UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MASTERCARD INTERNATIONAL INCORPORATED
Petitioner
v.
LEON STAMBLER
Patent Owner

Case No. CBM2015-00044
Patent 5,793,302

DEPOSITION OF SETH NIELSON, Ph.D.
Baltimore, Maryland
Tuesday, December 8, 2015

Reported by: John L. Harmonson, RPR
Job No. 99776

December 8, 2015
9:04 a.m.

Deposition of SETH NIELSON, Ph.D., held at the offices of Regus, 100 International Drive, Baltimore, Maryland, pursuant to Notice, before John L. Harmonson, a Registered Professional Reporter and Notary Public of the State of Maryland, who officiated in administering the oath to the witness.

A P P E A R A N C E S

On Behalf of the Petitioner:

BAKER BOTTS
1001 Page Mill Road
Palo Alto, CA 94304
BY: ELIOT WILLIAMS, ESQ.

and

BAKER BOTTS
30 Rockefeller Plaza
New York, NY 10112
BY: CHRISTOPHER PATRICK, ESQ.

On Behalf of the Patent Owner:

FLACHSBART & GREENSPOON
333 North Michigan Avenue
Chicago, IL 60601
BY: ROBERT GREENSPOON, ESQ.

S. NIELSON

P R O C E E D I N G S

9:04 a.m.

Whereupon,

SETH NIELSON, Ph.D.,

after having been first duly sworn or affirmed, was examined and did testify under oath as follows:

EXAMINATION

BY MR. WILLIAMS:

Q. Good morning, sir.

A. Good morning.

Q. Have you been deposed before?

A. I have.

Q. Okay. Any reason you can't testify accurately or truthfully today?

A. No.

(Exhibit 2004 and MasterCard Exhibit 1001 marked for identification and attached hereto.)

BY MR. WILLIAMS:

Q. I've put in front of you a couple of exhibits. Let's start with the one on top which

is Exhibit 2004.

Q. Do you recognize that?

A. It appears to be my declaration for this IPR.

Q. Okay. If you turn to page 40, there is a facsimile signature. Do you see that?

A. I do.

Q. Is that your signature?

A. It is.

Q. And did you sign this document?

A. I did.

Q. And have you had an opportunity to read the document?

A. Yes.

Q. And to the best of your knowledge, is it accurate?

A. I'm sorry. May I clarify? When you say I've read the document, do you mean the one in front of me or that I've read this exhibit before?

Q. The exhibit.

A. Yes, I've read it before.

Q. Do you have any reason to think that the copy in front of you is not an accurate copy?

A. I don't see any reason to believe that, no.

Q. How did you go about preparing this document?

A. I spoke with counsel about what questions I needed to provide opinion -- about which I needed to provide an opinion, and then based on that discussion I started drafting the document. After preparing a draft, I reviewed it, received some feedback, made some adjustments before submitting it for submission to the PTAB.

Q. Have you had an opportunity to read the document since you -- Well, let me back up.

The document is dated October 20, 2015. Is that around the time that you signed it?

A. Yes, I believe so.

Q. And have you had an opportunity to read it since that date?

A. I have.

Q. And anything in there that you would like to change?

A. I did come across a paragraph that -- it doesn't change any opinions, but I think it

has -- at least I would have reworded it.

Q. Which paragraph is that?

A. Can you give me a minute to find it?

Q. Yeah, no problem.

A. Paragraph 91.

Q. 91. Let me just get there. That's on page 31?

A. Correct.

Q. And what about that paragraph would you like to clarify?

A. The very last sentence. It currently reads: "The bank signs the public key and the electronic check but does not issue a certificate."

I based that sentence off of something I was reading in the Diffie declaration. But when I went back and looked at the Davies book, it assigns the public key a name and an expiration date.

Q. Okay. You're referring there to the disclosure in Davies of the portion of what Davies calls the check?

A. There is a disclosure. I would have to look up the exact page, but there is a

disclosure of Davies that is used in creating an electronic check, and that's what I'm referring to, yes.

Q. So how does that -- so how does that teaching of Davies then alter your views about whether the bank signs the public key and does not issue a certificate?

A. I'm not entirely sure. Davies uses the term "certificate" only for the thing given to the registry. So I'm still not sure if there is a certificate or not that's issued to the bank. But either way, it's still not a credential under the -- for purposes of the patent. So that's why I said it didn't change my opinion.

Q. Why do you say it's not a credential?

A. For the reasons that I identify in my report. Like I say in Paragraph 89, I think is where I set it forth that the check is not presented for purposes of establishing or determining the identity of the party.

Q. And so for that reason, the check is not a credential, in your view?

A. Yes.

Q. What about the data on the check? Is that a credential?

A. Which data?

Q. The data that you're referring to, the bank signature on the customer identity, expiration date and public key.

A. Well, that data is also not presented for purposes of establishing or determining the identity of the party.

Q. Why not? Why do you say that?

A. Because that data is not used in establishing the identity of the party. That data is used for determining, in this case, the originator of the bank's account to figure out where the funds are coming from.

Q. When you say "originator of the bank's account," what are you talking about?

A. I'm sorry. May I use the reference?

Q. The Davies reference?

A. Yes.

Q. Sure, of course. You brought a copy?

A. I did.

Q. Do you want to use that one?

A. It's just easier to find some of the

pages.

Q. I have a copy of the one filed in the IPR. If you would like to look at it, just let me know.

A. Sure.

So the data that we've been referring to is found on page 328, figure 1022.

Q. Uh-huh.

A. And the data here that I believe we're referring to in the context of Paragraph 91 would be what is identified by Davies as fields 5, 6 and 7.

Q. Sure.

A. So the customer identity, the customer public key and the expiratory date, in this case the information about where the funds are coming from for purposes of the check.

Q. So that field 5, customer identity, you're saying that's not presented in order to verify the identity of the customer?

A. Correct.

Q. So what's the purpose of putting the customer identity on the check?

A. So Davies in here compares it to a

paper check. It's just like with a paper check, you wouldn't have an account to draw money from without that information.

Q. So that information, customer identity, identifies the account that the funds are to be drawn from?

A. Well, it identifies the customer, and then you would have to have the bank be able to figure out what account that's coming from. But my point is that the purpose of it is to figure out where to draw funds from. It's like with a paper check. I don't present it to establish my identity to somebody.

Q. If you're going to accept a paper check from somebody, wouldn't you want to know their identity?

A. Well, when I worked food service, if we had concerns about their identity, we had to ask for something. So the check was not presented to us for identity. If we were concerned about it, we would ask for some other piece of information to establish their identity.

Q. Now, in this particular case what is the point of field date?

A. So the point of field date is to ensure that the public key has not been altered or modified.

Q. Is that the only purpose of section 8?

A. Well, if you're getting a check, you want to make sure -- especially an electronic check, you want to make sure that the information in it is accurate, that the data you're getting about where those funds are coming from is going to be correct and has not been forged.

Q. So how does field 8 do that?

A. Well, so field 8 is a signature by the bank, and that signature by the bank is the bank's -- the bank's -- It's a mechanism that you can use so that -- that the bank is saying that this information is correct.

Q. And one of the fields in that information is the customer identity, right?

A. The customer identity, customer public key and expiratory date are correct.

Q. Putting aside the exact disclosure of Davies -- we can keep it open if you want -- but I want to ask you a question more generally.

You've familiar with the term

"certificate" in the area of security?

A. I am.

Q. What does it mean typically in the field?

A. So it depends on context. But the most common one, usually like if you would just throw it out in a room full of computer scientists, I would assume that most of them would think of the certificates that we use with secure socket layer for web communication. So usually it's a certificate where data has been validated by a third party such as Verisign, and then it ties together a public key and some other piece of information.

Q. Would it tie together a public key and an identity?

A. It usually has identifying fields.

Q. And does it tie that information together by doing a digital signature over that information?

A. Yes, I believe that's correct.

Q. So can it be said, then, that in Davies sections 5 through 8 are a certificate?

A. Well, I don't know about calling it a

certificate in general. But comparing it to the certificate that we were just talking about, the use case is certainly different. When you have a certificate, for example, a certificate like an SSL certificate, it's not enough to just have a name because that's insufficient for its purposes.

And so one of the identifying pieces of information that has to be included for it to work correctly is a web address so that when you go to that web address and you are having, for lack of a better description, a conversation, when you're having the connection with that website, that you know that the website you've gone to is the website you think you've gone to.

Q. What makes you think that customer identity in Davies is a name and not something else?

A. It doesn't say very clearly. It just says customer identity. I'm thinking that because Davies compared it to a paper check, that it would be a name.

Q. Why wouldn't it be the customer's account number?

A. For the originator, that's possible, I guess. I'm thinking with a paper check you usually have a name and you have a payee name.

Q. So payee name is field 13 in the Davies check, correct?

A. Correct.

Q. And there is no other field that has the name of the customer or the originator, right?

A. I don't -- I don't see one, no.

Q. Only field 5 would include that information?

A. Yeah, that appears to be correct.

Q. And you agree with me that the information in this check has to include information for the originator's bank to identify the account of the originator?

A. So while it's not identified, obviously for it to work as a check there would have to be some way of identifying the account of the person paying.

Q. So Davies uses the name "drawer." Do you know what that is?

A. When I have read that word in context,

S. NIELSON

I have understood what it means. I'm trying to think about the definition off the top of my head.

Q. In the case of the Davies context, would the drawer be the same as the customer in field 5?

A. Is there a sentence that --

Q. That I'm thinking of?

A. Yes.

Q. I'm looking at page 330 of Davies under the heading "Point-of-Sale Payments by Electronic Check," on the second paragraph of that section, the first sentence there.

A. Okay. So for a point-of-sales payment, which is one of the -- Okay. Hold on a second. Let me just review the background here.

Right. So this one is referring to offline payments at a merchant terminal. So the drawer in this sentence would be the one issuing the check.

Q. Okay. So that would be in the case of the field data, field 5, the customer identity, would be the drawer?

A. Yes, I believe that is correct.

Q. And clearly Davies there is describing that the issuer bank is able to check the drawer's account when processing the check?

A. Yes. But he doesn't describe how that's done.

Q. Is there any other way it could be done besides using the data in field 5?

A. Well, the reason I'm hesitant on that is only because Davies on page 328 describes this as kind of a minimal set of information. And when it describes it as a minimal set of information, it's referring to the cryptographic verification of this transaction. And he doesn't go into detail on a lot of how the actual financial transactions are resolved.

So for example, like when you have, you know, customer identity and payee identity, it doesn't describe all the different processes that are used with paper checks, which it kind of compares it to, for resolving those issues which sometimes come up in real life.

Q. But you agree with me that he does disclose that the issuer checks the drawer's account when processing one of these electronic

checks?

A. Yes, but not how it's done.

Q. One way that it could be done is to use the information in field 5?

A. If the information in field 5 were sufficient.

Q. Okay. Was there any other disclosure in Davies that showed you there was some other way that the issuer could identify the drawer's account when processing the electronic check?

A. Let me take just a quick minute to review it.

Q. Yeah, please.

A. So I don't see any other descriptions. But the thing that I notice is that the identity that is described here is suggested it would be like a name. For example, when it refers to the black list also under the point-of-sales payment, again it's not described in detail, but comparing it to paper checks you would have a black list of names that you would refer to when not accepting a check.

And so, you know, it suggests to me that it very well might just be a name.

Q. You said black list is a list of names. Do you think that's what Davies is talking about when he uses black list?

A. Well, he doesn't go into a lot of detail. Again I'm interpolating a little bit based on the description of it being similar to paper checks.

Q. Other than Paragraph 91, are there any other paragraphs of your declaration that you think need to be clarified or revised?

A. No, not that I know of.

Q. Do you know who Whit Diffie is?

A. Whitfield Diffie? Yes, I am aware of him; I have never met him in person.

Q. You know he gave a declaration in this proceeding, right?

A. Yes.

Q. And you've read it?

A. Yes.

Q. Before that declaration, had you ever heard of Whitfield Diffie?

A. Yes.

Q. In what context?

A. I am familiar with Whitfield Diffie in

his work on what is commonly referred to as the Diffie-Hellman key exchange protocol.

Q. Is that a protocol that you teach in any of your classes?

A. Yes. Or -- Yes.

Q. What level of students do you teach the Diffie-Hellman protocol to?

A. My class is graduate level network security.

Q. And is that a class taught in a particular discipline? Is it an engineering class or a computer science class?

A. I'm not really sure. Johns Hopkins has both departments and institutes, and my work is sometimes under the umbrella of the computer science department and sometimes under the master's -- or the ISSI, the Institute for Security Systems Infomatics. So sometimes it's a special security institute and sometimes it's a department of computer science.

Q. Are students in that class generally seeking a degree?

A. Yes.

Q. And what degree are they seeking?

A. Well, so that depends. Most of them have been in that ISSI, and then they're seeking a master's degree in security infomatics.

Q. Okay.

A. And then I have a lot more students from undergraduate this year who would be seeking a bachelor's degree in computer science.

Q. Are you familiar with -- I apologize. I have a cold so some of my questions may be hard to understand, so just ask me to rephrase them.

Are you familiar with the term "public key cryptography"?

A. I am.

Q. What is it?

A. So public key cryptography is a very broad term. And then, of course, there is kind of common implementations of it. The broad term is just basically any type of cryptography where you have asymmetric keys. What that means is typically you will have one key that reverses the other key. So if you encrypt with the first key, you decrypt with the second.

Q. And so then is there symmetric cryptography in contrast to that?

A. Yes. I'm trying to think if I've ever heard of them using the term "public key cryptography" with symmetric keys. I can't think of any examples and it certainly wouldn't be common. But symmetric key is, in contrast, you have a single key that both encrypts and decrypts.

Q. So what is the "public" in public key cryptography supposed to indicate?

A. So in general -- again, it's kind of a broad concept. But the idea is that you have one key that you won't reveal to anybody, and then one key that you distribute. And that key that you distribute would typically be called a public key.

Q. Do you know when the idea of public key cryptography was first published?

A. So I am aware that Diffie and Hellman -- and Diffie is on record as there being one other person; Merkle I think was their name -- had one of the first public papers about public key cryptography. There was also some British work that was a year before but it was secret and not released until the '90s.

Q. In your declaration in Paragraph 24 you say you've reviewed materials related to the IPR. My question is: What materials are you referring to there?

A. The materials that I've reviewed are the petition; the response. Diffie's declaration. I've reviewed a transcript of Diffie's deposition. And I've reviewed the Davies reference, the Meyer reference, the references that are identified in this IPR as potentially being prior art.

I think that's everything.

Q. So I don't think you mentioned the '302 patent, but I assume you've read that?

A. I have read the '302 patent.

Q. Have you read the file history of the '302 patent?

A. I've only read parts of it.

Q. You know what I mean by file history, I assume?

A. I do.

Q. What about any district court opinions where the '302 patent has been at issue? Have you read any of those?

A. I haven't. Wait. Let me think a minute. I can't remember. I may have reviewed some related claim construction, but I don't think so.

Q. Okay. How are you being compensated in this matter?

A. So initially I was -- up until the first of this month I was an employee of Harbor Labs, a consulting company, and Harbor Labs would bill for my work on an hourly basis. And I'm now at a new consulting company called Ironwood Experts, and now Ironwood is billing for my time on an hourly basis.

Q. And what hourly rates has this work been billed at?

A. In both cases it's $425 an hour.

Q. And do you have an estimate of how many hours you've worked to date on this matter?

A. No.

Q. Has either Harbor Labs or Ironwood Experts prepared invoices for your time?

A. Harbor Labs has, yes.

Q. Have you seen them?

A. I haven't.

Q. So the '302 patent claims priority to an application that was filed in November of 1992; is that right?

A. That is my understanding, yes.

Q. Okay. And you were obviously not yet a person of ordinary skill in the art in November 1992, right?

A. I was not a person of ordinary skill in the art as of November 1992.

Q. Were you in school at the time?

A. I was in junior high.

Q. What's your experience in the banking or financial industry? Do you have any experience in that industry?

A. I have done some consulting work for some high-frequency trading. In my course on network security we do cover some issues of banking security. And I have mentored a research project, I guess it's only tangentially related, but on the topic of Bitcoin.

Q. Do you know what the -- do you know what an interchange system is?

A. I don't know off the top of my head.

Q. When were you first engaged for this

matter?

A. I'm trying to think of the date.

Q. Approximately is all I'm looking for now.

A. I would approximate maybe it's been about a year.

Q. Okay. And so how were you first contacted about the matter?

A. I was contacted by Robert Greenspoon.

Q. Okay. At the time you were contacted, had you heard of Leon Stambler?

A. Yes.

Q. How had you heard of him?

A. I had been previously contacted about being a consultant in another case.

Q. Another litigation matter?

A. Yes.

Q. And you said previously. How far previously from when you were contacted about this matter had you been contacted about the other matter?

A. I don't remember how far apart they were. Maybe within a year, around that time.

Q. Was that, then, the first time you had

heard of Leon Stambler, when you were contacted the first time?

A. Yes.

Q. So you've had an opportunity, then, to read the '302 patent, correct?

A. Yes.

Q. And what would you say is the invention that's being claimed, at least in Claim 51, as it relates to the '302 patent?

MR. GREENSPOON: Objection to form. Best evidence.

THE WITNESS: So you want me to give kind of a high-level description of Claim 51?

BY MR. WILLIAMS:

Q. I'm looking for your understanding of what is being disclosed here as the invention.

MR. GREENSPOON: Same objection.

THE WITNESS: I would -- I would accept the way the claim describes itself, a method for authenticating the transfer of funds.

BY MR. WILLIAMS:

Q. Okay. So any method for transferring

S. NIELSON

funds, then, would be what's invented here?

MR. GREENSPOON: Same objection. Would you accept a continuing objection?

MR. WILLIAMS: Sure, that's fine. I'll stipulate to that.

THE WITNESS: My understanding is that it's a transfer of electronic funds.

BY MR. WILLIAMS:

Q. And is that done via paper check?

A. So the embodiment that is described in the specification is certainly not a paper check.

Q. So show me where in the specification you're seeing something that's not a paper check.

A. Okay. That is incorrect. So it describes as using a paper check. Okay. So there is paper check that is generated. And then -- Well, let me just read what it says here.

Q. Where are you reading from?

A. I was just about to say that. Column 4, line 52. So it says: "Figure 7 illustrates how the originator generates a check in accordance with the present invention. This process preferably takes place at the originator's terminal or computer. It is assumed

that the originator would be generating a check in the usual manner and would include on it all of the information usually found on a check, as well as the information normally recorded or imprinted on check forms such as the recipient's name and TIN," which is the taxpayer identification number, "and the originator's personal account number and bank identification number. Preferably, the terminal includes a check reader and a printer which can read necessary information from the originator's check form and print information on the form."

Q. So that suggests to you that what is being described here as the invention is a paper check?

MR. GREENSPOON: Object to the form.

THE WITNESS: Well, no. Because Claim 51 is about the funds transfer. And in the embodiment, that happens when the paper check is to be cashed, and then it uses an electronic process for doing that transfer.

BY MR. WILLIAMS:

Q. So then what's being described here is

using a paper check and then processing that paper check electronically?

MR. GREENSPOON: Object to the form.

THE WITNESS: I don't know that this excludes an electronic check. I just think that it is also usable on a paper check, and then when you're cashing it, it does the electronic funds transfer described in Claim 51.

BY MR. WILLIAMS:

Q. So was the idea of doing electronic funds transfer new as of November of 1992?

MR. GREENSPOON: Object to form. Also the relevancy.

THE WITNESS: I am unaware of any system that had all the elements of Claim 51. There were other systems that discuss electronic funds transfer.

BY MR. WILLIAMS:

Q. The Davies book talks about electronic funds transfer, correct?

A. The Davies book does describe transferring funds electronically, uh-huh.

Q. Okay. You brought a copy of the

Davies book to the deposition today. Is that one that you had before this case?

A. No.

Q. So did you acquire that for the purpose of this matter?

A. Yes.

Q. Where did you get it?

A. I -- I believe I received it from counsel.

Q. Now, you talked about the TIN earlier in your answer about the '302 patent. What was the TIN?

A. The TIN is -- I believe it is an acronym for taxpayer identification number.

Q. And is that data that's used in the '302 embodiment?

A. Yes.

Q. What's it used for?

A. It's used for identifying the account. So there are two. There is a TIN for the originator and there is a TIN for the recipient, and those are used for identifying the accounts of the person paying and the person being paid.

Q. So does the -- Okay. The person

paying, that's the originator?

A. Yes.

Q. Does the originator have more than one TIN?

A. I'm under the impression that a person can only have one TIN. In the embodiment described in the patent specification there is a one-to-one correspondence between the TIN and the account.

Q. Okay. So the invention that's described in the '302 patent only works if the originator has only one account?

MR. GREENSPOON: Object to the form. Mischaracterizes the testimony.

BY MR. WILLIAMS:

Q. Is that right?

A. I don't think that's the only way it works. I'm saying the way it's described there, it associates an account with a TIN.

Q. Does the '302 patent describe how this invention could work if the originator had more than one account?

MR. GREENSPOON: Object to the form. Relevancy.

S. NIELSON

THE WITNESS: So -- so it doesn't give an explicit description. But in Column 4, starting at line 39, it says: "Various additional information is saved in the user's file, such as his personal account number (PAN), name, phone number (PHN), account balance, and other relevant information. The user's TIN, PAN or PHN can be used as an index to access the user's file."

So the examples that it gives here is with the TIN being the index, and that would have a one-to-one correspondence where you would only have one account per TIN. But if you were using the PAN, for example, then you would have the invention operating the same way but with the PAN instead of the TIN.

Let me qualify that really fast. For this claim, the PAN would also have to be credential information in the previously issued credential.

BY MR. WILLIAMS:

Q. What's the credential that's discussed

in connection with this embodiment of the '302 patent?

A. So the Claim 51 focuses mostly on the credential information. It doesn't describe a lot about the credential here. So the other sections of the specification that describe credential issuing would be how those credentials would be issued. And the non-secret information, the credential information that it's talking about would be, for example, the TIN.

Q. What's the difference between a credential and credential information?

A. Give me just one quick minute to review.

So the credential would be information that is presented for -- a document or information that is obtained from a trusted source that is transferred or presented for purposes of determining the identity of the party. The credential can also contain information that is non-secret information, and that is described as being used in Claim 51.

Q. So your definition of credential used the word "information" in it. I'm trying to

figure out is there a difference between credential information and credential.

A. Sure. So the key point is that the credential has to be the information that is presented for the purposes of determining the identity of a party. But there is nothing that prevents that information from having information within it that, while not identifying -- you know, while not being presented for purposes of determining the identity of a party, or at least it's not sufficient, is not credential information.

Q. So when you say "presented for purposes of identifying a party" --

A. Yes.

Q. -- what do you mean?

MR. GREENSPOON: Object to the form. Misstates the testimony.

THE WITNESS: So a credential, the examples that were given in the specification include things like identity cards or some way where you present it for purposes of establishing that you are who you say you are.

S. NIELSON

BY MR. WILLIAMS:

Q. So for example my birth certificate, would that qualify as a credential?

A. I believe that you could use a birth certificate in the same way that you would use an identity card.

Q. Mr. Greenspoon sitting next to you, if he handed you my birth certificate with my name on it and you had never met him before, would you know that he was falsely presenting that to you?

A. So when we have --

MR. GREENSPOON: I resent the accusation.

BY MR. WILLIAMS:

Q. Go ahead. I didn't mean to accuse him of any wrongdoing. It's a hypothetical.

A. So we have credentials that we use in -- you know, outside of the digital world where, based on the type of credential, we may want more than one. With a birth certificate, that's an example where often you would want more than one credential to establish the identity. But it doesn't mean that the birth certificate isn't being used to establish the identity.

Q. But you agree with me that by itself the birth certificate is not dispositive as to whether the bearer is actually the person he's purporting to be?

A. Right. But when I said that the credential is presented for purposes of determining that, it does not mean that a single credential absolutely establishes the identity of somebody.

Q. I'm looking at Paragraph 31 of your declaration. And this is the section where you're talking about the '302 patent.

A. Yes.

Q. Just for background.

So you're introducing here the idea that the '302 patent discloses more than one embodiment that relates to validating funds transfers associated with a check. Because you say, "How the originating bank validates funds transfer depends on the embodiment." Do you see that?

A. Yes.

Q. So I take that to mean there is more than one embodiment discussed in the '302 patent

that you think are relevant to the validation of funds transfers.

A. So only one of these two is what is described in Claim 51.

Q. Okay. That's what I wanted to find out.

So what are the two that you are thinking of, the two embodiments?

A. So as I describe them here, there is a version where the VAN is decrypted, and then there is another version where the VAN is not decrypted but you reproduce the VAN and compare the two, which is matching the steps of Claim 51.

Q. Okay. So which is matching the steps of Claim 51?

A. The second embodiment that I describe there.

Q. The words you used in Paragraph 32 were "regenerate the VAN," right?

A. Sure, that would be correct.

Q. So one embodiment does a regeneration of the VAN, correct?

A. Yes.

Q. So in that case, regeneration means

that it was generated -- that that's at least the second time the VAN is being generated?

A. Yes.

Q. And so when is the first time the VAN is generated in that embodiment?

A. So the VAN is generated the first time with the -- before it is sent to the originating bank.

Q. So let me talk about the other embodiment. The one you talked about is decryption I think; is that right?

A. Yes. Well, the word is "decode," but it's similar to decryption.

Q. The way the patent talks about it is decoding?

A. Correct.

Q. Can you explain that embodiment to me? How does it work? And you can refer to the figures of the patent if you need to.

A. So as I describe here in my report, what happens is that you have the receiving bank that receives the VAN decoding it. And so that would be similar to decrypting. And then that information can be validated once it's decrypted

with the other information that was sent.

Q. And how would that work?

A. Well, so the VAN would be some encoding of the other information that's being sent.

Q. So then in that embodiment -- Where is this taking place, by the way?

A. This is the originating bank validating the funds transfer.

Q. So in that embodiment, the originating bank receives the VAN and the information that's encoded in the VAN, correct?

A. For example, that would be like what's in the check or the TIN.

Q. So the check data?

A. Something like that, yes.

Q. So that's received separate from the VAN?

A. Or together with it, but not -- In other words, you receive the VAN, which is some amount of encoded information, that when you decode it you can verify it against the other transmitted information.

Q. So when you decode the VAN in that

case, what comes out of that process?

A. Let me check the figures here.

So Column 5 -- Let me make sure I'm looking at the right -- So Column 5, which is referring to Figure 7, describes the creation of the VAN starting about line 19. "The data output of the coder" -- that's where they use the term "encoding" and "decoding." They have a coder and an uncoder, which in the figures you'll see is a C for coder and a U for unencoder.

"The data output of the coder 30 is a variable authentication number (VAN), which codes the information to be authenticated, based upon information related to the recipient and information related to the originator. Note that the VAN is alternatively generated directly from INFO and information associated with at least one of the parties, without the intermediate step of generating the JK," which is a joint key. "The VAN and at least a portion of the information relevant to the transaction are written or imprinted upon the check 32, thereby becoming a permanent part of it. Alternatively, the check may represent an electronic transfer of funds or

some other type of electronic transaction. In this case, the VAN and at least a portion of the information relevant to the transaction are included with the electrical signals associated with the electronic transaction."

So in this case the coding takes its input, some of the financial information and some of the information relative to one or both of the parties.

So you want me to describe how that's decoded?

Q. Uncoded.

A. Uncoded? Sure.

Q. Well, I'm really interested in knowing what is the output of the uncoding operation, then.

A. Sure. Let's jump down in Column 5 to line 55 where it starts describing Figures 8A and 8B. "Figures 8A and 8B illustrate the authentication process at a terminal when the recipient presents the originator's check to be cashed. The terminal communicates via a network of the banks involved in the transaction. Preferably, the terminal includes a device which

can read information directly from check 32."

Now, as I said earlier, that can be an electronic check or, if it's the paper check, it would be reading the VAN off the -- the printed VAN off the check.

"Alternatively, the terminal operator can manually key information into the terminal, based upon information appearing on the face of the check..."

I'm going to skip ahead just a little bit.

Okay. We need to move over to Column 6, starting at about line -- I guess that's 66. "In the same manner as coder 28 of Figure 7, coder 56 therefore produces the joint key JK. JK is applied as the key input to an uncoder 58, which receives the VAN from check 32 as its data input. Uncoder 58 therefore reverses the coding operation performed by coder 30 of Figure 7. If the information on the check has been unmodified, the coder 58 should therefore reproduce the information INFO from the check which was sought to be authenticated."

Q. So is that then explaining that the

uncoder -- if the process worked, then the output of the uncoder is the information which is the same as the information that came from the check?

A. So for this embodiment, it would be some subset of that information. I don't think it has to be the complete information.

Q. But some subset would need to match in order to verify that the check is authentic?

A. That's what I believe it is saying there, yes.

Q. So that embodiment is the one that is actually shown in Figure 8B, right? So box 58 of 8B is the uncoder that you were just referring to, right?

A. I'm sorry, I was looking at 8A.

Q. 8B. Box 58 is the uncoder you were just referring to?

A. Yes, that appears to be correct.

Q. And that's showing that the output of the uncoder (U) is INFO, and that's the same as the INFO that's coming into the comparator box 60 from the check?

A. Yes.

Q. And this is the embodiment that you're

saying is not covered by the claims?

A. Yes.

Q. Okay. So where is the embodiment that is actually covered by the claims?

A. So in my report I describe the lines here. Let me just double-check what they are. It looks like we're back to Column 7.

Right. Yes. So starting on line 12, just a little bit farther from where we were reading: "Alternatively, the joint key JK from the coder 56 can be used to code the information (INFO) from the check to generate a new VAN, which can be compared with the VAN from the check to authenticate the check."

Q. That's the embodiment that you believe is covered by the claim?

A. Yes.

Q. Okay. And why is the first one not covered by the claims? What is it in the claims that leads you to believe the claims don't cover that embodiment?

A. Because Claim 51 is describing what's happening at the originator's bank when they're verifying the information. And so when it is

generating a variable authentication number, that's that second embodiment.

Q. How do you know that that claim is talking only about what is happening at the originator's bank?

A. Well, I think I've described that at some length in my report. Do you want me to --

Q. So you can't, just looking at the claim by itself, figure out how you concluded that it's only describing activities at the originator bank?

MR. GREENSPOON: Object to the form.

THE WITNESS: Well, I know the basics of my report. If you want me to go into details --

BY MR. WILLIAMS:

Q. Without looking at your report, can you tell me what it is about this claim that leads you to believe it's only describing activity at the originator's bank?

MR. GREENSPOON: Object to the form.

THE WITNESS: Sure. So these four steps that are described here for Claim 51 I believe need to be performed by a single

entity. First of all, just because that's how I interpret the claim language as I read it, but also because that's the only -- that's all I see described in the specification. I don't see a description in the specification for having those steps done by different parties.

BY MR. WILLIAMS:

Q. What about the embodiment that we just read that you said is not covered by the claims? Doesn't that describe exactly that?

A. Well, no. Because we don't have -- we don't have descriptions for how we would do other necessary elements of these steps.

Q. Like what?

A. Well, so for example, take these two steps at the beginning. Right? We receive funds transfer information and then we generate a variable authentication number.

Q. Uh-huh.

A. So my understanding of -- and it's a hypothetical so hopefully I'm stating this correctly. But my understanding of what you're suggesting is that those two would be done --

Well, maybe I should just make sure.

So what way are you breaking up these -- where are you putting the break here in your hypothetical? Like which entity do you see doing which steps?

Q. Well, let's say, for instance, the entity that generates the check does the first two steps, the receiving and generating.

A. Okay. So in the boxes we would have the -- we would have -- that would refer, then, to Figure 7 where it says we're going to create a VAN on INFO.

So if I understand you correctly, you're saying that the receiving funds transfer information would be this arrow of INFO going into Figure 7?

Q. Yeah.

A. And then the output of that VAN is the generating?

Q. Correct.

A. So then we have these other two steps where we say "determining whether at least a portion of the received funds transfer information is authentic by using the VAN and the

credential information."

So the reason why I think that doesn't work is because we've got the received funds transfer information which -- So okay. If we look in the first limitation, we have the receiving the funds transfer information. And then in steps 2 and 3 where we have generating and determining, it says that we're generating using the received funds transfer information and we're determining on the received funds transfer information.

So in my mind, those two steps both depend from the receiving step. It depends -- I'm not trying to use a legal word. What I'm saying is that the generating has to be on the received funds transfer information, which refers to the first step, and the determining the received funds transfer information also refers to the first step.

So we would have to have the same entity doing the generating and the determining because they're both doing it on the same piece of information.

Q. Okay. That's helpful.

S. NIELSON

MR. GREENSPOON: It's been probably an hour.

MR. WILLIAMS: I think it has been an hour. Do you want to take a break?

MR. GREENSPOON: Sure.

MR. WILLIAMS: Why don't we take five minutes.

(Recess taken.)

BY MR. WILLIAMS:

Q. So I understand now how you're getting to this conclusion. Let me just ask you a couple more questions about it.

If MasterCard were to perform the algorithm that's shown in Figure 8B, as disclosed here in Figure 8B, they wouldn't practice the claim, right?

A. I --

MR. GREENSPOON: Hold on. Object to the form. Relevancy.

Go ahead.

THE WITNESS: I would -- I don't know how to answer the hypothetical without actually seeing the system to evaluate it.

MR. GREENSPOON: Also improper

S. NIELSON

hypothetical. Let me add that objection. Incomplete.

BY MR. WILLIAMS:

Q. So you don't know what system actually implemented Figure 8B from reading the patent?

MR. GREENSPOON: Object to the form.

THE WITNESS: Well, I think what I'm saying is that when I look at Claim 51, I think I've described which written description I think that is. So obviously if there is something that doesn't practice the steps of Claim 51, then it doesn't practice the steps of Claim 51. But it's hard for me to give a hypothetical answer without seeing more details.

BY MR. WILLIAMS:

Q. Is there any figure in the patent that discloses the algorithm that you say is what practices Claim 51?

A. Well, so I think the way that the text in Column 7 lays it out is that Figure 8B is still more or less correct. The only difference is that, you know, it's a fairly common computer science approach to compare a hash or something

of -- you know, some coding. And so Figure 8B is still a very accurate read, it just has got a slight change to how it does the verification of the VAN.

Q. So step 58 and step 60 would not be performed the way that they're shown in the figure, in accordance with the embodiment that you believe is disclosed in Claim 51?

A. Yes, that is my understanding.

Q. Okay. And there is no other figure that shows the algorithm that you believe practices Claim 51?

MR. GREENSPOON: Object to the form, algorithm.

THE WITNESS: I don't -- I don't believe there's another one that has it in total, but I believe there are other places in here where there is comparison of two VANs. I would have to look. Do you want me to go ahead and look?

BY MR. WILLIAMS:

Q. Sure, why don't you go ahead and look and tell me where you see that.

A. No, I guess they do not have any

examples of comparing two VANs in the figures that I can find.

Q. So earlier you said you might have looked at district court opinions interpreting the claims, the language of the claims.

A. Yes. I was trying to think if I've ever seen any.

Q. Do you recall now either way if you did?

A. I don't know. I don't think I have.

Q. Do you recall seeing any district court opinions that interpret the claims such that all four steps of Claim 51 must be performed by the same entity?

A. Well, like I said, I don't think I've seen any, so that would exclude that.

Q. Let me ask you about the claim construction standard you applied. You refer to this starting around Paragraph 41 of your declaration.

A. Yes.

Q. In Paragraph 43 you say that the BRI does not apply to the terms of the '302 patent. And BRI there means broadest reasonable

interpretation. Do you see that?

A. I do.

Q. And you go on to say that the terms must therefore be interpreted according to traditional construction.

What does that mean?

A. So I'm not a lawyer. I'm basing this on information that I understand --

Q. Let me rephrase the question.

What is your understanding of what the distinction is between BRI and traditional construction?

A. So as I say in here, I've worked in other IPR proceedings where it has been the BRI. And the understanding that I have had is that you try to interpret the claims as broadly as you think they could be conceivably interpreted, whereas my understanding is in this IPR, because the '302 patent has expired, that you do not apply a BRI to the claims.

Q. Okay. Is there a difference between BRI and traditional construction?

MR. GREENSPOON: Object to the form.

BY MR. WILLIAMS:

Q. In your view?

A. Well, I don't know the legal -- how I would describe that legally. Certainly when I've been working with IPRs where I've used a BRI, I will just say generically that it's been a very broad interpretation of claims, whereas when I've been working in cases that do not use BRI, it's usually more narrowly focused in some way or another.

Q. Have you worked on cases that are in district court rather than in the Patent Office?

A. Yes.

Q. And what's the standard that you've applied in the district court cases that you've worked on?

A. Well, again, based on what I'm told by counsel, once the court has issued a Markman -- I've actually worked on cases where they don't issue a Markman before the report is due, which is difficult. But generally speaking, when there is a court's claim construction, then the way the court construes the terms is how I use those terms in coming to my opinions.

Q. And in the cases where there hasn't

been a construction before you've had to write a report, then what's the methodology you use in those cases to interpret the claims?

A. In those cases what we did is we actually analyzed it using both the -- you know, the counsel that I was working with, their proposed constructions as well as the opposing counsel's proposed constructions. And so we would actually do an analysis based on both views.

Q. So do you have any understanding of how a district court case is supposed to interpret claims, what the methodology they're supposed to use is?

MR. GREENSPOON: Are you going to spend a lot of time on this line?

MR. WILLIAMS: No. But I think it's important that we have an understanding of the witness's understanding since he relies on it.

MR. GREENSPOON: Well, I will repeat the objection --

MR. WILLIAMS: That's fine.

MR. GREENSPOON: -- to the form. The

form objection is based on calling for legal conclusions by someone who is not a lawyer.

THE WITNESS: No, I don't know how a district court uses their methodology. I mean, I don't know what their methodology is.

BY MR. WILLIAMS:

Q. You don't know how a district court is supposed to interpret claims?

A. I have no legal training in that, no.

Q. Right. Have you ever been instructed on what the methodology is that the district court is supposed to use in interpreting claims?

A. I may have had discussions about it, but I certainly have no knowledge that I can rely on.

Q. Okay. What is a digital signature?

A. Similar to what I said about public key cryptography. It's a broad term. When people think about digital signatures in the computer science world, most typically what pops up is doing something like an RSA signature or at least, you know, contemporary.

Q. Contemporary? What do you mean,

"contemporary"?

A. Well, the idea of digital signatures has undergone some evolution in how it's used over the last couple of decades.

Q. All right. Let me just turn your attention back to November 1992. What was a digital signature at that time?

A. So there was a lot less of a standard for how it was done, especially because it was used so much more rarely. Nowadays just about everybody is using digital signatures all the time and so it's been standardized.

But the basic idea is that you attach some kind of cryptographic authentication code that in one form or another allows you to determine -- usually it's going to determine that the message has not been altered, and then it sometimes also means that you know more or less who is the author of the message.

Q. In 1992, were digital signatures known?

A. Like I said, it's a broad term. Digital signatures were definitely used in 1992.

Q. And at that time, if someone of

ordinary skill in the art were to hear the term "digital signature," would they understand that that's the result of a cryptographic operation?

A. Yes. Almost always you would have to have some kind of cryptography to have it be a real signature. Otherwise you would usually just call it an authentication code. Even that might be cryptographic. But digital signature, the connotation is almost always cryptographic.

Q. Would a digital signature, then, in 1992, typically have been performed using some sort of computing device?

A. Yes.

Q. What's an error detection code? And then again I'm going to turn your attention to November 1992.

A. Sure. Error detection codes are even older. They've been around for a very, very, very long time. Again, it's very broad. It really refers to any type of system where you can detect that an error has occurred. Usually it's some data that's sent along, extra maybe. Even a parity bit some people might have considered a very primitive form of an error detection code.

Q. Would a digital signature in 1992 have performed the function of an error detection code?

A. Well, it depends.

Q. Are you finished with that answer?

A. I'm thinking. I'm thinking.

Let me -- I want to double-check my report. I think error detection code has a...

Q. Sure. I will let you know I think Paragraph 56 is where I see it used. It may be other places, however.

A. Right. So are we talking about error detection code in the context of this patent?

Q. Sure. Do you think the patent uses the term "error detection code" in a specialized way?

A. No. I would say that this definition is very natural for error detection code. But like I said, because it's so broad, I'm sure that you can find somewhere some computer science reference that would use something slightly different. But I'm saying that this is a very, very good definition of error detection code.

Q. Would this definition cover a digital

signature?

A. Yes.

Q. And why do you say that?

A. Well, the definition here, it says "the result of applying an algorithm for coding information that when applied to original information creates coded information." Let's go that far.

So most of the time when you have a digital signature, it operates on the original information and produces some kind of code or extra information. "Wherein changes to the original information can be detected without complete recovery of the original information."

If somebody changes a message that has a digital signature, then you will be able to tell that it's changed but you can't necessarily recover what the original message was.

Q. That's fine.

Let me ask you to turn to Paragraph 61.

A. Okay.

Q. The very last clause of that paragraph reads: "Counsel informs me that claims cannot be

of a broader scope than the invention described by the specification."

Do you see that?

A. I do.

Q. What did you understand that to mean? Is that a way that you can interpret what the claims mean?

MR. GREENSPOON: Object to the form.

BY MR. WILLIAMS:

Q. Well, let me ask you this a different way.

Did you use that principle in determining what the claims mean in this case?

A. I'm not entirely sure I understand, only because -- I'm just trying to make sure I understand. In this paragraph I'm talking about enablement. I don't -- I mean, I definitely use the specification to interpret the claims, but I don't -- I don't think that I was using this information from counsel to interpret the claims.

Q. So what was the purpose of putting this paragraph here? How did it influence your opinion?

A. Because my understanding is that there

is a difference between enablement and interpreting what the language in claims mean.

Q. Did you provide an opinion about enablement in this proceeding?

A. So as I explain in the next paragraph, I say that there is not sufficient written description to enable Claim 51 where multiple entities divide up the performance. So whatever that means legally, that's what I did.

Q. Okay. So it was based on the fact that the specification doesn't enable multiple entities to perform the claims, you determined that the claims therefore were limited to a single entity? Have I said that correctly?

A. I don't think that there is enough written description to enable multiple entities performing those steps.

Q. Okay. I tell you what, let's table that for one second. Let me just go back to the error detection code very quickly.

A. Okay.

Q. The idea that a digital signature can function as an error detection code, do you think that was well known in the art by November of

1992?

A. The only reason I'm hesitating is because even though you can use a digital signature as an error detecting code, that's not how it's normally used. So normally an error detection code is for -- I'm just saying -- Let me rephrase.

Let me say it this way. Digital signatures were known in the art in 1992, and I'm sure that if you asked somebody if a digital signature would catch errors in a message, they would say yes.

Q. Is a message authentication code an error detection code?

A. Yes.

Q. Let me ask you to turn in Davies to page 261.

A. Sure.

Q. In this section of Davies he's talking about digital signatures; is that right? This is in Chapter 9 which is entitled "Digital Signatures."

A. Yes.

Q. So on page 261 in the middle of the

page there is a paragraph, and the second sentence reads: "In principle, the signature provides error checking."

Do you see that?

A. Yes.

Q. Does that indicate to you that Davies at least understood, by the time he wrote this, that a digital signature could be considered an error detection code?

A. Yes. The reason why I'm being hesitant is because we often distinguish between errors, like line errors, like random errors, versus forgery or malicious alteration. There are a lot of error detection codes that detect when things have gone wrong accidentally but won't deal with malice. Digital signatures were designed specifically to deal with malice. And so that's the reason why I've been kind of differentiating between the two.

Here where he's talking about errors, he is talking about forgeries. It even says that in a previous paragraph. That's the only reason that I was being a little hesitant on the distinction.

S. NIELSON

Q. Okay. But it would also capture accidental errors, correct?

A. It would. The thing is that most of the time by the time you've gotten to where you're checking the digital signature, there are other error detection codes that have already caught accidental errors.

Q. I see. Let's go back to Paragraph 62.

A. Sure.

Q. Okay. You say: "A person of ordinary skill in the art would not have sufficient written description in the specification to enable implementing Claim 51 such that multiple entities divide up the performance of the comprising steps."

Do you see that?

A. Yes.

Q. And you stand by that today?

A. Yes.

Q. Now, we've already looked at the disclosure in the specification of the generation of the VAN and the subsequent authentication of the VAN by two different entities, didn't we?

MR. GREENSPOON: Object to the form.

S. NIELSON

BY MR. WILLIAMS:

Q. Do you remember our discussion about that?

A. I do. I do. I don't know that I think that that reads on the elements of Claim 51.

Q. Right. And I think you explained why not already; is that right?

A. Yes.

Q. Because of the receiving step being necessary to the determining step?

A. Yes.

Q. And that's the reason that you conclude that there's not sufficient written description to allow multiple entities to divide up the performance of authentication test?

A. No. Because I think there are ways that the language of the claim doesn't necessarily prohibit dividing it up, but that it would require -- that there's not enough written description to know how to do that.

Q. You say in your last sentence that there would be undue experimentation required.

A. Right.

Q. What do you mean? What is the gap that would need to be filled in?

A. Sure. So in situations where you're going to have security -- So when I talk to my students about security, I always tell them it's all about the context. Once the context changes, you have to almost start over because everything changes.

And so if you've got secure information that was originally all being handled by one entity and then you split it up and start sending it off to other entities, then that's -- that's a very, very, very challenging problem.

Q. Sure. But that's not what's being described in the '302 patent, is it?

A. Well, I think that if you look at the steps of Claim 51 and their description as being performed by a single entity, when you break that up and you have to transmit sensitive data around, I think that that requires undue experimentation.

Q. What's the sensitive data that you're talking about?

A. So let's look at maybe steps 3 and

4 for example.

Q. I don't have the numbers down.

A. Oh, I'm sorry. So the determining step.

Q. Is that step 3?

A. Sure. I've listed it just because of the way it's visually depicted.

Q. That's fine. I just wanted to make sure I know what you mean.

A. Sure. So I was referring to receiving a step 1, generating a step 2, determining a step 3 and transferring a step 4.

Q. Okay. So go ahead.

A. So if you were to take the determining step and the transferring step and split those off into two separate entities, that is not at all clear how that would be done correctly for one of ordinary skill in the art.

Q. Okay. Well, let me just change the hypothetical to make sure we're not talking about different things. So I want you to consider the hypothetical where steps 1 and 2 are performed by one entity and steps 3 and 4 are performed by a second entity.

S. NIELSON

So in that hypothetical, do you still think that there's a lack of written description in the specification to enable that?

MR. GREENSPOON: Object to the form.

THE WITNESS: So if we have steps 1 and 2 done by a different entity than steps 3 and 4, I think I've already identified one of my concerns with it, which is that I don't think that reads correctly.

But if you're going to have -- so where you have the -- So I don't think there is written description to describe how you split that up between those two entities.

BY MR. WILLIAMS:

Q. All right. Do you have the patent?

A. Yes, I've got it.

Q. Let's just start with the basics. So how is the check being presented in this embodiment? Like physically where is the check showing up to begin this process?

A. So the word "check" isn't in Claim 51, but you're just referring to the embodiment that I --

Q. So the embodiment that's described

that you say corresponds to Claim 51 involves a check, doesn't it?

A. Yes.

Q. Okay. So that's the embodiment that I want to talk about it.

A. So it says that it's a check for -- it says it can be an other electronics funds transfer.

Q. Sure. That data, where is it first presented in this process?

MR. GREENSPOON: Object to the form. And to clarify, do you mean the completed check that has a VAN with it?

MR. WILLIAMS: That's what I mean.

BY MR. WILLIAMS:

Q. Is that what you understood?

A. I was just finding my place here first. Give me a second.

Q. Sure.

A. I just want to make sure I'm in the right place.

Q. I'm looking at Column 5, line 55, where the idea of Figures 8A and 8B are kind of introduced. It says they "illustrate the

authentication process at a terminal when the recipient presents the originator's check to be cashed."

Do you see that?

A. I do.

Q. So that's kind of what I was thinking of here. Is that what you're thinking of?

A. Right. So this would begin the electronic funds transfer -- Let me think about that for a minute.

Q. Okay.

A. Yes. So this would begin the electronic funds transfer process starting with the check being presented to be cashed.

Q. And there is a reference to a terminal here, right? Do you see that?

A. Yes.

Q. What is a terminal? Does that have a meaning in connection with this patent?

A. So I think earlier they described it, for example, as something that you would have with, like, a check reader if you've got a paper check. But in the case where it's just an electronic transaction, it would just be able to

receive the electrical signals.

Q. Okay, fair enough.

Is that at the bank that's going to be doing the steps of Claim 51?

A. No. No, it's not.

Q. Where is the terminal in this embodiment?

A. The terminal is at the -- so I would guess -- So it says here that the terminal communicates via a network of banks involved in the transaction. That makes it sound like its location is not necessarily fixed.

Q. So just looking at Figure 8A there is something called a recipient's terminal, right? If it helps you to unstaple that exhibit, you're welcome to.

A. 8A, recipient's terminal. Okay.

Q. So is that the terminal where the check data is received?

A. Well, for purposes of Claim 51 where we're talking about receiving funds transfer information, it's not there.

Q. Okay. So where in Figure 8A and Figure 8B does the step of receiving funds

transfer information take place?

A. So let me just line this up with the text here. But I think I've got it. Give me just a second here.

Okay. So there is -- But that's not the funds transfer. That's just the identity. They don't put a number on the little CPU there.

Okay. So yes, block 71. Okay. So in the text of the bank -- in the text of the bank, I apologize. In the text of the patent there is first an initial check on the originator. So at the originator's bank there is a check on the originator's identity. And then after that, it transmits the funds information.

Q. I'm sorry, at the originator's bank there is a check of the identity, you said?

A. Yes. So the recipient -- In the Figure 8A here there is a transmission from box 48 to box 62.

Q. Uh-huh.

A. That's from the recipient's terminal through his bank. You know, there is some check of his bank. But then there is a transmission to the check writer's bank, which is the originator.

S. NIELSON

Q. I see. So that step you refer to, step 71, request authorization to pay, that step is performed at the recipient's bank, correct?

A. No. It's performed at the originator's bank.

Q. Step 71 in Figure 8A, you're saying that's happening at the originator's bank?

A. Yes.

Q. You're sure? Do you want to take some time to read the embodiment before you commit to that?

A. Oh, I see. Okay. Right.

So the transmission there is from the terminal to his bank, and then the transmission from the bank to the originator's bank.

So Figure 8B is the originator's bank.

Q. Okay. So you agree with me step 71, that's happening at the recipient's bank?

A. Recipient's bank then communicates with the originator's bank conveying all the information about the transaction and requesting an authorization to pay. That is Column 6, lines 43 through 45. Yes. And that says it's block 71.

S. NIELSON

Q. So doesn't that disclosure show you that in this embodiment there are communications between multiple entities to carry out this transaction?

A. But there was no VAN generated on this received funds transfer information.

Q. Right. That happens at the originator's bank?

A. Yes.

Q. Okay. But clearly what Mr. Stambler in his patent has disclosed here is a system where all of the data is communicated from the recipient's bank to the originator's bank.

A. Well, yes. But I'm not saying that that meets the first limitation of receiving the funds transfer information.

Q. No. But you said earlier that he didn't provide a written description that would allow multiple entities to send data around because it's so sensitive. And in fact he does disclose that, doesn't he?

MR. GREENSPOON: Object to the form. Mischaracterizes the testimony.

THE WITNESS: What I'm saying is the

S. NIELSON

steps of Claim 51 are not disclosed being done by separate entities.

BY MR. WILLIAMS:

Q. Right. And you say that because where he actually does disclose the steps of Claim 51 being done by separate entities, that's actually not covered by the claims, right?

MR. GREENSPOON: Object to the form. Mischaracterizes the testimony.

THE WITNESS: I didn't say that he disclosed those steps being done by separate entities.

BY MR. WILLIAMS:

Q. But he does disclose an embodiment, and in fact it's the embodiment that's shown in Figures 8A and 8B that you say is not covered by the claims?

A. Well, he shows an -- the embodiment where it's being -- It's not even still being done by separate entities there. It's still all being done at one entity. You still have the check arriving there, the VAN being decoded. It's not covered by the claims, but I don't see it being done by separate entities.

Q. Let's just assume that the way the claim reads is that the receiving funds transfer information and generating step are done when the check is created and then steps 3 and 4 are done at the originator's bank. I know that you disagree that that's a proper way to read the claim, but my question to you is: Is there a written description for that reading?

A. Well, no. Because you have to have the generating of the VAN before you transmit.

Q. Uh-huh. Figure 8B shows exactly that, does it not?

A. No. Figure 8B shows that you have a VAN that has been received.

Q. Figure 8B shows a VAN being transmitted into this box U, does it not?

A. Yes. But that VAN has been received. It wasn't generated.

Q. So you're saying that even though the VAN somehow magically appears on the figure, it actually hasn't been generated yet?

A. I'm saying it wasn't generated at the recipient's bank.

Q. Okay. But you agree with me that the

VAN shown in Figure 8B was generated before it gets transmitted to box 58?

A. Yes.

Q. Okay. So now the question to you is: If you were to assume, putting aside -- I realize you disagree that this is a correct reading of the claims. But if you assume the claims could read on steps 1 and 2 being performed by one entity and steps 3 and 4 being performed by a different entity, that that has written description in the specification?

MR. GREENSPOON: Object to the form. Improper hypothetical.

THE WITNESS: No, I still think that there is not enough written description, and I'll show you why. If you look at 51 and you look for --

BY MR. WILLIAMS:

Q. I'm sorry, 51 --

A. Claim 51. I apologize. Claim 51, step 4, where it says that we transfer the funds, it says "if the funds transfer information and the VAN are determined to be authentic." What is described here would not authenticate the VAN.

Q. Why do you say that?

A. Because the VAN isn't determined to be authentic in this description, only that the check information matches it.

Q. How could the check information match the VAN if it wasn't authentic?

A. Because a forger could -- if you have an unsecured line, a forger can transmit a fake check but with a legitimate VAN for that fake check. For example, maybe with a replay attack or something like that.

Q. But in that case the VAN would still be authentic. You're replaying an authentic VAN.

A. But you don't check the VAN. There's no check on the VAN to determine if it's authentic. Just because it uncodes is not authentication.

Q. What's the difference?

A. So what I see described here in Figure 8B is that you do a check on the INFO but not a check on the VAN. Those are separate checks. There is only a check here for the check on the INFO.

On the other hand, where you have a

situation where you compare the VAN to a regenerated VAN, you're checking both the VAN and the data.

Q. So can you think of any other situations where the VAN, the decoded VAN, would match the information on the check other than a replay attack?

A. Not off the top of my head.

Q. Let me do this. Let's turn to Paragraph 66.

A. Sure. Of my report?

Q. Yeah, your report.

A. Yes.

Q. You say a couple of things in this paragraph, and I want to see if you're going to stand by them.

In the second sentence you say: "One entity receives the funds transfer information and another entity then determines the VAN."

Let me back up. First of all, what does "determine the VAN" mean here?

A. Generate the VAN.

Q. I see. Then "The claims and specification do not describe how the funds

transfer information gets from the first entity to the second."

Do you still say that that's true?

A. Yes, that is correct.

Q. So there is no description in the patent of how funds transfer information gets from the entity that generated the check to the originator's bank?

MR. GREENSPOON: Object to the form. Mischaracterizes the testimony.

THE WITNESS: What I said is, if one entity receives the funds and another entity determines the VAN, generates the VAN, it doesn't describe how the funds transfer information gets from the first entity to the second. That is correct.

BY MR. WILLIAMS:

Q. Does the patent describe how the information gets from the entity that generated the check to the originating bank?

A. Can you ask that question again just to make sure I understand it.

MR. WILLIAMS: Can you read it back?

(Whereupon, the requested portion was

S. NIELSON

read back by the Reporter.)

THE WITNESS: So to be clear, you're talking about when the check is generated, like when it's created, when it's written? Like with Figure 7?

BY MR. WILLIAMS:

Q. Yes.

A. Okay. And you're asking if there is anything in the specification about how the check gets back to the originating bank?

Q. How the information from the check gets to the originating bank.

A. Yes.

Q. There is a description of that, right?

A. Yes.

Q. The funds transfer information is on the check, right?

A. Yes.

Q. And the VAN is on the check, correct?

A. Yes.

Q. Let me ask you about another sentence here in Paragraph 66.

A. Yes.

Q. It might be the last sentence. It

says: "Because the VAN is an authentication number, it would have to be transmitted securely."

Do you see that?

A. I do.

Q. How did you reach that conclusion?

A. Okay. So if the VAN is being determined if it's authentic -- So if I'm transmitting a message along with a signature and I can intercept that, then there are ways that I can take advantage of that. Well, I've given an example already. For example, a replay attack.

Q. And so because of the possibility of a replay attack, you've concluded that the VAN has to be transmitted securely?

A. I'm saying that somebody who is doing a security design has to make sure they've taken all of those factors into consideration, none of which are described in the specification.

Q. Right. The specification doesn't describe transmitting the VAN securely, right?

A. The specification doesn't describe breaking these steps up and having them done by multiple people.

Q. Listen to the question I'm asking.

Does the specification describe transmitting the VAN securely? I can save you some time. The specification describes the opposite, doesn't it?

Look at Column 6, line 12, that paragraph.

A. Oh, I see what you're asking. You're asking if it describes sending it insecurely?

Q. Yes.

A. I see. Okay. So the difference here is that this is describing -- In other words, what's described here by the patent does not necessarily mean that you could translate this unsecured line at this phase into any other place where you broke it up just because it was done somewhere else.

So what I'm getting at is that for somebody who is going to implement the patent, the person implementing the patent doesn't know from how it's being transmitted in one block, if it's appropriate to transmit it that same way in another block. Because when you're doing a secure design, one of ordinary skill in the art

is not going to have the background for designing a cryptographic protocol. So if the way it's written in the specification tells them to do it a certain way, that's fine, but they're not going to go experimenting with it to figure out a way to expand beyond it.

Q. So the description that is at Column 6, line 12 to 16, is describing transmission of the information that's read from the check to the recipient's bank, correct?

A. That is correct.

Q. And that would include the VAN?

A. Yes.

Q. And it says that that's preferably done over an unsecured line?

A. Yes.

Q. So at least in this section of the patent, the way the VAN is treated is that it's perfectly fine to send the VAN over an unsecured line?

A. Well, the VAN is not being sent by itself.

Q. Okay. But it is being sent, correct?

A. That is correct.

Q. And that's the only place that the VAN is sent to the -- that's the only way that the VAN is sent to the recipient's bank, correct?

A. I believe that's the only thing described.

Q. And then subsequently the recipient's bank transmits all that information to the originator's bank?

A. Yes.

Q. Okay. Let me move to some questions about Davies, I think.

A. All right.

Q. So in Paragraph 71 of your declaration there is your discussion of the Davies reference.

A. Sure.

Q. You said: "Although Davies does not say it explicitly, the recipient of the check can only trust the funds transferred encoded therein if he or she also trusts the registry and verifies the chain of signatures."

Do you see that?

A. I do.

Q. How do you know that? Is that just from your knowledge of digital signatures? If

it's not explicit in Davies, how did you reach this conclusion, I guess is my question.

A. Yes, that's my knowledge of public key cryptography.

Q. So by November of 1992, was the idea of a -- Well, let me back up.

So you're referring here to page 328 of Davies. It might help to have that in front of you.

So the first two sections of the check shown at the bottom of 328, fields 1 through 8, is that a signature chain that you're referring to in that sentence of Paragraph 71?

A. So in computer science we would commonly refer to this as a signature chain.

Q. And why is it called a signature chain?

A. Well, public key cryptography is great but it still has kind of a point of failure, and that is how do you know to trust the key that signed it. Right? You've got this public key, but that doesn't mean that it came from the right person.

And so typically the way that -- Well,

so the way that Davies proposed that this be solved is that you have some kind of registry that -- you know, he gives a couple of different examples for what a registry might be. In this particular case, he suggests that it could be like the central bank of a country and they would be some kind of trusted party.

So when you receive something signed by a person, then you see who signed their key all the way back up to somebody you trust.

Q. All right. So Davies does say that this is a hierarchy of keys, right?

A. I don't know if he uses the word "hierarchy," but that's the basic idea.

Q. The middle of 328 it says: "The implementation of an electronic check requires technically little more than a digital signature facility with a key registry to authenticate public keys. A hierarchy of keys is proposed."

A. Yes.

Q. So he does say hierarchy?

A. He does.

Q. The question is: In your sentence in Paragraph 71, you say Davies doesn't say it

explicitly. What is it that's not explicit in Davies about this?

A. So the sentence Davies gives is that anyone can verify the bank's public key using the signature and public key of the key registry. Also, in the same paragraph, that the bank authenticates the customer's public key.

So what I was saying is that it doesn't explicitly say that when you receive a check, if you want to trust it, you first authenticate the check, then you authenticate the signer of the check, then you authenticate the signer of the signer of the check.

Q. Do you think that a person of ordinary skill in the art in 1992 would have understood that idea from the disclosure of Davies?

A. I think so.

Q. So he does talk about the central bank being a key registry. But a few pages later, on page 331, in the middle of the page just before the heading "Development of the Intelligent Token," he says: "If public key signatures come into use first in payment systems that financial institutions will establish key registries."

Do you see that?

A. I do.

Q. So that would be a situation where the banks would set up some sort of key registry system. Is that how you interpret that?

A. Well, I don't see that as really being any different where he's describing it as the key registry being the central bank of a country. I mean, it's a hypothetical, like if this happens, it will look like this.

Q. Okay. So then let me turn to the next page, Paragraph 72 in your declaration.

A. Yes.

Q. You say: "It should be noted what is authenticated by this hierarchy of signatures is funds transfer information, not the individual presenting the check."

What do you mean by that?

A. So like I was describing earlier, the check is not being presented to establish the identity of anybody.

Q. Well, isn't it not being presented to establish the identity of the person who wrote the check?

A. I wouldn't say so, no.

Q. So you don't need to know anything about the person who wrote the check in order to process the check, you're saying?

A. You don't need to know anything more than whether or not it's a legitimate bank account.

Q. Okay. But in fact, the bank has signed the customer's public key and tied that to their identity on the check, right?

A. But that's not even necessarily the identity of the person writing the check. For a personal check, you would often have that kind of -- but even then -- So, for example, if I have a checking account in my name and my wife's name, either one of us may be able to sign for that account. But that wouldn't establish our identity when we present it.

Q. You would agree with me that the way Davies describes this is that the digital signatures in that, for instance, field 8 is to authenticate the public key of the customer?

A. That it is a -- Yes, it is a signed public key.

S. NIELSON

Q. And the purpose of it, according to Davies, is to authenticate that key?

A. Well, again, it's to make -- Yes, you are authenticating that the funds transfer information is accurate. But it's not being presented to --

Q. Let me ask you about paragraph -- sorry, field 8.

A. Sure.

Q. Field 8 is the signature of the bank?

A. Yes.

Q. That signature is generated before there is any funds transfer information?

A. That's correct.

MR. GREENSPOON: I would just ask that you let him finish his answers when he's giving an answer.

BY MR. WILLIAMS:

Q. Was there a part of your last answer that you need to finish?

MR. GREENSPOON: Three or four answers ago. I was waiting for a time to tell you.

THE WITNESS: Go ahead.

BY MR. WILLIAMS:

Q. So it can't be that that signature is authenticating funds transfer information because there's none that exists when the signature is created?

A. Well, that's not accurate, because the purpose of that customer public key there isn't to identify the customer. It's to authenticate the funds transfer information in the next sequence.

Q. What do you mean?

A. Well, the parts 9 through 15 are signed by that customer. The only way that you would be able to trust that funds transfer information is if the bank has also authenticated it, and you only trust the bank if it's signed by this trusted key registry.

Q. Now, you agree with me, though, that the way Davies describes the processing of this check, those signatures are checked during the processing?

A. That would make sense.

Q. And if those signatures don't check, then the funds aren't transferred?

A. Yes.

Q. In Paragraph 74, the last sentence reads: "From the perspective of the recipient it makes no difference for verification purposes if the check was signed by a token or not."

What do you mean there? I mean, if the check is not signed, it's not going to get processed correctly, right?

A. I don't think I meant whether it's signed or not. I'm pretty sure that what this sentence is saying is that it doesn't matter if it was signed by a token or by something else.

Q. Okay. You agree, though, that the electronic check being described in Davies, the recipient only gets their money if the check was properly signed?

A. Yes.

Q. If you could turn to Paragraph 76.

A. Sure.

Q. So Davies talks about this thing, this intelligent token. And that's the token you're referring to back in Paragraph 74, right?

A. Yes.

Q. And that's the thing that Davies says is going to actually be involved in putting this

customer signature onto the check?

A. Well, it said that was one way you could do it.

Q. Do you have an understanding of what this token is that he's talking about?

A. Well, he just describes it as an intelligent token or a smartcard. So these were seen as a bigger deal in 1992, kind of before everybody had smartphones. And the idea was that you would have some little device with some processing power. Depending on the type, sometimes it would have a keypad, sometimes it wouldn't.

In the security community, the idea was that you could keep some secrets with you. Or this one is described as not having -- Well, right. So yeah, private customers of the bank can carry their keys more conveniently, for example, in an intelligent token or smartcard, and then suggests a PIN as a way of protecting secrets on a device.

Q. So the smartcard meaning that it would have some computing capability?

A. Some computing capability.

Q. And memory for storing like the secret key, for instance?

A. There would have to be some memory in it.

Q. Okay. And that's the thing that, in Davies, issues these checks that are being discussed, right?

A. Well, I wasn't always sure that that was clear, because -- well, so it says it's functioning as an electronic checkbook. I felt like there were a lot of details in it that were just left unclear.

Q. Your interpretation, at least as reflected in Paragraph 74, is that the intelligent token is used in issuing checks?

A. Well, certainly you would have to sign it, like you and I both agreed that you would have to sign it. From that perspective, that, in my mind, is when the check is issued.

Q. Fair enough.

You say there are some similarities between the two examples. And I take the two examples to mean an example where you're doing an ATM transaction and an example where you're doing

a transaction at a point-of-sale terminal?

A. That's what I say at the beginning of 76.

Q. Okay. And you say those two examples are similar but are separate and distinct?

A. Yes.

Q. All right.

A. And just to be clear, my exact language was there are some similarities.

Q. All right. Fair enough.

Now, the ATM example, do you agree that it would use the same structure as the electronic check, the same data format as the electronic check shown in Figure 10.22?

A. Well, that is something that I felt it left fairly vague. So, you know, it references Figure 10.22. I'm over on page 331. This is starting about a third of the way into the page. "All the messages carry similar information but their purposes are different. To differentiate these messages and provide for even wider use, the format of Figure 10.22 includes the transaction type." And then it lists some possible transaction types.

It's not entirely clear how changing the transaction type would adjust your format for 10.22.

Q. Well, 10.22, field 10, that's transaction type?

A. Right.

Q. So isn't that the field that's being discussed there?

A. Right. What I'm saying is, you don't need, say, Item 13 or 14 in 10.22, or at least it's not necessarily going to be the same set.

Q. So you say at the bottom of 76 that if the transaction type is an ATM, there would be no need to write payee identity into the check. And that's field 13, right?

A. Field 13, yes.

Q. So I don't understand, though, why you say that. Someone is going to need to be paid, right?

A. Well, if you're doing an ATM withdrawal, then the customer's identity would be the same identity as the payee.

Q. Why do you say that?

A. Because the money is being withdrawn

from the customer's account to be given out in cash.

Q. Right. But the assumption that he's making here is that the customer is at an ATM that is not his bank's ATM, right?

Well, let's make it more concrete. Look at Figure 10.23.

A. Okay.

Q. Doesn't that show you that the ATM is somewhere besides the card issuer bank?

A. Okay.

Q. So wouldn't in fact you need to make a payment to the payer bank in this case in order to complete the exchange?

A. But I don't think that the payment from B to A is what goes into the check payee field.

Q. So how in the world does the issuer bank know who to pay?

A. Well, I don't know -- I'm not saying that there wouldn't be a message between the two. I'm just saying that I don't know that it's the check.

Q. Right. You agree with me that the

thing that's shown in Figure 10.23 is there is a payer Bank A and a card issuer Bank B. That's the customer's bank?

A. Yes.

Q. And those are distinct banks?

A. Uh-huh.

Q. And that Bank A needs to get paid before any money is going to go out of that ATM, right?

A. Yes.

Q. So there has to be some way for the card issuer bank to know who to pay?

A. Yes.

Q. Wouldn't it be logical to put that identity into the check field for payee identity?

A. Well, I don't know that that's necessarily true. I guess I'm still thinking about my paper check example. We don't use paper checks at an ATM, but when you write a check to cash or something, that the payee identity is -- I'm not sure. I don't know.

Q. It would be one way to do it, though, right, would be to identify Bank A in that field 13?

S. NIELSON

A. Well, the reason why that seems odd to me is that this has to work for when you're at your own ATMs as well. So what goes into the payee field then? I don't see that that makes sense.

Q. But in the case where you're not at your ATM, what I just said would work, correct?

A. I'm not sure. I don't know.

MR. WILLIAMS: So we can take a break if we need one, otherwise we can keep pushing through here.

(Off the record.)

THE WITNESS: Let me just add on to that last answer. The reason why I'm not sure is because Davies doesn't describe it. You know, there are a lot of different ways we can conjecture about it, but my point was it's not described.

BY MR. WILLIAMS:

Q. He describes the ATM example as involving making a payment to Bank A, though?

A. Yes, he does.

Q. And that's the bank where -- that's the payer bank?

S. NIELSON

A. Yes.

Q. Let me turn to page 83 of your dec.

A. Okay.

Q. Here you're talking about the petition, so maybe I should try to get that in front of you.

(Petition for Covered Business Method Review incorporated into the deposition record and attached hereto but not marked as an exhibit.)

BY MR. WILLIAMS:

Q. So I've put in front of you the petition which is --

MR. GREENSPOON: This is Petition Number 1. Is that what you intended?

MR. WILLIAMS: Yes.

MR. GREENSPOON: Because there was a corrected petition.

MR. WILLIAMS: There was, but I don't think it's going to matter for the purpose of this question, though.

MR. GREENSPOON: We'll take it as far as we can take it.

MR. WILLIAMS: Yeah.

S. NIELSON

MR. GREENSPOON: We'll just have to sort of object to the document. I don't know if there will be any problems with your question.

MR. WILLIAMS: That's fair enough.

BY MR. WILLIAMS:

Q. I recognize you may not have seen this in this particular format before. But let me just ask you about your Paragraph 83 where you say under the heading "Example 1," the petition cites to a section?

A. Yes.

Q. What were you referring to there? I do have a copy of Paper 7, but it's been marked up. So if you need it, I can show it to you, but otherwise it's easier to work from that.

A. That's fine.

Q. So in this paragraph you're talking about the petition's analysis of the preamble, Claim 51 I believe; is that right?

A. Yes.

MR. WILLIAMS: I think our Paper 7 actually says "Paper 1" on it. At least my copy does. Can I just see this real quick?

S. NIELSON

This one is actually correct, it's just got the wrong caption on it.

MR. GREENSPOON: Okay, that's fine. I'll withdraw the objection. You didn't print in color, though.

MR. WILLIAMS: No. Sorry.

THE WITNESS: So can you be more clear in your question? Which part of my --

BY MR. WILLIAMS:

Q. So I guess the question that I'm really trying to get an answer to -- and now I've misplaced your declaration. Give me one second.

So I'm just trying to figure out, when you say the petition cites to a section of Davies that has nothing to do with electronic funds transfer, what are you referring to? I just can't tell.

A. Example one here says --

Q. "Here" meaning --

A. I'm sorry. This is page 24 of the document in front of me, "Petition for Covered Business Method Review." There is a chart here, and on the left-hand side of the chart it says Claim 51, 51(3)(a). On the right-hand side of

the chart it says: "Example 1. Davies describes that Bill presents the check for payment to his own bank which sends the check to payer's bank. The payer's bank debits Ann's account and the payee's bank credits Bill's." And it says Davies at 10.2, page 285.

Q. Okay.

A. So that section here in 285 is talking about a paper check clearing scheme.

Q. Okay. So 285 of Davies?

A. Of Davies, yes.

Q. So this is in Chapter 10 which is entitled "Electronic Funds Transfer," right?

A. Yes.

Q. So your point, I guess, is just that this example seems to be talking about the pre-existing paper system rather than the electronic system?

A. Well, the subsection 10.2 says established payment mechanisms.

Q. Okay.

A. The first line of which is the three main payment systems in operation today are cash, checks and credit cards.

Q. Okay. So the existing payment systems at the time of Davies includes electronic funds transfers, right?

A. Well, it says that the three main are the cash, checks and credit cards. Then what it describes over here, the bank check, and it goes from pages 285 to 286, all describe paper check handling.

Q. Okay. So now the bank check is introduced at page 285, right?

A. Yes.

Q. And then on the next page, 286, at the end of that paragraph he says, the very last sentence of the paragraph, or the last two sentences of that section: "are changed into a modern form as a message with a digital signature that is going to be regarded as an electronic check. At the end of this chapter we show that this kind of message can be a basis of many different payment systems." Correct?

A. That's what it says.

Q. Okay. And you're saying that this section, then, has nothing to do with electronic funds transfer?

A. Well, the chart that is shown, the Figure 10.1, and the description that is given, was describing the previous system. And even though it's saying it's adapted into a modern form, I felt like by itself without any further information, that it was not describing electronic funds transfer.

Q. And the next paragraph, 84, the second sentence. Here you're talking about Example 2 of the petition.

A. Yes.

Q. The second sentence reads: "While the electronic check does deal with electronic transfer of funds, it does not identify an account associated with a second party."

What's your basis for saying that?

Actually, let me withdraw the question and ask it a different way.

You agree with me that the electronic check in Davies includes data to identify the second party?

A. Yeah, it includes a payee identity.

Q. I'm sorry. So is the second party here the payee or is it the drawer?

A. It's the payee.

Q. Okay. You're basing that off of the way the claim talks about the first party and the second party, right?

A. Let me make sure. Yes, a transfer of funds from an account associated with a first party to an account associated with a second party.

Q. Okay. So the Davies check doesn't identify an account of the person being paid? That's your point?

A. Yes.

Q. I got it. Okay.

The payee, however, is identified in the Davies check?

A. It has an identity field for the payee, yes.

Q. All right. In Paragraph 86, the last sentence says: "Davies never ties together paper checks and key registries."

So the electronic check in Davies includes a signature of a key registry, right?

A. The electronic check includes a signature by the key registry.

Q. And you agree with me that Davies does tie together paper checks and electronic checks when it says on page 286 that you could change the paper check into modern form as a message with a digital signature?

A. Well, I don't know that that goes in reverse. I don't know that you apply digital signatures to paper checks.

Q. Isn't that what Davies tells you to do, convert a paper check into a modern check by using digital signatures?

A. Well, no. I would say that he's saying to convert it into an electronic check with digital signatures.

Q. Right. I'm sorry, maybe I just didn't understand your last answer.

So Davies teaches that you can take a pre-existing paper check and convert that into a more modern form by making it electronic and using digital signatures?

A. Yes.

Q. Okay. In Paragraph 89 -- We've talked about this already a little bit. It says: "The check is not presented for purposes of

establishing or determining the identity of the party."

A. Yes.

Q. And here I think we're talking about the party who wrote the check, the drawer of the check, right?

A. Correct.

Q. Okay. So again, when the check is presented to the originator's bank, it's done so that the originator can determine whether to transfer funds, right?

A. Right. But it's not being presented to establish the identity of the party presenting it.

Q. Well, doesn't the originator need to determine which account to draw the funds from?

A. Yes. But that's not necessarily the person presenting it. Right? What I'm saying is that anybody can present this check, and that's not used to establish the identity of the person presenting it.

Q. But it is used to establish the identity of the person who wrote the check?

A. Certainly the identity of -- it would

need account information one way or another.

Q. Account of the person who wrote the check?

A. Correct.

Q. And the last part of that paragraph reads: "There is no evidence in Davies that a check is a certificate."

So we talked about certificates a little bit in connection with Paragraph 91, but I guess I'm not sure what this means. Would you agree with me that in Davies the check includes the certificate in the check data?

A. So Davies definitely uses the word "certificate." And in fact the way it reads, it says these first basically four fields are in effect a certificate by the key registry which authenticates the bank's public key.

Q. So the check includes a certificate?

A. It includes a certificate on the public key.

Q. All right. In Paragraph 91 -- this is the one we already spoke about. You've explained that last sentence previously, right?

A. Correct.

Q. So do you agree, then, that the bank, in Davies, issues a certificate that is included in the check data?

A. I'm not sure. I think -- I mean, the reason I'm not sure is because I don't know why but Davies chose to describe the first entries as a certificate but didn't choose to describe the next entries as a certificate. So I've been -- I'm not certain. It could be, it might not be.

Notice that even for the first one, it doesn't say it's a certificate. It says it's in effect a certificate. He's not giving a rigorous description of a certificate there, so I'm not sure.

Q. Looking around Paragraph 96 and 97 where you're talking about the token in Davies.

A. Yes.

Q. And you say -- for instance, 97, you say the token would not need to have the customer input things like customer identity.

So are you saying that in that case the token would just store that information already? It's prestored onto the token?

A. That's certainly a possibility.

Q. And that's the sort of thing that could be done by the intelligent token that Davies is describing?

A. Yes. Basically, kind of like they described, you would have a drawer of checks where it would have the preset information. It's entirely possible for that to be stored in the token, and then you only need to fill out the fields that are changing.

Q. Well, one of the fields that changes is the check number, right?

A. Yes.

Q. And Davies describes that that can be controlled by the token, right?

A. Where is that line that you're referring to?

Q. Let me find it for you.

A. I'm not saying I disagree. I would just like to -- Because I felt like it left a lot of details about what was in the token --

Q. Yeah. So I'm looking at page 330, the bottom of that page. "If digital signatures have a weakness," that paragraph.

A. "If digital signatures have a weakness

it is the fact that signed documents can be copied, and this places on the issuer bank the requirement to detect and eliminate duplicate checks. The check sequence number is administered by the intelligent token and is therefore as secure as the customer's secret key."

Q. So you agree, right, that Davies talks about how that check number can be administered by the token itself?

A. Yes.

Q. And that's the data that gets populated into field 9?

A. Of Figure 10.22, yes.

Q. In Paragraph 98 you say -- I think this is maybe the second sentence. "It does not say what form that request or message takes."

A. Yes.

Q. What message are you talking about?

A. In the example that it gives on pages 330 to 331, it does not describe what information is given to the ATM -- I'm sorry, is given to the token and how the token processes that.

Q. Okay. I just wanted to make sure I

understood that this is talking about the data going into the token. That's what you're referring to here, right?

A. Yes.

Q. Okay.

A. Yes.

Q. You agree with me that the output of this process would be this electronic check format?

A. In some form. I'm not -- I'm still not entirely clear on exactly how the fields might change. But it describes it in Davies as being something similar to 10.22.

Q. So the token -- What was the technology as of 1992 that existed in terms of tokens or smartcards?

A. Well, it's kind of interesting because unrelated to this case I've done reports and studies on tokens, and there was actually a lot of discussion and debate about exactly what form they should take. There were issues with, you know, you could have some that were more powerful but then they would require more battery, they would be heavier, should they have a screen that

displays some sensitive information so you're not trusting it going back to the terminal. It was never really standardized or it never really became popular enough to kind of say this is what the smartcard technology was. There were a lot of prototypes, a lot of things that were tried.

Q. Do they exist in the banking industry?

A. I'm not sure. I'm not sure if some of the -- Well, because a lot of the papers that were written were about using it for financial transactions. But like I said, you know, there were different -- not standards but different designs and different feature sets that were proposed.

Q. Okay. Let me ask you --

By the way, I think we're going to get done before lunch, so unless you need to break, I'm comfortable just trying to push through.

A. I would prefer to push through.

Q. Sure. Let's do that.

In Paragraph 110 you make reference to Meyer.

A. Yes.

Q. So as I understand it, you didn't do

any analysis as to whether Meyer discloses the elements of Claim 51?

A. So in the petition, the only thing I saw where Meyer was cited for 51 was -- I think it was 51B, and it wasn't -- it didn't address any of the gaps that I identified for Davies, so I didn't address it individually.

Q. Okay. But you did look at, I guess, Claim 56 for Meyer?

A. Yes.

Q. So in Paragraph 113 you say -- So you're referring to Meyer's use of a PIN being XOR'd with a private key?

A. Yes.

Q. You say: "This, however, ignores that the claim requires credential information to be protected and credential information must be non-secret."

What did you mean, that the claim requires credential information to be protected?

A. So the claim language actually reads from Claim 56 -- I'm starting -- Let me just read the whole thing.

"The method of Claim 51 for further

securing the transfer of funds, at least one party being previously issued a credential by a trusted party, the credential information including information associated with the at least one party, and a second variable authentication number (VAN1), the VAN1 being used to secure at least a portion of the credential information to the at least one party..."

So the language is that it had to be secured. I described that as being protected.

Q. Okay. And you say that the private key protected by Meyer is secret?

A. Yes.

Q. That private key that's protected, it has a corresponding public key, right?

A. Yes.

Q. And that public key is not secret in Meyer?

A. The public key is not secret.

Q. Is there a relationship between the public key and the private key in Meyer?

A. What do you mean, "relationship"?

Q. I mean the way Meyer discloses these keys, is there a mathematical relationship

between the public key and the private key?

A. Sure. A public key is connected to a private key. A public key is the inverse.

Q. Of what?

A. Of the private key.

Q. Let me ask you about Paragraph 121.

A. Sure.

Q. So here we're talking about -- it looks like you're talking about a combination of Davies with another reference called Fischer.

A. Yes.

Q. Do you recall what the Fischer reference discloses as relevant to the combination being discussed here?

A. I mean, I see what's in my report. I refer to two parts of what Fischer combines. Beyond that, I would have to see Fischer.

Q. In Paragraph 121 you give a quote from Davies basically, right? "The second section of the check contains the customer identity and his public key, signed by the bank."

Do you see that?

A. Yes.

Q. So based on that, you concluded: "I

do not see that one of ordinary skill in the art would have thought another reference is necessary."

A. Yes.

Q. Necessary to do what? What do you mean?

A. Well, so like I say in my first sentence here, in Mr. Diffie's declaration he says that Davies does not explicitly disclose that the recipient may authenticate the sender's public key before using it to verify the message signature. But Davies does say the second section of the check contains the customer identity and his public key signed by the bank and therefore verifiable.

So I don't see that one of ordinary skill in the art would have thought another reference was necessary to add in to combine with that.

Q. And that's because you think that the disclosure in Davies would already have suggested to someone of ordinary skill in the art that you could actually verify the hierarchy of keys in doing the authorization process?

S. NIELSON

A. Yes.

MR. WILLIAMS: Why don't we just take a break so I can chat with co-counsel here, and then I'll be ready to wrap it up.

(Recess taken.)

MR. WILLIAMS: I have no further questions.

MR. GREENSPOON: Thank you, Eliot.

EXAMINATION

BY MR. GREENSPOON:

Q. Dr. Nielson, I just have a few follow-up questions.

Could you refer to Paragraph 59 in your report.

A. Yes.

Q. Take a moment to see what it says.

Counsel asked you earlier whether you studied claim construction opinions. Does reading -- and you thought probably not. Does reading Paragraph 59 refresh your memory in any way about whether you studied claim construction opinions in preparing your declaration?

A. So I remembered reading claim constructions, I just couldn't remember the

source of them.

Q. You can put that aside.

Counsel also directed your attention during his questioning to the customer identity field in Davies; I think it was on page 329.

A. 328, yes.

Q. 328, thank you. And you've got the page open?

A. Yes.

Q. Can the originator bank in the Davies disclosures take the customer identity field in combination with any other customer-specific information to uniquely identify a customer account?

A. So the customer public key would be unique to a customer. So certainly almost by itself you could identify the customer just from the public key.

Q. And still looking at that general part of Davies, you were asked some questions about I believe it was field 8. Do you recall that?

A. Yes.

Q. And field 8 is the signature by the bank of fields 5, 6 and 7, right?

A. Yes.

Q. And just for a recap, would you please state for the record what fields 5, 6 and 7 read to be?

A. Customer identity is field 5. Customer public key is field 6. And expiratory date is field 7.

Q. So my question is this: Does the signature by the bank of those fields meet a purpose of associating a public key of the customer with the customer identity?

A. So all three of those fields, the customer identity, the customer public key and the expiratory date, are all signed together by the bank. So you certainly can't -- you couldn't swap in one piece of information here for another.

Q. So then all three of those items are associated by that field 8?

A. Well, they're signed together. I mean, you couldn't change one without altering the signature.

Q. And so that role that you've just acknowledged that field 8 plays, is that role

significant to the funds transfer in the Davies context, that is the final act of actually transferring the funds?

A. Well, so there's a couple of things that are important about those fields. You want to make sure that the customer public key is tied to the customer identity, and you want to make sure that the expiratory date hasn't passed.

Q. And then the final word on this topic. Are those considerations significant to the final act of funds transfer in the Davies context?

A. Would you repeat the question?

Q. That's okay. I'll withdraw the question.

MR. GREENSPOON: No further questions.

MR. WILLIAMS: Just give me one second.

I have nothing further.

(Deposition adjourned at 12:19 p.m.)

ACKNOWLEDGMENT OF DEPONENT

I, SETH NIELSON, Ph.D., have read or have had the foregoing testimony read to me and hereby certify that it is a true and correct transcription of my testimony with the exception of any attached corrections or changes.

_____

SETH NIELSON, Ph.D.

[ ] No corrections

[ ] Correction sheet(s) enclosed

SUBSCRIBED AND SWORN TO BEFORE ME, the undersigned authority, by the witness, SETH NIELSON, Ph.D., on this the _____ day of _____, _____.

C E R T I F I C A T E

STATE OF MARYLAND

I, JOHN L. HARMONSON, a Notary Public within and for the State of Maryland, do hereby certify:

That SETH NIELSON, Ph.D., the witness whose deposition is hereinbefore set forth, was duly sworn by me and that such deposition is a true record of the testimony given by such witness.

I further certify that I am not related to any of the parties to this action by blood or marriage; and that I am in no way interested in the outcome of this matter.

IN WITNESS WHEREOF, I have hereunto set my hand this 18th day of December, 2015.

_____

JOHN L. HARMONSON, RPR

My commission expires: 08/02/17

---------- I N D E X ----------

WITNESS	PAGE
SETH NIELSON	
Examination by Mr. Williams	4
Examination by Mr. Greenspoon	122

---------- EXHIBITS ----------

	PAGE
MasterCard Exhibit 1001	4
U.S. Patent 5,793,302	
Exhibit 2004	4
Declaration of Seth Nielson, Ph.D.	

* * *

DOCUMENTS REFERENCED AND ATTACHED
BUT NOT MARKED AS EXHIBITS

Petition for Covered Business Method Review	103

ERRATA SHEET

CASE: MasterCard International v. Stambler

DATE: December 8, 2015

WITNESS: SETH NIELSON, Ph.D.

Reason Codes:

1. To clarify the record.
2. To conform to the facts.
3. To correct transcription errors.

Pg.	Ln.	Now Reads	Should Read	Reason
___	___	_____	_____	_____
___	___	_____	_____	_____
___	___	_____	_____	_____
___	___	_____	_____	_____
___	___	_____	_____	_____
___	___	_____	_____	_____
___	___	_____	_____	_____
___	___	_____	_____	_____
___	___	_____	_____	_____
___	___	_____	_____	_____

_____

Signature of Deponent

SUBSCRIBED AND SWORN BEFORE ME

THIS ___ DAY OF _____, _____

_____