the U.S. Patent and Trademark Office, 1961 Stout Street, Denver, CO 80294.

P-R-O-C-E-E-D-I-N-G-S

(1:01 p.m.)

JUDGE CASS: Good morning, everyone. This is the oral hearing in a series of related cases between Visa, Inc. and Cortex MCP, Inc., IPR 2024-00486, 487, 488, 489, and 490. I am Judge Russell Cass and with me on the panel today are Judges McShane and Szpondowski.

Can we start by having an identification from each side of who is present?

MR. ARGENTI: Good morning, Your Honor. Matt Argenti from Wilson Sonsini on behalf of Petitioner, Visa, Inc. With me today is backup counsel Patrick Medley, and we also have a number of representatives from Visa attending via the public link.

JUDGE CASS: Thank you. And for Patent Owner.

MR. WILSON: Douglas Wilson of Armond Wilson, LLP, for Patent Owner Cortex MCP, Inc. And also watching via the link is at least one representative from Cortex.

JUDGE CASS: Thank you. And now we will now begin. Both sides will have some time to present arguments as to all of the related cases being heard today. As far as your presentation goes, Petitioner will proceed first, followed by Patent Owner's response. Petitioner may then use any remaining time for rebuttal to respond to Patent Owner's arguments and then, finally, Patent Owner may use any of its time for surrebuttal responding to Petitioner's rebuttal.

A few reminders before we begin. As I think one or both of you noted, there is a public line for this case. We're not aware of any

confidential information that may be discussed. If that's not the case, please let us know.

When you're arguing, please speak slowly. And if you hear another voice, such as myself or one of the other judges appearing remotely, please stop so that people don't talk over each other. That makes it easier for the court reporter and just makes things run more smoothly.

If either party believes the other party is presenting an improper argument, such as a new argument that was not made in the parties' briefs, please raise that issue during your presentation and do not object at the time and interrupt the other party's presentation. Also, we've received the parties' demonstratives, and I know you've given at least me a set here. It's your choice, you can refer to them by slide number, or we have them all and can project them if you'd like; whatever you prefer.

I'll be keeping time and can give you a warning when you've gone into your rebuttal time if you'd like. Are there any questions from the parties before we begin?

MR. ARGENTI: No, Your Honor.

JUDGE CASS: All right. Let's start with Petitioner then. Would you like to reserve time for rebuttal?

MR. ARGENTI: Yes, Your Honor. You read my mind. I'd like to reserve 15 minutes, please.

JUDGE CASS: All right. I will put 45 minutes on the clock. And are you ready to begin?

MR. ARGENTI: I am.

JUDGE CASS: All right. We will start then.

MR. ARGENTI: Again, my name is Matt Argenti on behalf of Visa. Today, I'm going to be referring to our demonstrative exhibits which have been submitted in each of these IPRs as Exhibit 1058.

Your Honors, the patents challenged in these four IPRs claim systems for managing and verifying credentials. Patent Owner contends that this extends to tokenized payments, but Patent Owner did not invent tokenization, at least as its own prior art shows. Patent Owner also argues that their key contribution to the field was having the credential issuer verify an electronic representation of the credential. But when they point to examples in their specification, it's things like confirming credential information that's included in a user's request or providing additional credential information or providing an image of the credential. We see the same thing in the prior art of record.

Turning to slide 2 now, here we see the grounds of challenge for the 531 patent. We have grounds based on the Oborne reference and grounds based on the combination of Stafford and Purves, and the disputes center on those references. Patent Owner doesn't dispute aspects of the grounds that include the Neafsey reference, or at least not based on the Neafsey reference. There's no dispute, so I won't spend time addressing that one today.

Turning to slide 3 and the 854 patent, we, again, see that the grounds involve the same Oborne, Stafford, Purves, and Neafsey references as in the 531. The four challenged patents here all had similar claims, and they're all related. And the disputed issues in these four IPRs largely overlap, so I plan to focus my discussion on the 531 patent and then briefly

touch on the other patents at the end.

Moving through slides 4 and 5, the grounds for the 859 and 973 patents also rely on those same references.

So turning to slide 6, the four challenged patents share a common specification. It describes generating and verifying officially verifiable electronic representations of credentials, which the patents call OVER Files. These OVER Files can comprise any officially-verifiable electronic credential; that's what the specification says. And it gives examples, like a driver's license, an ID card, or a professional license.

There are three main components or actors in the system that these patents describe. As we see in the figure at the lower left, there's an OVER File Storage Client. We can think of that as a user device for the person with the credential. Then there's an OVER File Generation and Verification Engine. That is the server that generates an OVER File in response to a request from the user. It sends the OVER File to the user, and it responds to requests to verify the OVER File as corresponding to a credential. And, finally, there's the OVER File Third-Party Client. That's the third party that wants the user credential. So a user can use an OVER File to convey some electronic information to the third party, so the third party can then be allowed to reach out to the OVER Engine to get verification of the credential.

If we turn to the next slide, slide 7, we see Claim 1 of the 531 patent, which is generally represented with the claims at issue here. This claim recites the same three components that we just saw in the figure: the OVER Engine, the OVER File Storage Client device, and the OVER File

Third-Party Client verifying device. And it recites the same flow of information that I just discussed: a user requests an OVER File, the OVER Engine provides it to the user, the third party scans information associated with the OVER File from the user's device and sends a verification request to the OVER Engine, and the OVER Engine responds with an authentication message indicating whether the scan corresponds to credential information stored in the OVER Engine.

Now, a key disputed limitation here is Element 1.3 that's underlined in red. It requires generating an OVER File comprising a virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential based on the information associated with the credential of the user. And that gets us to claim construction.

Turning to slide 8, here, we see constructions advanced in our petitions. First, we applied construction of the claimed OVER File that encompasses both a file comprising an image of the credential and a file comprising a token. A token is basically a stand-in for a credit card number or other credential. It's a surrogate for the actual credit card number. For example, it could be a randomized number that a customer can use during a purchase to give to a merchant instead of the actual credit card number.

JUDGE CASS: Now, counsel, as I'm sure you know, in our decision on institution, we stated that an OVER File encompasses a virtual representation of one or more credentials to be used for verification of those credentials. Do you have any issue with that construction?

MR. ARGENTI: Well, so the virtual representation doesn't

need to be used for verification, so I would qualify that a little bit. It's the OVER File and it's actually the scan of the OVER File that's transmitted to the third party, so the OVER File needs to comprise a virtual representation, but there's nothing in the claim that requires that the virtual representation be the thing that's used to verify.

JUDGE CASS: What would be an example of a situation where verification was done without the virtual credential?

MR. ARGENTI: Well, I think exactly as we proposed in our grounds where, in view of the teachings of Purves, there's an image associated with the credential that's provided to the user so that they can keep track of multiple credentials that they have access to at the same time. But that image doesn't need to be what's provided to the third party.

JUDGE CASS: I see. So going to the spec of the patent, so Figure 7 and 8, would those be examples of OVER Files?

MR. ARGENTI: Let me go back to 7 and 8 here, Your Honor. Your Honor, I don't think that this was something that was teed up in the briefing. I understand you have a question. If the written description says these are examples of OVER Files, I'm not going to dispute that; but I don't know offhand whether the written description actually says that.

But what I do know is that the claims aren't limited to the examples in the specification, and they certainly are clear, when they talk about an OVER File that comprises the virtual representation, the OVER File can include other things beyond the virtual representation. And then when you get to the third-party verification, it is based on a scan that's associated with the OVER File. The claims are explicitly written to not

require the virtual representation must be the thing that's used for the third-party verification.

JUDGE MCSHANE: So, Mr. Argenti, this is Sheila McShane, Judge McShane. So, basically, and let me get this right, so your position is that, essentially, verification of the credentials meets the claim language; is that right?

MR. ARGENTI: Verification of the credential -- I think the claim language is verification of an association between the credential and the scan associated with the OVER File. But correct— that one way that that's satisfied is by verifying that the credential, although I want to make sure that we're not getting into a different disputed issue because these claims have a lot of verifications that are written in them. So I believe that the question that Judge Cass had went to what's provided to the third party to be used for the second verification in the claims, which is different than the first verification that's recited when it's talking about generating the OVER File.

JUDGE MCSHANE: What I'm talking about is what's recited on -- this is the 531 patent -- recited in Limitation 1.3. That's the verification I'm talking about.

MR. ARGENTI: Right. Which is a different verification than what Judge Cass had been asking about, and so, to your question, Your Honor, it's a little bit more nuanced than that, and that's what I was going to get into here and then when we discuss the grounds of challenge. Our construction for the "verified by an issuing agency," as we see here on slide 8, was that the issuing agency has verified a virtual representation in an

OVER File as being an official representation of a credential and that is as opposed to just verifying the underlying credential.

However, then Patent Owner didn't dispute this construction, but they came back and pointed to the DMV example in their specification, which we said, well, that is verifying the underlying credential information, you're checking the underlying credential information. So based on Patent Owner's arguments, you can verify the credential as a way of verifying the virtual representation. That's not at odds with the construction here, right, as long as the virtual representation is verified. If the means of doing it is by verifying the credential, which appears to be Patent Owner's argument, then, okay, we see plenty of examples of that in the prior art.

So I think where our petition presented examples in the prior art of verifying the virtual representation that we're directly verifying the virtual representation. Based on Patent Owner's examples, they view the claim as encompassing that forms of verification of the credential can also extend to verifying the virtual representation.

JUDGE MCSHANE: Yes. Well, Patent Owner can speak for themselves in their time, but I thought that in surreply Patent Owner came back and they cite to the spec itself at the time, but they also came back, I think, fairly strongly and said that the verification has to be the verification of the virtual representation, full stop. I mean, I feel like that your contention. If you want to comment on that point. Otherwise, we'll let the Patent Owner speak for themselves.

MR. ARGENTI: I do think that's probably a question that's well directed to Patent Owner. In our view, they say that and, yet, they are

still pointing to examples of verifying the underlying credential information. They have not backed away from their DMV example. They say that is an example of verifying the virtual representation. And, if that's true, we point to the same things in the prior art.

JUDGE MCSHANE: Okay. Thank you.

JUDGE CASS: All right. Counsel, I want to follow-up on this a little bit. So we have the DMV example in the spec, and that's verifying the credential itself. You could also verify the virtual representation. So, a virtual representation could be something like, let's say, a QR code, right.

MR. ARGENTI: A virtual representation could be a QR code. I would agree that the virtual representation could be the QR code. The claims do require that the virtual representation be verified by the issuing agency, so I don't want to disassociate those limitations or act like I'm, you know, picking the claims apart piecemeal; but I would agree that a QR code could be a virtual representation.

JUDGE CASS: Okay. And I think you say, like, an image. Is that another example --

MR. ARGENTI: An image, a QR code. I mean, really, as I'll explain in a few slides, I think the parties agree, the experts agree, that all that is required to be a virtual representation in this context is that it be electronic and it, in some way, be associated with, be tied to and be a stand-in for the underlying credential.

JUDGE CASS: So, if you have, let's say, a bank account number, if you're transmitting that electronically, it's going to be in 1s and 0s, electronic form, does that make it a virtual representation?

MR. ARGENTI: I'm not sure that that's an issue that we've reached in the briefing. I think probably it would be based on the broad view that seems to be agreed on here, but we don't need to go that broad when we're looking at the prior art combination.

JUDGE CASS: Okay. So when we talk about verifying a virtual representation that would include, let's say, a QR code, checking the QR code to see that the QR code actually represents the bank account number.

MR. ARGENTI: Absolutely.

JUDGE CASS: Okay. So, I was trying to go back to the spec, and, obviously, we have the driver's license example, which, I think, as you pointed out, appears to be a verification of the underlying credential. Are there examples in the spec, and I know this is not controlling, but are there examples in the spec of verifying the virtual representation rather than the underlying credential?

MR. ARGENTI: There is bald language in the specification that says you can verify the virtual representation. Beyond that, I am not aware of examples in the spec of how that would be accomplished. Patent Owner has put forth what they say are examples of that, but, to your point, I don't think there's great disclosure of what they meant by that in the specification.

JUDGE CASS: Okay. And just so I'm clear, there appears to be a construction floating around that maybe I should say puts a gloss on your construction here that the verification of the virtual representation can include virtual representation of the underlying credential itself. Is that a

construction that you agree with?

MR. ARGENTI: I think what's important here is that this construction is undisputed. And then what we're doing is looking at Patent Owner's arguments in response to that where they don't dispute the construction. They say here's an example of it. We're saying the examples in the prior art are the same as that construction. I think Patent Owner has tried to frame this as a claim construction issue. I don't agree that it's a claim construction issue, given that they are, at least on their face, saying that this is not a disputed issue.

So, I think asking whether we agree with that construction is really kind of beside the point when Patent Owner themselves are the ones who argue that their example fits within the agreed-upon construction.

JUDGE CASS: Well, if you disagreed with the construction, that might be important. So, I guess maybe I should ask it that way: do you have any disagreement with Patent Owner's construction?

MR. ARGENTI: We have not taken a position on whether we agree or disagree with that construction, nor do we need to. All we have pointed out is that the prior art discloses what they are saying the claims encompass.

JUDGE CASS: All right. Thank you.

MR. ARGENTI: So turning to slide 9 and the prior art, first, the Oborne reference. Oborne is a Visa prior art reference describing a tokenized payment system. It provides tokens corresponding to a user's accounts, like bank accounts or credit cards. A user requests a token. The server generates a token and links it to the user's payment account and sends

the token to the user to be given to a merchant when making a purchase. The merchant sends the token back to the token server for verification that it corresponds to the account valid for the purchase.

And Oborne says the token server can be operated by the issuer of the financial account that's linked to the token, so a bank or a credit card company is the one giving the user a token that corresponds to the account held with that institution. Oborne also says the tokens can be pre-funded, meaning funds are exclusively allocated to that particular token. So what Oborne says is that not only can the bank or credit card company create the token that corresponds to one of their accounts, but there can be verification, Oborne uses the word assurance, of a particular amount of funds available for that token.

Turning to the next reference on slide 10, Stafford. As we see in the abstract, Stafford describes a system for storing, and validating, and disseminating credential information. Instead of calling them OVER Files or tokens, Stafford calls its credential stand-ins “key signatures” because they are provided to a third party and used to unlock access to the confidential information.

In Figure 2, Stafford describes the process of generating the key signatures and providing them to a user. The credential information is encrypted with a particular one-time pad key, which is then combined with another key and used to generate a hash value, which is the key signature. The key signature is sent to the user.

Then, in Figure 3, the user can give the key signature to a third party in lieu of credential information or in addition to credential

information. The third party sends the key signature to the system server and is given the credential information in return, thereby authenticating that the key signature corresponds to the credential information stored at the server.

Turning to slide 11, like Oborne, Stafford, and the challenged patents, Purves describes a system for managing credentials. Purves calls this a virtual wallet, which you can store a user's payment accounts, so bank accounts, credit cards, gift cards, and other forms of payment can be stored in the payment and used for transactions. Purves explains that the wallet entry can display helpful information related to the credential, like a nickname, the brand of the card, or an image of the card. And Purves also explains that, in some circumstances, the wallet system can generate the credential itself.

Now, excuse me, Your Honors. I'm going to skip slide 12 and Neafsey because there are really no disputes that center on the Neafsey reference. So turning to slide 13 and the Oborne combinations. As we explained in the 531 Petition, many of the challenged claims are obvious in view of Oborne alone. For certain dependent claims, we also explained that a person of ordinary skill would have been motivated to combine Purves's teachings regarding credential generation and providing credential images to give a simple visual indication of the credentials available to the user.

So turning to the disputed issues, starting on slide 14. Patent Owner argues that Oborne does not satisfy the requirement for a virtual representation that's been verified by an issuing agency. But as we've explained, Oborne teaches or suggests this in multiple ways. First, Oborne

discloses that the issuer of the underlying financial account can also be the one generating the token, so that is a verified virtual representation. The token is verified because it is coming from the bank that also manages the account. Consistent with that, as we see here in the top right of slide 14, Oborne says that the token can be linked to the account by servers at the issuer. So the issuer knows that that linkage exists. By providing the token, the bank is verifying it as official and connected to the underlying account. Otherwise, they wouldn't issue it.

Now, in slide 15 --

JUDGE SZPONDOWSKI: I'm sorry. Is that an inherency argument? Because it kind of sounds like an inherency argument.

MR. ARGENTI: No, it's not an inherency argument. It's the described generation of the token by the bank that is the verification. It's not an inherency argument where we're saying, well, that must necessarily happen behind the scenes. It's the generation itself that is the verification and that's specific --

JUDGE SZPONDOWSKI: And where does Oborne explicitly say that the token is verified by the issuer?

MR. ARGENTI: It doesn't use those words, but the plain disclosure that the issuer of the financial account can be the one generating the token is the explicit disclosure that we're relying on. Patent Owner is placing --

JUDGE SZPONDOWSKI: And what disclosure in Oborne and what paragraphs do you think give you the strongest support with that?

MR. ARGENTI: Certainly, the paragraphs cited here on slide

14, which is disclosing that the issuer of the financial account can also be the one generating the token, as well as the disclosure of the linkage between the two. We may have additional disclosures cited in our briefing. I certainly wouldn't want to remove that from the analysis. But I think this disclosure here is sufficient for the interpretation that the plain disclosure of Oborne disclosed a verification.

JUDGE CASS: This is Judge Cass. Let me ask a couple of questions to follow-up on that. So the bank generates the token but has a lot of confidence in its software, so it doesn't have an explicit step where it goes back and checks, you know, does a second check to make sure it did the right thing. Would that be a verification according to Limitation 1.3?

MR. ARGENTI: Yes, it would, Your Honor. It would.

JUDGE CASS: And why is that?

MR. ARGENTI: So we addressed that other circumstance, like in our other reasons that Oborne teaches or suggests this. But just the generation itself is, to the user, a verification that the token is linked to the account. The claims don't require to whom the verification is -- they don't require a verification message at all. Patent Owner's expert conceded that during his deposition. So they also don't require a particular party or entity be the one for whom this is verified. The generation by the bank is a verification for the user.

JUDGE CASS: So if that's the case, I mean, what's the purpose of including this “has been verified” language? Couldn't the claim just say a virtual representation of the credential that was, you know, issued by an issuing agency? What additional meaning does the word verification have?

MR. ARGENTI: I think that's probably a better question for Patent Owner in terms of what's the purpose of it. But I will say that if the claim recited generated by an issuing agency, that would be much narrower from the certain perspective of the current claims don't require any -- it's the OVER Engine that's generating. It doesn't require that the issuing agency be the one doing the generating, so that would be a narrowing limitation from that perspective.

I think, here, it's really a special circumstance in Oborne where Oborne is talking about the bank being the one generating the token. We're not contending that any and all generations of tokens or virtual credentials satisfy this limitation. We're not reading the limitation out of the claim. We're pointing to a particular disclosure in this prior art reference that satisfies it.

JUDGE CASS: So, in other words, I mean, by having the issuing agency, having the issuing agency involved is kind of what Limitation 1.3 is really directed to, that you couldn't have just some other party generate a representation without involvement of the issuing agency because then you might not know, you might not have as much confidence that it's accurate.

MR. ARGENTI: That's exactly right, Your Honor. The claim requires the involvement of an issuing agency. It does not require that the issuing agency be the one generating the token. But what we're pointing to in Oborne, where it is the issuing agency that generates the tokens, that's one way that this limitation is satisfied.

JUDGE CASS: All right. I apologize, but I'm going to ask you

a question about the patent again, so you might need to get your notebook.

MR. ARGENTI: Okay.

JUDGE CASS: I'm looking at, just happen to be looking at the 489 case. But, in that case, paragraph 47, there's what appears to be a code, XML, listing of what I think is the token, and there's various different, I take it, pieces of data in there, including client details, client fingerprint, some other stuff, a bunch of other stuff. I guess my first question is: is that the token in Oborne? My second question is what would be the virtual representation in there?

MR. ARGENTI: So just to be clear, we're looking at paragraph 47 of Oborne and, in particular, the example token data structure.

JUDGE CASS: Yes.

MR. ARGENTI: So to your question, yes, this is one example of a token in Oborne, and it's something that we cited and that both parties have had arguments about. In terms of what is the virtual representation, I think it's the entire token data structure or whatever -- the entire token data structure. It's not just the account number or anything like that. The token itself is the virtual representation of the underlying encounter.

JUDGE CASS: Okay. So then your position is, by the process of having the issuer generate this XML token data structure, that would be the verification in the step 1.3?

MR. ARGENTI: Right.

JUDGE CASS: All right. Thank you.

MR. ARGENTI: So, now, turning to slide 15, and, as if the plain disclosure we just discussed wasn't enough, Patent Owner's arguments

confirm that Oborne satisfies the verification requirement. As we've already discussed, they point to a DMV example in their Patent Owner response. Oborne discloses, essentially, the same thing. It says that the token issuer can first obtain assurance that funds from the funding source have been uniquely allocated for the token. And Oborne also talks about contacting the pay card issuer for confirmation of the pay card information. That is no different than their DMV example of reaching out to the DMV to obtain information for the OVER File. This is funding and account information for the token in Oborne.

Turning to slide 16, apart from Oborne's express disclosure of this limitation, the petition also explained that it would have been obvious. As our expert, Dr. Shamos, testified, the bank or other account issuers would logically verify that the token accurately represented the credential before providing it to a customer. So this goes to the question about inherency. If there's an underlying separate step that's required, that's what we're saying is obvious. I don't think the claims do require that, but that would have been obvious in view of Oborne.

As Dr. Shamos explained, it would be a problem if tokens were out there in the marketplace that had not been linked to a payment account, particularly where the bank was the one that issued the token from one of its own customer's accounts. Verifying that the token was linked to the credential would, of course, increase confidence among customers, merchants, and even the bank that the token legitimately represented the credential.

Think about the alternative. Patent Owner is proposing that

Oborne be interpreted to suggest that a bank would get a request from a customer for a token linked to an account at the bank, and the bank would issue the token without ever confirming that the account actually existed. That's an unreasonable interpretation of Oborne, and it certainly doesn't undermine our obviousness showing. In fact, as we see here on slide 16, Patent Owner's expert conceded that he had not considered whether it would be desirable for Oborne to provide tokens that had been properly linked to a payment account. And when asked, he admitted that might possibly be true. Of course it's true. Patent Owner has no legitimate argument that it isn't.

JUDGE MCSHANE: Mr. Argenti, on this issue, looking at the testimony, there is the concept that, you know, it's a routine step and it's logical and so on, and Patent Owner made arguments that what his testimony really represents is that the expert is employing common sense. What do you have to say about that?

MR. ARGENTI: Well, as we say in our briefing, this is not a common sense analysis. The Federal Circuit has a particular framework for a common sense analysis. We did not make a common sense assertion here. Those are not words that you will find in the expert testimony or in the petition.

So there's very little support for Patent Owner's argument that arguing something is routine or logical somehow transforms it into a common sense analysis that requires the Federal Circuit framework. The Federal Circuit certainly has not said that. When you look at the two previous Board cases that they're citing for this sleight of hand, it doesn't hold up. In those cases, there were multiple steps interrelated and dependent

on each other and multiple modifications of the prior art to arrive at the claimed invention.

That's not at all what we're doing here. Our obviousness theory is rooted in Oborne's disclosure, the things that Oborne says. Oborne says the bank can issue a token. Oborne says there can be linkage at the financial institution associating the token with an account.

All Dr. Shamos is saying is, yes, it would make sense to do that before you're issuing the token for the user. The bank has a lot of reasons to make sure that the underlying account actually exists and is linked to the token. So this is very different. This is not a common sense analysis.

JUDGE MCSHANE: Okay.

JUDGE CASS: So let me ask another question just to make sure I understand in your obviousness argument, you know, what is the verification that's being done here. So if we take, as an example, this XML token in paragraph 47 of the patents of Oborne, in your obviousness analysis, you know, what is it that you're saying is obvious, would be obvious to do here? Is it go through and verify all the information in the token? Is it verify the account number? You know, what specifically --

MR. ARGENTI: So we can focus on the account number in particular, right. The user sends a request for a token. Say I want a token for my bank account. Here's the account number. Lacking this obvious limitation, the bank would just issue a token for that account number without ever actually looking up or confirming that that is an account number at the bank. So that's what we're saying is obvious is that not just creating the linkage but also confirming that that's an actual account number and then

confirming that this token is now linked with this account number.

JUDGE CASS: So wouldn't that be verification of the underlying credential and not verification of the virtual representation?

MR. ARGENTI: So they're related to each other, but they are distinct from each other. You could get the request from the user and verify the account. What we're saying is that it would be obvious to confirm the linkage between the token and the account, not just confirming that the account exists but then confirming that this linkage exists, which is right there in the example token.

So, again, this is not a huge link for obviousness. It's supported by the disclosure in Oborne.

JUDGE CASS: So it wouldn't be going to the account and saying is this a valid account in general and is there money in it. It would be looking at the, for instance, looking at the token file, seeing the data that's in the token file, putting that into a database, seeing if it returns the account, et cetera.

MR. ARGENTI: It would be both, but, yes, certainly, we're arguing that it would be obvious to verify the linkage between the token and the account before providing the token to the user.

JUDGE CASS: All right. Thank you.

MR. ARGENTI: So if we turn to slide 17, the only other argument that Patent Owner has with respect to Oborne and the independent claims of the 531 patent is that we failed to identify with particularity what aspect we rely on for the OVER Engine claim element. They argued in their Patent Owner Response that we relied on Oborne's PPT system generally,

but I want to read a quote from their Preliminary Response: "Again and again, the petition points to Oborne's token server to satisfy the OVER Engine claim limitations." They knew exactly what we were relying on at that point.

And when we pointed out that we cited the token server, rather than the claim and merchant portions of the PPT, then they came back and said that we relied on the token database for one aspect of the claims, not the token server. But Oborne describes that the token server and the token database can be integrated together, for example in Figure 15 and related written description, like paragraph 152.

JUDGE MCSHANE: So on this one, Mr. Argenti, so just looking at Figure 4, okay, we just looked at Figure 4. When you're doing the mapping, right, what are you mapping in this Figure 4 to the OVER engine specifically?

MR. ARGENTI: Sorry, Your Honor. Let me just flip to Figure 4. I think it's starting off on the wrong foot to say that this is the only mapping that we have. Certainly, we have been clear that we are mapping to the token server; and, certainly, we cite and rely on Figure 4. But, again, we rely on other disclosure from Oborne saying that these are not all distinct components from each other. They can be. They don't have to be. They can be combined. And, certainly, there is disclosure that we have cited of the token server and the token database being combined.

So we are relying on the token server. We also cited the token database functionality with respect to, I believe it's Claim 1.6. We don't dispute that.

JUDGE MCSHANE: All right. Thank you.

JUDGE CASS: So, in other words, it would be within your position that the OVER generation engine is the token server in combination with the database, whether those are the same thing or separate things.

MR. ARGENTI: Agree, except to the extent that Patent Owner argues they can't be separate and fall within the scope of the claims, I don't think they've really teed that up in their briefing. So I don't want to fall too hard into a concession here at oral argument, but, certainly, we're citing both of those. They're explicitly cited in the petition.

JUDGE CASS: All right. Thank you.

MR. ARGENTI: Thank you. So that is the discussion of Oborne and Claim 1. Now, I'm mindful of the clock and that my time is rapidly ticking. You've had a lot of great questions. Does the Board have any guidance as to whether they would prefer that I move on to the dependent claims for Oborne or the Stafford ground?

JUDGE CASS: I'll just tell you you've got seven and a half minutes, and I don't have a preference.

MR. ARGENTI: Okay. I'm going to keep moving through then and we'll see what we can fit in here. For Dependent Claim 2 on slide 18 of the Oborne grounds, this claim recites a second OVER file for use on a second device of the user that's invalid for use on the first user device. There's no dispute at this point that Oborne discloses that the user can have multiple devices. Oborne also teaches device fingerprinting for security, which Dr. Shamos explains is a technique that ties particular credentials to particular devices. As seen here, that includes an example in Oborne where

the token file includes a device MAC address.

So if we turn to slide 19, as Dr. Shamos explains, in view of Oborne's disclosure of multiple user devices and client fingerprinting, it would have been obvious to a POSA to use the device fingerprinting for device-specific tokens invalid for use on other user devices. In particular, Oborne discloses an interface for creating new tokens where the user can select the activated devices for that token. If the token was automatically valid for all user devices, as Patent Owner argues, that configuration in Oborne doesn't make sense.

If we turn to slide 20 and Dependent Claim 7 and 20 --

JUDGE CASS: Before we move on from Claim 2, so Claim 2 requires that the official representation or the second OVER File is invalid for the first OVER File. Using the XML example in Oborne that we looked at, how would that work? If somebody tried to use the token for, let's say, an iPhone but they were using an iPad, or I tried to use the one from my iPhone but I was using my iPad and that had a different device fingerprint than -- I take it that wouldn't work.

MR. ARGENTI: That's right --

JUDGE CASS: How would that actually get implemented?

MR. ARGENTI: Dr. Shamos explains that's what client fingerprinting is, that's what device fingerprinting is, is that, when you have a device ID, like a MAC address that's built into the token structure, then the request to use the token has to be coming from that device or else it wouldn't work.

JUDGE CASS: And when you say it wouldn't work, does that

happen -- how does that happen? The device sends, is the device rejected, or would the third-party verification apparatus reject it? At what point would that happen?

MR. ARGENTI: I don't think Oborne is specific on the details of the operation, so I don't think it's limited to one of those options. I think, practically, it would more likely be coming on the server side, potentially on the user side. It's hard to envision it happening with a third-party device, but I'm not a software engineer, so maybe it could be.

JUDGE CASS: Okay. Thanks.

JUDGE SZPONDOWSKI: I have a question about that, as well. Can you just clarify, because I'm just not following, how the fingerprinting shows that it's invalid for use in the first OVER File Client or Storage Client device?

MR. ARGENTI: So the fingerprinting identifies the devices on which it is valid for use; and, therefore, it is implicit that it is invalid for use on other devices.

JUDGE SZPONDOWSKI: I would be using the same fingerprint on my iPhone versus my iPad, wouldn't I?

MR. ARGENTI: Not when the fingerprint is specific to a device ID, such as a MAC address.

JUDGE SZPONDOWSKI: Okay. Thank you.

MR. ARGENTI: So slide 20, Claim 7 and 20, here, the claims require a status indicator indicating an invalid credential and credential information that indicates a reason for an invalid credential. As we pointed out, there are numerous examples of this limitation in Oborne, including

sending one type of rejection message for insufficient funds and a different message for exceeding the maximum number of allowed transaction attempts. Moreover, as Dr. Shamos explained, these elements in this claim limitation were commonplace and would have been readily apparent in view of Oborne's teachings, as well as the state of the art.

Patent Owner has no meaningful response, other than to say Dr. Shamos's testimony is conclusory and uncorroborated, but that's not true. Unlike Dr. Malek, Dr. Shamos cites numerous examples corroborating his testimony about the state of the art and impose his understanding of Oborne.

Turning to the next slide, 21, in Claims 8 and 29, this goes to the remote storage requirement. As we explained in our petition, Oborne expressly discloses use of remote storage facilities for its PPT system. We see that in paragraph 133. Patent Owner argues that only applies to program components and not databases or data components. That's a false distinction. Oborne talks repeatedly about use of distributed databases consistent with this remote storage disclosure.

JUDGE MCSHANE: Mr. Argenti, I think Patent Owner also asserts that you're citing to paragraph 150 is new in reply. What's your response to that?

MR. ARGENTI: This is not a paragraph that we cited for this claim in the petition. This is in response to their argument. They said that we, the Petitioner, was misinterpreting paragraph 133. In response to that, to rebut that argument, we cited plenty of other aspects of Oborne that are entirely consistent with our interpretation of paragraph 133.

JUDGE MCSHANE: All right. Thank you.

MR. ARGENTI: So turning to the next slide, slide 22, and Dependent Claims 12 and 13 where Patent Owner argues that our mapping is inconsistent with Claim 11, all of these claims recite a credential identifier. And for that, they say that we rely on Oborne's account number for Claim 11 but Oborne's token identifier for Claim 12. The issue here is pretty simple. We cited both the account number and the token identifier with respect to Claim 11, so our mapping in Claims 12 and 13 is not inconsistent.

Turning to slide 23, Independent Claim 19, this requires that the OVER File comprises a credential image. Here, we refer to Purves. We brought Purves in for that aspect of the claim. Their arguments here are repeats of the security arguments and other arguments that they make with respect to the Stafford ground. They can be rejected for the same reasons. Hopefully, I have time to get to that.

JUDGE CASS: Yes. You have about 30 seconds before you start going into your rebuttal time.

MR. ARGENTI: Understood, Your Honor. Thanks. I think I probably will go into my rebuttal time just a little bit. For slide 24 and Dependent Claim 23 and some others that depend from it, Claim 23 recites that the OVER Engine requests the credential from the issuing agency. Their argument here is that we did not provide a motivation to do this, but, as we pointed out in our reply, this aspect of Purves that we are relying on is part of what Purves describes in terms of generating and adding a credential to the wallet, in particular adding it to the wallet. That's what we addressed in the motivation. We explicitly referenced Claim 23 in our motivation, so

there's no credible argument that we did not include this in our rationale to combine.

Now, turning to slide 25 and the combination of Stafford and Purves, as we've explained in the briefing, this combination brings in Purves' teachings regarding representative credential images that Purves describes as a way to help users identify the key signatures to be given to a third party, and it brings in its teachings regarding use of QR codes as a way to convey the key signatures in Stafford and to the third party, which would increase convenience and reliability.

We can turn to slide 26. Specifically, when addressing Element 1.3 of Claim 1, we explain that in the combination of Stafford and Purves, the OVER File would include the key signatures encoded in QR format, as well as an issuer-verified image that represents the credential. Again, this will help the user manage the key signatures and identify which one they want to use, which one corresponds to particular credential information, and also provides a convenient means to pass the key signatures along to a third party using that QR code.

So turning to slide 27, looking at the key signatures, the key signatures on their own satisfy Element 1.3, which is disputed here. These are a virtual representation of the credential. The parties agree that virtual in this context just means electronic or digital, and the experts also agree, as we see on this slide, that the key signatures represent the user's credential documents. We see that in Dr. Malek's testimony, as well as Dr. Shamos's analogy to a coat check ticket. So there's no dispute about the virtual representation requirement.

The key signatures are also based on information associated with the credential. They are generated as a result of a request to prepare the credential information for release, and they are specifically tied to that credential information. Plus, the key signatures are computed from the one-time pad key that is used to encrypt the credential information. That one-time pad is information associated with the credential because it's what's used to encrypt and decrypt it, and the key signature is based on the one-time pad.

Finally, based on Patent Owner's DMV example that we talked about for Oborne, the key signatures are verified by the credentials-issuing agency because Stafford teaches verifying the underlying credential information. So Stafford on its own is known to satisfy Element 1.3, but then we get to Purves in the combination.

So we can turn to slide 28. There's no dispute that the images Purves teaches are virtual representations verified by the issuer as official representations, and they are, of course, based on information associated with the credential because they are based on the credential itself, regardless of whether the image is a generic representation of the image or an actual image of the credential. So Patent Owner's arguments attacking Stafford is lacking that and failed to address the grounds combination. And looking at Patent Owner's arguments that Purves comes up short—they're easily dismissed.

Turning to slide 29, first Patent Owner argues that Purves does not disclose storing the credential representation on a user device. Well, again, there's no dispute that Stafford and the ground or the combination

satisfies this. And, regardless, Patent Owner mischaracterizes Purves, which does teach storage. Dr. Malek conceded that it has transient storage. It's admitted. It has web page form to the user's device. It's stored in a RAM for display to the user. Patent Owner has never raised any argument why that wouldn't be enough to satisfy the claims.

Turning to slide 30, Patent Owner argues that Purves somehow fails to satisfy Element 1.3 because the reference doesn't disclose using card images or verification. But, again, this goes to the two verifications in the claims that we talked about earlier. That argument is based on the second verification, not the first verification. So we don't need to use the card images to verify the OVER File with the third party. All we need to do is have verified card images included in the OVER File, and that's in our combination and they've never disputed that.

So turning to slide 31 and the disputed issues of the rationale to combine. They argue that Purves' electronic wallet teachings don't make sense to combine with Stafford. Patent Owner's argument presumes that the credentials are released at the same time that the key signatures are generated. They say, well, if you're releasing the key signatures at the time you acquire them, why do you need to keep track of them. But that's not what Stafford teaches. Remember, Stafford discloses key signature generation and credential release as two separate processes, Figure 2 and Figure 3. So the user receives the key signatures, but they aren't used until the user gives them to a third party to be exchanged for the credential. And Stafford says that the user can have multiple sets of key signatures at the same time, so it makes perfect sense to give the user a tool to keep them

straight.

Turning to slide 32, Patent Owner argues that the one-time use key signatures in Stafford don't make sense to combine with the teachings of --

JUDGE SZPONDOWSKI: Mr. Argenti.

MR. ARGENTI: Yes.

JUDGE SZPONDOWSKI: I'm sorry. Could you just explain a little more what this combination looks like? You want to incorporate Purves' credential images into Stafford's system when Stafford gave a hash value that's then mapped to the virtual credential representation of the stored credential, and I guess I'm just struggling with why a person of ordinary skill in the art would be motivated to add those images to Stafford's system and what that looks like.

MR. ARGENTI: In terms of what it looks like, I mean, the best -- we didn't design a particular embodiment of how this would be combined, but I can give you kind of an abstract representation if we flip back to slide 26 where we have the keypad signature that's encoded in QR code format, as well as the card. This is the information that we are saying would be included in the OVER File that's sent to the user. As opposed to just a key signature that's a string of characters, we're encoding the key signature as a QR code and we're adding an image to the OVER File that's going to help the user keep that straight.

In terms of the motivation to do it, we have identified, as I just mentioned, that the image would help the user keep this straight when the user has multiple key signature OVER Files for multiple different packages

of information, which is consistent with what Stafford says. And it is going to give the user a convenient way to communicate the key signatures to the third party with the QR code scan. As Dr. Shamos explains, if you're doing this manually by writing down numbers or having the third party copy something off a screen that's prone to error, it's more labor intensive. The QR code is an easy scan that was widely used at this time. Neither one of those beneficial motivations is disputed. They have no response that that wouldn't happen in this combination. Their arguments about why the POSA wouldn't do it go to the security issues, to the disparate relationship purportedly between these references. So they're not arguing that those would not be helpful modifications.

I'm going to try and save myself five minutes, Your Honor, so I will get through -- given that I've touched on the rationale and the arguments against the rationale right there, they're incorrect. As we see on slide 31, 32, which is where we address that these references, Stafford and Purves, are not so different. There's no big distinction between an electronic wallet and one-time use key signatures. Purves discloses storing things in the wallet that are used one time, whereas Stafford discloses applications that are entirely consistent with what Purves is talking about, whether it's e-commerce purchases of goods or services. So there's quite a bit of overlap between these references.

As to the security arguments that Patent Owner has raised, none of them hold up. Both references teach encrypted communications, which, basically, gets rid of all of their security concerns. If you're encrypting the package of OVER File information that's sent, the image, as well as the key

signature, whether in QR code format or not, that's going to be a secure form of transmission that's consistent with what's going on in both Stafford and Purves. There's certainly nothing in Stafford that indicates only the key signatures and just the key signatures can be transmitted to the user. In fact, when the key signature is used to unlock the credential information, the credential information is provided to the third party, including by transmission to the third party. So there is nothing in Stafford that's consistent with Patent Owner's argument that, whoa, you can't send anything other than the key signature, that's a big safety breach.

So I think that can conclude the Stafford and Purves discussion. Unless there are any other questions, we can jump to slide 37, 38, 39. Essentially, we have tables here listing how these issues for the 531 patent match up to the disputed issues in the other patents. They entirely overlap. They don't have arguments for the other patents that are unique beyond what we just discussed, except for, if we turn to slide 40, Claims 19 and 21 of the 859 patent --

JUDGE CASS: I'll just let you know you have about five minutes left of your rebuttal.

MR. ARGENTI: Thank you, Your Honor. I will briefly point out their argument that we didn't present argument on those claims in the petition is not true. We identified them with particularity in the grounds. We also, as we have here on this slide, explicitly said in the petition that Claims 19 and 21 have the same content as Claim 2 of that patent. We provided the same, the detailed argument for slide 2 -- Claim 2. I'm rushing. And then our expert, Dr. Shamos, confirms that the same analysis applies,

but you don't even need to turn to Dr. Shamos's analysis when we have assertions in the petition that all three of these claims are the same, they provided their substantive rebuttal to this issue on the merits of the prior art in their surreply, so there's really no valid argument that we didn't address it in the petition. Thank you.

JUDGE CASS: All right. Thank you, counsel. You have four minutes remaining in your rebuttal time. All right. Counsel for Patent Owner, would you like to reserve time for rebuttal?

MR. WILSON: I'd like to reserve five minutes.

JUDGE CASS: Five minutes. Okay. Get that set up here. All right. So are you ready to begin?

MR. WILSON: I'm ready, Your Honor.

JUDGE CASS: All right. You may begin.

MR. WILSON: All right. Thank you, Your Honors. I'm going to jump right in, and I'm going to start on slide 3 on my demonstratives. And what I plan to cover this now-afternoon, at least for those of us in Denver, are the issues that I think are simplest and cleanest for the Board to simply reject all of the Oborne and Stafford grounds. So I won't be going through all the dependent claims, for example, but, if Your Honors have questions, I'm happy to answer them. And if not, we'll just rest on our briefing for those claims.

So I'm going to jump right in with the first issue on slide 3, which is that Visa failed to show any art meets Visa's construction of issuing-agency verification. Now, if we look at slide 4, what we have on slide 4 is the 531 Petition argument, Visa's argument, on claim construction.

I think I heard Mr. Argenti say earlier that this is not a claim construction issue; and, yet, that is exactly how the Petition tees it up. It is this is in the claim construction section and, looking at the middle of the paragraph there on slide 4, they say, during prosecution, applicant argued that this phrase requires that the issuing agency verified that the virtual representation is an official representation of the credential. Accordingly, the petition construes this phrase to require that an issuing agency have verified a virtual representation in an OVER File as being an official representation credential. That's their Petition construction.

Now, as we've heard, they are abandoning that in reply, but this is the Petition. If we turn to slide 5, we're going to see there's a reason they took that position, and that's because, on slide 5, you'll see claim 1 of the 531 patent, but every challenged claim has this same language. It's a virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential. That's the actual claim language. Their construction just mimics the words of the claim. That's not something you can run away from. That's not something you even need to construe. It is literally the words of the claim.

So turning to slide 6, when Visa comes back in reply and says Patent Owner concedes that something less than this can satisfy the claim, we can't. The claim language is what the claim language is. We can't change the words of the claim any more than Petitioner can, and so we can't say, hey, the claims don't actually require this. They do. And aside from that, we didn't say that. If we look at slide 6 and the language from Visa's reply brief, it says Patent Owner argues that an example of the specification

corresponds to this limitation. In this example, the OVER Engine checks the driver's license number against the DMV's database. The database's response includes additional information, e.g. a name and address and credential image, and indicates the validity of the requested credential. Patent Owner, thus, admits that a virtual representation of the credential may be verified by an issuing agency by checking credential data against an issuing-agency database.

We admitted no such thing, first of all. That example involves actual verification of the virtual representation, as I'll point out momentarily. And when it says the validity of the requested credential in that quote, the requested credential there, as we'll see, is, in fact, an OVER File. So what it's indicating is the validity of the OVER File. But the column 6 in the 531 patent makes that abundantly clear, as I'll show you in a moment.

But aside from the fact that this is factually incorrect, it is legally irrelevant. We can't change the words of the claim. They say what they say, and Visa has to show what the claims say, not what it says we contend.

Now, turning to slide 7 --

JUDGE MCSHANE: So, counsel, on this point, okay, just to be clear, you know, the Petitioner would say you admitted this, you're saying, no, you didn't admit this, and you're saying that just doing this verification cannot in its step, step 1.3, it cannot be just checking the credential data; is that your position?

MR. WILSON: That is our position, yes, that the words of the claim say that the virtual representation must be verified by an issuing

agency and that must happen for the claim to be satisfied. Checking underlying credential data is insufficient.

So looking at slide 7, this is column 6 from the 531 patent, but, as counsel for Visa articulated, all the specifications are the same. This language is in every patent. You can see on the first paragraph we're discussing this example, and the highlighted language there in the top paragraph says the application gateway may request 126 generation of the OVER File. So let me stop right there. What's being requested is generation of an OVER File. That's the requested credential.

It goes on to say verification of the generated OVER File credential. So what's it asking for? Two things: generate an OVER File and verify the generated OVER File credential. It's asking for the same two things that the claim says. And when we look down at the bottom, we can confirm that that, in fact, happens. It says the issuing agency may also provide a status indicator for the generated OVER File credential.

So, again, not only did it say it was verifying the requested credential, which is the OVER File, it also provides this additional example where the issuing agency provides a status indicator for the generated OVER File credential. These are examples of verifying the OVER File, which contains the virtual representation.

And if I may add, because I think this will come up later, if you look in that bottom quoted portion on slide 7, just above the highlighted portion it says, in some embodiments, the OVER File may be generated by the issuing agency database 130 and sent to the OVER File database 128 for storage and distribution to the user device. Here, the OVER File in this

example is being generated by the issuing agency, and guess what? It still provides a status indicator for the generated OVER File credential. So there's no question generation and verification are two distinct steps.

JUDGE CASS: So, counsel, what was the example of the status indicator here?

MR. WILSON: The status indicator would be -- it could just be a true or false bit, right, or it could be a valid or invalid, anything like that that says this OVER File is a valid representation of the underlying credential because, as the patent discusses elsewhere, for example, the OVER File can expire, right. And if that expires, it just changed to invalid. Now, all of a sudden, it's no longer verified. And so any indication by the issuing agency that the OVER File is a valid representation of the underlying credential would suffice.

JUDGE CASS: And, counsel, I'm not sure if you're going to get to this, so, in your Patent Owner response, you did cite this driver's license example in the patent, which does seem to suggest that what's being verified in that example is the driver's license. Is that an example of the verification step of Limitation 1.3?

MR. WILSON: So the passage, which, by the way, is at page 12 of the Patent Owner response in the 531 patent, the 486 IPR, that passage says the issuing agency database may respond by indicating the validity of the requested credential. The requested credential here is the OVER File, as we just saw from the top of column 6. On slide 7, it says the application gateway may request generation of an OVER File and verification of the generated OVER File credential. So that language referring to the validity

of the requested credential is the OVER File, the validity of the OVER File.

Now, whether you agree with that interpretation or not, column 6 is specifically describing verification of the OVER File, as we just saw. So whether you like this passage or whether you would refer to the bottom of column 6 and the status indicator or the top of column 6 where it says it's explicitly requesting verification of the generated OVER File credential, whichever of those you choose, the point is this is an example of two things: generation of an OVER File and verification of the OVER File. So whether you agree or disagree that the requested credential there in the passage quoted on page 12 is the OVER File, the point was, in this example, an OVER File is verified and column 6 is abundantly clear about that.

JUDGE CASS: So let me try to understand this driver's license example better. So, here, in this example, the entity that's generated the OVER File, is that the DMV or is that some other entity?

MR. WILSON: So it can be either one and, in fact, at the bottom of column 6, it's actually the DMV, right. The portion that shows up on slide 7 that I quoted to you earlier, it's actually the DMV that's providing it.

JUDGE CASS: Okay. So then it says in column 6 that the OVER File database may contact the state DMV or provide the driver's license identification number to the issuing agency database. And then it says the issuing agency database may respond to indicate the validity of the requested credential containment with the driver's license identification number. So it's a little unclear to me whether -- when I first read this, this suggested to me that it was providing the driver's license number and it was

then indicating the validity of that number and then providing information linked to that number, such as the person's name, address, et cetera. You say that's not what's happening here?

MR. WILSON: What I'm saying is, when it says our interpretation of this passage is, when it says indicating the validity of the requested credential, we understand that to be referring to the requested OVER File credential because, earlier in column 6, it says we're requesting an OVER File and verification of that OVER File credential.

JUDGE CASS: Why is it saying to provide the driver's license identification number?

MR. WILSON: Because the OVER File contains the driver's license number.

JUDGE CASS: But what it's verifying is the number, right, not the virtual representation of the number; isn't that true? I mean, I guess I'm not seeing -- what it seems here to be saying is that it's verifying the number.

MR. WILSON: I disagree, Your Honor. I think it's referring to the requested credential, which is the OVER File. But whether you agree or disagree, in column 6, it is verifying an OVER File, and you can see that down here at lines 59 through 61 where it says the issuing agency may also provide a status indicator for the generated OVER File credential. It is plainly providing a verification of the OVER File credential.

So whether you agree or disagree with the portion that we quoted, column 6 is an example of a clear disclosure of verification of an OVER File credential.

JUDGE CASS: Could OVER File credential, could that mean a

credential that is stored in the OVER File, such as a driver's license number?

MR. WILSON: So if we take a look at column 6 and my references are to the 531 patent, but, again, this is in every other patent just in a slightly different citation. But column 6, lines 18 through 20, it says the application gateway may request 126 generation of an OVER File and verification of the generated OVER File credential. It is requesting generation and verification of the OVER File credential. So when it provides a status indicator, that's an indicator of the validity of that generated OVER File credential, not some underlying credential.

JUDGE CASS: Okay. Are there other specific examples in the patent at issue here, other than this driver's license example, that would help us better understand what's being verified is the OVER File and not a credential in the OVER File?

MR. WILSON: I'm not aware of any, Your Honors.

JUDGE CASS: All right. Okay. Thank you.

MR. WILSON: But for the point that Your Honor asked about earlier about the inclusion of the driver's license, if you look at column 12, again, referring to the 531 patent, starting at line 48, it says, as shown in Figure 9, the credential display 600 may comprise text sections and, again, it uses the DMV example. And if you look at line 57, it says text section C, 610, may be configured to display a driver's license identification number. And this is a display of an OVER File. So the OVER File contains a driver's license number, at least in the example in the specification, if that makes sense.

JUDGE CASS: Okay. Thank you.

MR. WILSON: Okay. So turning to slide 8, I now want to jump to Oborne and the fact that these details show that Oborne taught issuing-agency verification of an alleged OVER file.

So turning to slide 9, as I think I belabored already, there are a few steps in every challenged claim some form of generating an OVER File and a separate step of a virtual representation of the credential that has been verified by an issuing agency to be an official representation of the credential. Again, these are two distinct claim requirements.

If we turn to slide 10, we can see that the Petition, as Mr. Argenti, actually, articulated, just generation itself is a verification. That's exactly what they're arguing here on slide 10 of the Petition and the Reply Brief. That is incorrect. The claim has two distinct requirements: generation of an OVER File and verification by the issuing agency. But they rely on generation alone.

JUDGE MCSHANE: Counsel, let me ask you this: you know, are you suggesting that Oborne would generate a token and it wouldn't do anything in its process to make sure that it's generating a valid token?

MR. WILSON: I guess you're asking me to infer between the lines of Oborne outside of what it actually discloses, and the answer is I don't know. Oborne discloses what it discloses, and I think what you're suggesting is an obviousness argument or wouldn't it be obvious over Oborne to do this, but there's no articulation of any rationale for that, other than what's already in the petition. And so I can only respond to the arguments that Visa has made, and saying that Oborne wouldn't issue a token without verification when Oborne describes issuing a token without

verification, it's hard for me to answer that question any other way than Oborne discloses issuing a token without verification. I mean, that's, literally, what the disclosure says. We pointed out how, when you look at the step-by-step process for issuance of a token, there is no verification step. It simply generates a token, and the claim requires two distinct things: generation of a token and verification by the issuing agency that it's an official representation. It's just not there. I mean, I can't infer it, you know. It's just not there.

And turning to slide 11, now, this is interesting, slide 11 is interesting because this gets to the reply argument that pivot to the new construction of issuing-agency verification that we and Cortex have unequivocally disavowed. Visa says they're not advocating that construction, but they're happy to rely on it. So I can't tell whether they're for it or against it, but let me just point out Dr. Shamos plainly stated that verifying credential data alone is insufficient to meet the petition's construction of these claims. If you look at the quote on the right, he says or he's asked, so you agree then that verifying that the credential data supplied by the user is correct does not meet your construction of verified by the issuing agency supplied in your opening declaration of these IPRs, correct? He says I think that's right. So he admits that merely verifying underlying credential data does not satisfy the opening construction by Visa of these claims.

JUDGE SZPONDOWSKI: So what's your response to the disclosure in paragraph 47 of Oborne where the issuer is generating a token and is obtaining assurance that the funds have been uniquely and exclusively

allocated for the token. I mean, isn't that verifying the token in Oborne?

MR. WILSON: I think that's verifying the underlying credential. That's like checking a bank account or a credit card and saying are there sufficient funds here. If there are, yes, we'll authorize this transaction. But verifying that there are sufficient funds is not a verification that a token, for example, is an official representation of the underlying credential. They have nothing to do with each other.

JUDGE CASS: So, counsel, how is this different from the driver's license example in the spec of the patent at issue?

MR. WILSON: So the difference is that, in one case, I think, if you're referring to Oborne's example, Oborne's example is saying, hey, this account has money in it, you can use it. That's like saying, hey, you have a valid driver's license. The status indicator, for example, that Oborne describes providing for the generated OVER File for a driver's license is different in that it indicates the validity of the virtual representation as distinct from the underlying credential. That's how those are different.

JUDGE CASS: So I want to ask you another question. So for step 1.3 you're saying that credential, virtual representation of the credential has been verified by an issuing agency, could that occur, for instance, the issuing agency generates the file and then immediately just does a check on it? Would that be sufficient? You know, kind of at the end of the generation process.

MR. WILSON: Sure. I think that would be sufficient, as long as there's an explicit check to say does this file that we generated represent officially the underlying credential.

JUDGE CASS: Okay. And so what if it took, generated the token, OVER File, whatever you want to call it, and then said we're going to check some of the information in there, but we're not going to check every piece of data, would that be good enough or does it have to check everything? How do we know, you know, what's required for it to be verified?

MR. WILSON: What's required is for the issuing agency to sign off on it as an official representation of the underlying credential. So whatever it needs to check to make itself happy that this token or this virtual representation is going to be an official representation of the underlying credential, whatever makes it happy, then that's sufficient, as long as that's an explicit check that's being done.

JUDGE CASS: So if you have a system that says, okay, I can generate a token and then said, okay, we're going to go verify the account number, put that into our bank database, make sure it's valid, it's got funds, et cetera, and then we're going to set a bit in the token saying it's valid; would that be good enough?

MR. WILSON: Yes, I think it would be.

JUDGE CASS: Okay. Thank you.

MR. WILSON: Okay. Turning to slide 12, this is Visa's argument of why Oborne discloses this. I think we've already hit this pretty hard, but I just want to point out a few things. Visa argued earlier that there's nothing in here invokes common sense, right. Well, the language that invokes common sense is saying, since verifying the token would be a routine step, based on the credential data received, that's invoking common

sense. And I think they said the Federal Circuit has not endorsed that view, but let me point out, in *DSS Technology*, which is a case we've cited and, in fact, I'll cover in more detail here momentarily, in *DSS Technology*, at pages 1374 to 1375, the Federal Circuit says here the Board relied on a gap fill, ordinary creativity instead of common sense to supply a missing claim limitation. In cases in which common sense is used to supply a missing limitation as distinct from a motivation to combine, our search for a reasoned basis for resort to common sense must be searching. The Board's reliance on ordinary creativity calls for the same searching inquiry.

It doesn't matter what words you use. If you're using a proxy for common sense, then it invokes common sense. Ordinary creativity, routine step, it would be logical, all those, as the Board has said, are proxies for common sense.

JUDGE CASS: So, counsel, by your logic, this is a single reference obviousness case, wouldn't that reasoning apply to every single reference obviousness case?

MR. WILSON: No, I disagree.

JUDGE CASS: Why not? What's an example of a single reference obviousness case that wouldn't raise this problem?

MR. WILSON: So I can use a single reference in my ground and say, you know, this particular claim would have been obvious based on this single reference. However, I can invoke as part of that obviousness inquiry the knowledge of a person of ordinary skill in the art. That knowledge makes, like, ten, references to disclose a feature, and so those ten references disclosing that feature then would show that that feature was

within the knowledge of a person of ordinary skill in the art and so it would be obvious to combine with a single reference. And that's still a single reference obviousness case, but it's based on the knowledge of a person of ordinary skill in the art based on disclosure of the feature in prior art. Here, we do not have disclosure of this feature, issuing-agency verification, in any prior art. Nothing. There's not a single reference that discloses it, and we are solidly in the *DSS Technology* paradigm of a claim limitation that is missing from the prior art.

So I want to point out also that the only rationale that's shown here are the last 12 words of this passage on slide 12: doing so would increase confidence that the token would represent the credential. That's it. That's the obviousness argument at its core. Twelve words. That is not a reasoned analysis with evidentiary support. You can see the cite here. That's a cite to the expert declaration, who says, verbatim, the same thing. We all know that that's entitled to little or no weight, so there is no reasoned analysis, no evidentiary support.

Turning to slide 13, we have the three points from *DSS, Technology*, about what you do in common sense analysis, and I'm going to skip the first point. Point number two, common sense is invoked to fill in a missing limitation only when the limitation in question was unusually simple and the technology particularly straightforward. And point three, references to common sense, whether it's supplying motivation to combine or a missing limitation, cannot be used as a wholesale substitute for reasoned analysis or evidentiary support, especially when dealing with a limitation missing from the prior art reference as specified.

Now, turning to slide 14, let's talk about unusually simple or particularly straightforward. Here, what we have is an evidence comparison. We've got Dr. Malek on the left who in, as you can see, 25 paragraphs of his declaration talk about why the limitation here is not unusually simple and the technology is not particularly straightforward.

What does Dr. Shamos, Visa's expert, say? Absolutely nothing. Nothing with the petition. And did he come back and reply in response to Dr. Malek's point? No. He submitted a reply declaration, but he refused to respond to Dr. Malek's points. The evidence on this point, these two points, unusually simple and particularly straightforward, is undisputed. On this record, the Board cannot find that this limitation is obvious.

JUDGE MCSHANE: Counsel, on this point, I'm just curious, so, you know, the language says the limitation in question was unusually simple and technology particularly straightforward. With the technology particularly straightforward, on that issue, I know that your expert talks a lot about the claim as a whole, but when you're looking at the technology and let's say, for the sake of argument, we limit it, should we limit it to the limitation of the verification step rather than looking at the claim in total?

MR. WILSON: So I think you need to look at both. The first inquiry is whether the limitation in question was unusually simple. Dr. Malek addresses that, and he points out, for example, that Oborne has a whole list of additional verification techniques. He doesn't list this one at all. If it were unusually simple or well-known in the art, surely he would have listed it. That's his explanation, and he has additional analysis of the limitation in question to show that it is not unusually simple. And he also

discusses extensively why the technology is not particularly straightforward with references to the prior art that Visa has cited and provided.

So this record is undisputed, and we have evidence to back up both of these points. Visa, who bears the burden of proof, has nothing.

Turning to slide 15, Visa also had to provide a reasoned analysis and evidentiary support. Again, there is nothing here in this Petition. All we have are the 12 words. And as we turn to slide 16, we can see the insight here, this paragraph 241, about Dr. Shamos's declaration. And I'm going to start in the middle of the paragraph of 241 there on slide 16. He says the issue of a token representing a payment credential would logically ensure that the token accurately represented the credential. Again, that's an invocation of common sense and doesn't move the obviousness analysis. It's essentially a non-statement.

Next sentence: The existence of unofficial, forged or altered tokens in the marketplace would create problems for both issuers and users. What kind of problems? Are those problems for Oborne's system? How would issuing-agency verification, which Visa is pulling out of the air, making up out of whole cloth, how would that solve those problems? We don't know. There's no reasoned analysis and, certainly, no evidentiary support.

And, finally, the next sentence: It would be a routine step to verify that the token was an official representation of the credential based on the credential data received and doing so would increase confidence that the token legitimately represented the credential. Again, that's verbatim from the Petition. It's entitled to little or no weight, aside from the fact that there

is no reasoned analysis or evidentiary support there.

So Visa cannot carry its burden on this record to show obviousness of issuing-agency verification. It simply cannot. But, wait, it gets worse. Turning to slide 17, we see that Dr. Shamos has opined creating identity documents in the digital world was challenging for several reasons. Number two, a digital credential can easily be copied, forged, or altered, and it is difficult to issue a challenge to a remote network user to prove that they are the person named in the credential. And in paragraph 120 on the right, he says a solution to problem two is to require the presenter of the credential to furnish additional information to prove that they are the person named in the credential. He says this protects against credentials being copied or stolen. In the banking industry, this was done starting in 1967 by requiring a user to enter a PIN at an ATM machine. He says we know about this problem of unofficial, forged, or altered tokens; it's already been solved. You require user authentication at the time of the transaction; that's how you solve it. It's been done since 1967. So why wouldn't a person of ordinary skill in the art use that? Why would a person of ordinary skill in the art resort to grabbing issuing-agency verifications out of the air, out of the ether, when Dr. Shamos says this problem has already been solved?

Well, guess what? Turning to slide 18, Oborne uses exactly what Dr. Shamos said. "In some implementations, the token server may determine whether the user token is authenticated. If the token server determines that the user is not authenticated, option no, the token server may generate an authentication failed message and initiate an error-handing routine and/or a user enrollment routine, such as the PTT 500 component

discussed above in the description with reference to Figure 5. If the token server determines that the user is authenticated, option 'Yes,' the token server may continue processing at 713a." Oborne already uses user authentication at the time of the transaction, which is exactly what Dr. Shamos says solves this problem. So why are we grabbing issuing-agency verification out of the air?

JUDGE CASS: So, counsel, I'm looking back at Oborne and, specifically, say, page 8, paragraphs 47, around paragraph 47. It says one of the ways you can generate the token is to have, for instance, the user fills out a form that has the information that you want in the token. And I think the patent has a similar example where you can fill out a form and it can scan it and, basically, send all that information to the token or OVER file generator. And as we all know, I mean, we can make mistakes when we write down long strings of numbers or scanners can make mistakes when they try to read our handwriting or things like that, so, you know, given that that's pretty well known, why wouldn't it be obvious to verify the information that's in there?

Oh, I'm sorry. I think somebody has lost sound. Okay. We're good.

MR. WILSON: Okay. So just to be clear, you're articulating a new obviousness rationale --

JUDGE CASS: Well, I mean, I don't want to say whether it's new or not new, but I'm just curious why that would not be obvious. I think we may be having some -- oh, I'm sorry. I think I just muted myself and didn't realize it. Let me ask my question again so everyone hears it.

So looking at Oborne around paragraph 47, there's a discussion about how a client can generate a form that has all, you know, information in it and then that information on the form can get put into a token or OVER File, and I think the patent has some similar discussion when it talks about the driver's license example. And we all know that, when we fill out forms with long numbers on them or we scan them, that sometimes we can make mistakes or the scanner can make a mistake, something like that can happen. So why wouldn't it to be obvious to just run a check on that information on the form just to make sure it's accurate?

MR. WILSON: So I guess I don't understand the specific context. You're saying when the application comes in and they're trying to find the credential, do they check the information to make sure that the entered information is correct so that you actually get a real credential, a real underlying credential; is that what you're saying is a check?

JUDGE CASS: Yes. Just to make this more concrete, so you've got a form on information to create a token. Maybe one is bank account number, so you write in your bank account number. Maybe another is driver's license number, so you write that in. And there might be other information, as well. And then that goes to a system, say the token OVER File generation system that takes the information in the form, creates a record, kind of like we saw in paragraph 47 of Oborne that's got a token with a bunch of information in it, and puts together that record as the token. But it all came from information on a form, so why wouldn't, before the token actually gets issued, they want to go back and actually verify that the account number was correctly entered in the file and that the driver's license

number was correctly entered in the file and other such information was actually correct by verifying it against some official record of it?

MR. WILSON: So I think Oborne actually does disclose that, and that's in the form of checking the underlying credential there. So, in other words, if you're saying I want a token to represent this bank account, Oborne will go and verify that there is actually a bank account there, maybe even that there are funds in it, to verify that what you're referencing is actually a real credential and there is actually a real credential here before it generates a token.

So, yes, Oborne discloses that. What it doesn't disclose is, once I've done that, now I'm generating a token that's going to be a virtual representation of that file and verifying the token is actually an official representation of that bank account. That's the piece that's missing.

JUDGE CASS: You could do this in a couple of ways. You could verify the information as part of the generation of a token, or you could generate the token and then you could verify the information after that, right? And wouldn't the latter be a verification of the token?

MR. WILSON: No, I don't think so. I think you're trying to confirm that there is a valid underlying credential, that the underlying credential is valid. So I think whatever or wherever you do it in, if you're just checking to see is there a real credential here, is there a real driver's license with this number, that's verifying that the driver's license actually exists, not verifying that the token or the virtual representation is an official representation of the valid underlying credential. Those are two distinct steps: again, generating the OVER File and then verifying the OVER File.

What you're describing, I think, is part of generation. Do we actually have a credential here --

JUDGE CASS: I guess I'm struggling a little bit because when you look at paragraph 47 of Oborne, this looks to me like an XML file with a bunch of information in it. I'm struggling a bit between how do you know what's verification of the token that has information in it versus verification of the underlying credential, which also matches information in the token? It strikes me as kind of maybe a fine line, and I'm trying to make sure I understand what's on what side.

MR. WILSON: So I think what you're looking at, and I'd have to go back and re-read this passage in Oborne to be sure, but I think what you're looking at in paragraph 47 is or what Visa at least contends, I know this much, that they contend that that is a token. That is the -- OVER File is the virtual representation; it's everything. So that's the end result of the process.

The beginning would start with an application, and I'm sure, if you flip back in Oborne, you'll find the application and it probably contains similar data structures, you know, bank account and all those sorts of things. So when Oborne receives that, it's going to, in the Oborne system, the PPT is going to go back and check and say is there really a bank account here. But it doesn't check that token data structure in paragraph 47.

JUDGE CASS: What would checking the data structure look like?

MR. WILSON: I'm sorry?

JUDGE CASS: What would checking the data structure look

like?

MR. WILSON: It would look like an additional verification step by the issuing agency actually. So let's be clear. Although, yes, Oborne says that the issuing agency can operate the token server, it doesn't have to, but the verification must be performed by the issuing agency to say, yes, we will accept this virtual representation as a proxy for this underlying credential. We don't see that anywhere in Oborne.

JUDGE CASS: All right. Thank you.

MR. WILSON: Okay. I just want to quickly address the, turning to slide 22, the fact that Visa's petition identifies the PPT apparatus as the OVER Engine, and we heard some argument about that earlier. It's beyond question that the Petition identifies the PPT apparatus as the OVER Engine, and what we've heard now are three versions of this argument because the Petition identified the PPT apparatus as the OVER Engine, the reply brief identifies the token server, and then, today, we heard Mr. Argenti identify the token server in combination with the token database. So three versions of this argument. Shifting arguments don't work in IPRs. It's improper.

So looking at the Petition passage on slide 22, and this same passage exists in every one of the petitions. And, in fact, you don't have to take my word for it. All of the institution decisions conclude that the OVER Engine in Visa's theory is the PPT apparatus. They say it explicitly. So the Board interpreted the petitions the same way we did. Visa can't change its position in reply, and it certainly can't change its position today at the oral argument.

And let me just jump ahead to slide 26 and say Dr. Shamos disagrees with Visa. Their own expert, beginning on the left, says, just to clarify here, you are not saying that Oborne's token server is, by itself, an OVER Engine, are you? And he says, so I guess there's a difference between what I said or didn't say and what I actually believe. Always the words you want to hear your expert say. So I don't think I have a statement that says that the token server is the OVER Engine. He refused to say it. He would not say the OVER Engine is the token server.

So Visa is required to put forth in its petition a ground of invalidity with specificity. The statute requires that, Section 312(a)(3). It didn't do it. Now we're in the third iteration of this. Looking on the right, Dr. Shamos says, so my question, though, is as little different. This is after pages of transcript trying to get him to identify an OVER Engine. So my question, though, is a little different, and that is what in Figure 6 constitutes the OVER Engine if the OVER Engine has to both generate and verify tokens? Well, I can't tell because it depends on the implementation. He was unable to identify an OVER Engine. That should end the matter, and the Board can confirm the patentability of all challenged claims over all Oborne grounds on that basis alone.

Now, I want to skip ahead to slide 29. Now we've shifted gears. Now we're in Stafford, in the Stafford - Purves combination, and this is whether or not key signatures can constitute the OVER File or the virtual representation of the credential, which is Visa's position, as you can see here in slide 29 taken from the Petition. The key signatures taught by Stafford correspond to the recited OVER Files and, in fact, they say a hash value,

thus, acts as a virtual credential representation of the stored credential derived based on the information associated with the credential, and that's the key problem for their OVER File argument.

They argue two things: the user's private key and the one-time pad are derived based on information associated with the credential or the information associated with a credential because that's how you get the hash values, but neither one of those things is true. As we see on slide 30, in Stafford, each one-time pad is used to encrypt a bundle of credentials. The unencrypted ID files, plural, are symmetrically encrypted using one-time pad. So when Dr. Shamos was asked about this on the right, he agrees. So a single release of information can contain any number of credentials, correct? It could. So the ID files, no matter how many there are, are encrypted together with a secure one-time pad, correct? That's what that seems to say. A one-time pad, a bundle of credentials --

JUDGE CASS: So, counsel, what are these credentials, the ID files?

MR. WILSON: They could be anything. They could be bank accounts. They could be birth certificates. They could be passports. They could be anything.

JUDGE CASS: Are you saying that those credentials might not have anything to do with the credentials that go into the OVER File, or would they be credentials that are going into the OVER File?

MR. WILSON: So I don't think there is an OVER File in Stafford. They certainly don't have anything to do with the one-time pad or the user's private key. Those two things are completely independent of

whatever credentials end up being encrypted.

Now, their argument is that, because a one-time pad is used for a single instance of encrypting this bundle of credentials that, somehow, all of those credentials in that bundle are now associated with this one-time pad and, therefore, you know, by circular logic, you end up with, a-ha, the one-time pad is information associated with the credential. It's just not true. In Stafford's system, if I encrypt these same credentials for a second release of information, they use a different one-time pad. So there is no correspondence between a one-time pad and any credential in Stafford. The same is true of the user's private key.

If we turn to slide 31, you'll see now in Stafford -- this is Dr. Shamos again. Now, in Stafford, the user is assigned a private key as part of its use of Stafford's system, correct? Yes. And the user's private key is persistent, regardless of how many credentials the user uploads or how many releases of credential information the user purchases, correct? I think that's generally true. The private key is given to the user before they upload any credentials. It is not associated with any credential.

So turning to slide 32, you can see the key or pad, pad key one, used for the one-time pad, is encrypted with a user's private key, and that's how you get IdSec1, the first hash value, and, ultimately, how you get IdSec2, the second hash value. That's their argument. These things are not associated with any credential.

Okay. Now I want to turn to slide 34 and now we're back to issuing-agency verification but on the Stafford ground. And we can see in the Petition that the Petition’s position is Stafford teaches that it's encrypted

credentials, the underlying credential that is, may be verified by the issuer and may include storing an image of the credential, a scanned copy. So all we're talking about here in Stafford are verifying the underlying credentials.

However, to the extent that Stafford does not expressly teach that the key signature file sent to the user include a virtual representation verified by the issuing agency, this aspect of the claim is met by Purves. So they're relying on Purves.

Now, turning to slide 35, this is their argument for Purves. And you can see again -- but the difference is this argument is disclosure. Purves discloses this. And if we look at it, the argument is nonsensical on its face. Dr. Shamos repeats it nearly verbatim, which entitles his testimony to little or no weight.

And if we turn to slide 36, you will see the actual argument broken down. First, the rationale, let's start with the rationale at the end. Since an actual credential naturally represents itself, I'm not even sure what that means, but how does that have any bearing on the representative image provided from an issuer at the time? I don't know. It's not explained. This is supposed to be disclosure in Purves. There's no citation to Purves. There's no argument that Purves explicitly discloses a representative image being verified by the issuing agency. There's nothing here.

Now, let me jump ahead to my last point, and this is in slide 39. And this point is the combination of Stafford with Purves, and I think the Board got this correct in its institution decisions. Stafford is a completely different system than Purves. Stafford is a highly secure system for the disclosing credentials, things like a birth certificate or a bank account or

whatever. Purves is a totally different system, and we can see here Figure 2 on the left of slide 39 has, Dr. Shamos and I agree, at least 13 numbered steps to release information. And, now, can you imagine a scenario in which any consumer goes to the store and is willing to engage in these 13 steps and pay a fee to use their credit card, that doesn't make any sense. What about going to a movie theater and handing a ticket to a ticket agent using these 13 steps and paying a fee or boarding a plane and going through these 13 steps and paying the fee. Nobody is doing that. That's not what Stafford is for. It is an entirely different system.

And turning to slide 40, Purves is a virtual wallet for consumer transactions. You can see that in the abstract right there. The enrollment of payment accounts in a consumer's virtual wallet. These are two totally different systems for totally different purposes. So the question is how and Your Honor asked Mr. Argenti earlier how do you incorporate one system into another, and he said it wasn't his job to articulate the specific embodiment. Well, but it is.

And turning to slide 41, here's why. If we look at slide 41, and this is the same slide I read earlier that shows that what Stafford does is encrypts a bundle of credentials at a time, not just one. So which of those credentials do you pick to create a representative image of to include with the hash values in Stafford to show you what credentials you've encrypted? It doesn't make any sense. Stafford is doing a bundle of credentials, not one; so this doesn't make any sense. And guess what? Those credentials may use a different hash value in the next disclosure. So if I use the same representative credential on two sequential exposures, how are they

distinguishing -- this makes no sense. This combination makes no sense.

And if Your Honors don't have any additional questions, I'll reserve the rest of my time.

JUDGE CASS: All right. Thank you, counsel. You have two minutes left before your argument time was used up, so that will give you seven minutes for your rebuttal.

MR. WILSON: All right. Thank you, Your Honor.

JUDGE CASS: All right. Counsel, you have four minutes remaining in your rebuttal, so you may begin when ready.

MR. ARGENTI: Thank you, Your Honor. First, going to the Oborne discussion and the DMV example, we already discussed that at length, but I just want to point out their position now is that the DMV example is verifying the OVER File as opposed to the OVER File request. I would refer the panel to page 12 of their Patent Owner response where they cited the disclosure that talks about verifying the information contained in the OVER File generation request. Their argument in the Patent Owner response stands on its own. That's what we responded to in the reply. So for them to shift positions now is untimely and --

JUDGE CASS: Counsel, I think, if I understood it correctly, their position was that that was a verification of the OVER File because there's a status indicator, so I was wondering if you could respond to that.

MR. ARGENTI: So that's a separate disclosure, and it's really irrelevant. As we discussed earlier when I was up, there are examples where they are pointing to or in that column that at least pay lip service to the idea of verifying the virtual representation. There's very little disclosure of that.

That doesn't change the fact that this is the example they relied on in the Patent Owner response. This is the one that we responded to explaining why it's the same in the prior art. We interpreted that as a broader interpretation of the claim scope to which we are entitled to respond as a Petitioner. For example, refer to the Federal Circuit *Axonics* decision for that proposition.

But, regardless, even if they weren't applying a broader interpretation, that doesn't change the fact that, well, then we're just back to the Petition grounds. The Petition stands on its own with respect to showing how, if you have to verify the virtual representation, if that has to be the thing that's verified and, if verifying the underlying credential information can't be a form of verifying the virtual representation, that was the basis of the Petition. So that analysis still stands on its own. There's nothing that has changed about that.

As to their citation to the *DSS* case in support of their common sense argument, I didn't see anything in that *DSS* case that says, well, it's a common sense argument; even if you're not saying it, you're relying on common sense. To the extent that they talked about gap-filling there, that's, again, distinguishable from our circumstances here where we're pointing to disclosure in Oborne itself, the disclosure that says it can be the bank that issues the token, the disclosure that says that there can be a linkage, a confirmation of funds available to that particular token and that that linkage can be stored at the bank.

So we're not gap-filling. We're explaining why the disclosure of Oborne that's there renders this limitation obvious.

They argue that Dr. Shamos concedes somehow that this

problem had been solved through user authentication. Oborne also talks about user authentication. User authentication is a separate issue than confirmation or verifying that the token, the virtual representation, is valid. You can have a valid token in the wrong user's hand. That's what you're trying to avoid with user authentication. If the user authentication at the time of the transaction was seen as the solution for token verification, then it's already a failure because the user is going in and trying to use that token. What we're getting at in our combination is verifying that the token is valid at the time of issuance, which, again, is consistent with what Oborne discusses and describes and is entirely consistent with routine practice and logical in terms of getting everybody involved in this flow of information confidence that the token that's been issued actually stands for an account.

And, remember, Oborne talks about obtaining assurance that funds are available for a token, not just funds are available. Funds are available and linked to that token.

JUDGE CASS: Counsel, I think you're out of time.

MR. ARGENTI: I had a couple of points on Stafford, if I could make them quickly. But if not, I can sit down.

JUDGE CASS: I'll give you one minute.

MR. ARGENTI: Thank you, Your Honor. As to their slide 26 argument with Dr. Shamos and his apparent alleged concessions, they're selectively quoting him there. He pointed out immediately before that testimony that their questions had been inconsistent. That's what he was pointing out. And then, when he says he can't answer the question with respect to Figure 6, that's because you have to look at Oborne in its larger

context than the disclosure as a whole. As I already explained, Figure 15 and the related written description explains that all of those previous figures, including Figure 6, can be combined together.

As to their slide 36 argument arguing that we have not shown that Purves shows verification of card images, that's untimely. If you look at the Patent Owner response, they did not make that argument in their Patent Owner response. They only argued that Purves lacks the storage requirement and is not used for verification, as opposed to the image itself being verified. So that --

(Simultaneous speaking.)

MR. ARGENTI: -- where we made the argument.

JUDGE CASS: Thank you, counsel. All right. Counsel for Patent Owner, you had seven minutes. I gave counsel for Petitioner another minute, so I'll give you eight minutes. You may begin when ready.

MR. WILSON: Thank you, Your Honor. Unless you have questions, I won't take all of this time. Let me just -- I think there's only one point that's worth responding to here, and that is the last point that Mr. Argenti made that our argument about Purves not disclosing issuing-agency verification is untimely, we didn't make it in our Patent Owner response, I would refer the Board to page 55 of our Patent Owner response where, and I quote, it says: Purves does not teach using card images for verification and, thus, fails to provide the asserted verification by the issuing agency. It literally says that. The argument is fleshed out in pages 57 to 60, and you'll also find it in our surreply at page two. So the argument was made.

And that's all I have, unless Your Honors have any additional

questions.

JUDGE CASS: All right. I don't. And I don't see anything from any of my co-judges, so thank you very much.

MR. WILSON: Thank you, Your Honor.

JUDGE CASS: Does either party have anything to raise before we adjourn the hearing?

MR. ARGENTI: No, Your Honor.

MR. WILSON: No, Your Honor.

JUDGE CASS: Thank you very much. Well, counsel, I appreciate the time and effort you put in today. Clearly, you were both very well prepared and spent a lot of time organizing your presentations, and we appreciate it a lot. You'll be getting an opinion from us in due course. And with that, this hearing is adjourned. But if you could stay for a few minutes and see if the court reporter has any terms or other questions that could be cleared up, that would be terrific. Otherwise, have a great rest of your day.

(Whereupon, the above-entitled matter went off the record at 3:03 p.m.)

PETITIONER:

Matthew Argenti
Michael Rosato
Patrick Medley
Joseph Baillargeon
WILSON SONSINI GOODRICH & ROSATI
margenti@wsgr.com
mrosato@wsgr.com
pmedley@wsgr.com
jbaillargeon@wsgr.com

PATENT OWNER:

Michelle Armond
Douglas Wilson
Patrick Maloney
Yue Han
ARMOND WILSON LLP
michelle.armond@armondwilson.com
doug.wilson@armondwilson.com
patrick.maloney@armondwilson.com
amy.han@armondwilson.com