IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE PATENT TRIAL AND APPEAL BOARD

MASTERCARD INTERNATIONAL
INCORPORATED,

Petitioner,

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

LEON STAMBLER,

Patent Owner.
_____/

DEPOSITION OF WHITFIELD DIFFIE
PALO ALTO, CALIFORNIA
FRIDAY, OCTOBER 2, 2015

Reported by: LOUISE MARIE SOUSOURES, CSR NO. 3575
Certified LiveNote Reporter

Job No. 97941

FRIDAY, OCTOBER 2, 2015

9:32 A.M.

Deposition of WHITFIELD DIFFIE, held at the offices of Baker Botts, 1001 Page Mill Road, Palo Alto, California, before Louise Marie Sousoures, a Certified Shorthand Reporter and a Certified LiveNote Reporter

A P P E A R A N C E S

FOR THE PETITIONER:

BAKER BOTTS
1001 Page Mill Road
Palo Alto, CA 94304
BY: ELIOT WILLIAMS, ESQ.
CHRISTOPHER PATRICE, ESQ.
(VIA TELEPHONE)

FOR THE PATENT OWNER:

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

IT IS HEREBY STIPULATED AND AGREED by and between the attorneys for the respective parties herein, that filing and sealing be and the same are hereby waived.

IT IS FURTHER STIPULATED AND AGREED that all objections, except as to the form of the question, shall be reserved to the time of the trial.

IT IS FURTHER STIPULATED AND AGREED that the within deposition may be sworn to and signed before any officer authorized to administer an oath, with the same force and effect as if signed and sworn to before the Court.

- oOo -

--oOo--

WHITFIELD DIFFIE,

having been first duly sworn by the Certified Shorthand Reporter to tell the truth, the whole truth, and nothing but the truth, testified as follows:

EXAMINATION

BY MR. GREENSPOON:

Q. Good morning.

A. Good morning.

Q. Mr. Diffie, would you please state your full name for the record?

A. I am Whitfield Diffie.

Q. Is that your full name?

A. No, I have a first name I never use. It's Bailey Whitfield Diffie.

Q. I've seen that on an issued patent. If we see Bailey W. Diffie, that's you?

A. Yes, that is I. There's another Bailey W. Diffie is my father. He's not Bailey Whitfield, but he's Bailey W. On the other hand, he was an historian, so I don't think you'll find him in our work.

Q. I'll use Mr. Diffie today in the deposition.

A. That's fine.

Q. Mr. Diffie, you understand the '302 patent?
A. I understand aspects of the '302 patent.
Q. You don't completely understand the '302 patent?
A. I have not -- it's been -- we've been at this case for two and a half years. I have not read through the '302 patent, I think, at least in some time.
So I do not -- I cannot assert I understand every aspect of the '302 patent.
Q. When you signed your declaration in this matter did you understand the '302 patent?
A. When I signed it the first time I'm sure I did because that was, at the time, the first version of the declaration I presume I did.
Insofar as I understand what it means to understand a patent, as it's a long document, I'm sure you could find an aspect of it I would have to study for a little while.
Q. When you signed your declaration on behalf of MasterCard in this PTAB matter, did you understand the '302 patent?
A. Explicitly, I understood the claims at issue.
Q. That's very good.
So are you familiar, then, with its check

presentment disclosures?

A. I am familiar -- may we look at the claims because that --

Q. The patent is in front of you. You may look at any item that you need to to answer my question.

A. Okay. Thank you.

So I am familiar with claim 51 and the notion of authenticating the transfer of funds from an account associated with the first party or associated with the second party, I don't -- I don't remember the phrase "check presentment."

Q. All right. Are you familiar with the fact that within the disclosures of the '302 patent, there is description of the creation of a check?

A. You mean in the embodiment of the '302 patent?

Q. Correct.

A. I don't doubt you, but I didn't remember it.

Q. Do you recall that within the embodiment of the '302 patent, there are electronic fund transfer disclosures?

A. I perceive that as the general subject matter of the patent.

Q. Are you an expert in checking system clearinghouses?

A. Not particularly. I am -- I am familiar with all of the notions I have encountered in studying this case.

I am not familiar with how people do things in the real world, which is, I believe, a lot more complicated.

Q. More or less the same question, you're not an expert in electronic fund transfer clearinghouses?

A. I don't believe so.

Q. You're not an expert in the backend systems used in the real world to effectuate electronic fund transfers?

A. No.

MR. WILLIAMS: Objection to form.

BY MR. GREENSPOON:

Q. Turn, if you will, please, to figure 8B, which is sheet 3 of 15.

Would you confirm for me, please, figure 8B is a depiction of things that happen at the originator's bank according to the teachings of the '302 patent?

Point of information, columns 6 and 7 roughly will be the text description that goes along with this.

A. It will take me a moment to study this.

I remember this diagram, but I have not looked at it with any care in quite some time.

Q. Turn the page, so I'll give you a moment to refamiliarize yourself with this subject matter.

A. You said columns 6 and 7?

Q. That's right.

A. Okay.

I'm going to start with 40, which is the piece.

Q. Perfect. Just speak up when you feel that you've refamiliarized yourself.

A. Okay, I've read columns 6 and 7.

Q. Do you understand columns 6 and 7 as they relate to figure 8B?

A. I'm not at all sure that I do.

Q. All right. Let's give it a shot.

So let's see if we can confirm what's happened so far in the workflow described in this embodiment by the time we get up to figures 8A and figure 8B, okay?

So here's the question: By this point in the workflow, would you agree someone called an originator has created a check?

A. That appeared to me to have happened at the bottom of column 5, where I began reading.

Q. And on this check there's something printed in the embodiment, something called a variable authentication number or a VAN, correct?

MR. WILLIAMS: Objection to form.

THE WITNESS: Almost didn't see VAN until the top of column 7 or so. Let me go back and see if I can find out where that first occurs.

I was looking for that. I found the joint code, but I didn't see the VAN.

BY MR. GREENSPOON:

Q. While you review that, I'll tell you the pending question is: Can you please confirm that on this check there's imprinted a VAN in the embodiment? That's the question.

MR. WILLIAMS: Is there a particular part of the specification that you think discloses that? It might speed it up if you point to the witness where that is.

MR. GREENSPOON: I'm happy to. I myself am looking at columns 5, lines 25 through 28.

THE WITNESS: I was further down, I was looking at 45 to 50. Let me start again at the top of column 5.

MR. GREENSPOON: Sure.

THE WITNESS: Okay. You're right, it's line

25, the VAN and at least a portion of the information relevant to the transaction, are written or imprinted upon the check.

BY MR. GREENSPOON:

Q. I just wanted to establish that at this point in the workflow by the time we get to figures 8A and 8B, someone called an originator has created a check and the check has a VAN on it, correct?

MR. WILLIAMS: Objection to form.

BY MR. GREENSPOON:

Q. I didn't hear an answer.

A. I'm sorry, repeat the question, then, please.

Q. All right. So by the time we get to figure 8A and figure 8B in the workflow of the embodiment, an entity called the originator has created a check and the check has something on it called the VAN, right?

A. Yes.

Q. Okay. So where figure 8A and figure 8B start in the workflow is where a recipient, someone the patent calls a recipient goes to a terminal for the purpose of presenting the check, correct?

A. I -- we have to wave our hands around or something.

So I accept that's a -- I didn't think I started reading far enough back to see that was the

overall objective, but I can accept from this diagram that the objective is the check is somehow created and the recipient presents it to the terminal.

Q. You have no problem with the proposition of my question?

A. No, I have no problem with the proposition of your question.

Q. And figure 8B in particular is what happens with the information on the check at the originator's bank, correct?

A. It is not clear to me where. It appears to me that figure 8B shows the mechanism by which the check is validated presumptively by somebody who is going to pay on the check.

I was -- I'm not clear whether the terminal belongs to the originator's bank or the recipient's bank.

Q. To answer your question perhaps, may I turn your attention to column 5.

A. Yes.

Do you mind if I tear this apart?

Q. Go ahead. For the record, you mean separate the pages from the staple?

A. For the record, I mean may I separate the pages rather than divide each page into small pieces.

Q. It's my job to make sure you don't tear the patent apart, figuratively.

A. Okay. You're calling my attention to column 5?

Q. Yes. So starting at line 55 I'll read into the record "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."

Do you see those words in column 5?

A. Yes.

Q. Can you accept from that disclosure that the terminal could be a terminal at the recipient's bank but it need not be, in any case, it communicates with the recipient's bank and the originator's bank?

A. Yes, I accept that.

Q. Figure 8B, going back to that, can you confirm now that 8B is the set of activities that happen at the originator's bank in connection with the possible payment of the check?

A. Yes, I can.

Q. Okay. In fact, do you observe column 6, line 46 where it says "As shown in figure 8B, at the originator's bank," and there's more.

Do you accept that as a tying of figure 8B to things that have to happen --

A. At the originator's bank.

Q. Okay. In your understanding of what's going on in figure 8B in this embodiment and Mr. Stambler's '302 patent, would you agree that blocks 58 and 60 are where the authentication decision happens at the originator's bank?

A. Yes, that was the conclusion I reached looking at this diagram.

Q. And that authentication decision is made using the VAN from the check and then something else called a joint key, right?

A. Yes.

Q. That joint key where it appears at the originator's bank, am I correct that was originally constructed from, among other things, the originator's taxpayer identification number or TIN?

A. That's in -- I remember that from the text. I don't see the TIN here in the diagram.

Q. Do you see between the words terminal and remote CPU we see originator --

A. Originator's ID, yes.

Q. There's the letter O, TIN, in parentheses.

Do you see that?

A. Very good, yes.

Q. Joint key originally -- starting over.

Joint key, if you trace it back far enough, part of what goes into its construction at the originator's bank is the originator's TIN, correct?

A. Yes.

Q. And do you also accept in the disclosures of the Stambler patent one way the '302 patent describes the authentication process happening is for the originator's bank at that stage, namely blocks 58 and 60, to recreate or regenerate the VAN from the check information?

MR. WILLIAMS: Objection to form.

THE WITNESS: That was not my conclusion about what was happening here.

BY MR. GREENSPOON:

Q. Let me please direct you to column 7, which you've just had a chance to reread, line 12, I'll read into the record "Alternatively, the joint key from the coder 56 can be used to code the information (INFO) from the check to generate a new VAN, which can then be compared with the VAN from the check to authenticate the check."

A. Yes, that seems clear.

Q. Okay. Terrific.

Let me go back to my question, then.

Would you agree now, then, one way Mr. Stambler's '302 patent describes for making the authentication decision is for the originator's bank at this stage to recreate or to generate the VAN from the check info?

A. Well, that may be. I don't see that clearly in the diagram.

Q. You do accept, of course, that we read the diagram in light of the --

A. Of course, I understand -- I presume the diagram exists only to illustrate the text.

However -- so yes, if you're not asking me if I see it in the diagram, it was described in what you just read to me from the column 7.

Q. Okay. Thank you.

Then, do you recall from your refresh just now that it's at block 61, if you see in the diagram, it says check originator's account?

A. Yes.

Q. Check is in the sense of a verb but we will see in a moment.

In fact, I'll start the whole question over because --

A. I apologize. That word "check" is not the

object, but the English word check, meaning to verify or look into or examine or something like that.

Q. Right. Let me go back in baby steps.

Do you accept that the word "check" within block 61 of figure 8B is the verb sense?

A. I take your word for it.

Q. Like inspect?

A. Yes, I understood, as opposed to being the account of the check originator which would be another plausible reading of that phrase, yes.

Q. Okay. Let me go back in the flow of where we're looking at figure 8B.

At block 61, do you agree that the account debit will occur from the originator's account if the funds are there?

A. I presume that that is described in the text. It appears from the diagram the check originator's account 61 has two possibilities, one is NG, which I assume means is no good, and the other is the workflow continues to block 54.

Q. And so by the time we get to block 61, the authentication has succeeded, now we're at the stage where the originator bank simply sees there are funds available, right?

A. That appears to me to be so, yes.

Q. And then let's go now to claim 51.

You mentioned earlier that you're well familiar with claim 51, yes?

A. Yes. What column? It does not mean it would not help me to have it in front of me.

Q. It's column 33, it would be laborious to read the whole claim into the record.

So can I communicate with you today by talking about four steps, receiving, generating, determining and transferring?

A. Please.

Q. Okay. So in what we've just seen at figure 8B, would you agree that the originator bank in the described embodiment performed all four of those steps?

MR. WILLIAMS: Objection to form.

THE WITNESS: I need a moment.

MR. WILLIAMS: I'll also object as outside the scope, but I'll permit the witness to answer.

THE WITNESS: It appears to me that all four of those steps are performed in figure 8B that we've just been looking at in Stambler's embodiment.

BY MR. GREENSPOON:

Q. So in the '302 patent, in the embodiment we just walked through, all steps of the authentication

activity are performed by the originator bank, one entity?

MR. WILLIAMS: Objection to form.

THE WITNESS: If that's his only embodiment, it appears to me that in his embodiment, that is true.

BY MR. GREENSPOON:

Q. In your understanding and review of the '302 patent, did you identify any disclosure of any way that the '302 patent describes dividing up those steps so that different actors play that role or that different actors perform the respective acts?

MR. WILLIAMS: Objection to form. Hang on a second. Objection to form and outside the scope.

THE WITNESS: It appears to me that claim 51 could be satisfied that way, but that there is no requirement in claim 51 that the steps all be performed by the same entity.

BY MR. GREENSPOON:

Q. Okay. The question is a little bit different.

Is there any disclosure in the detailed description of the '302 patent of those four steps being divided up among more than one entity?

MR. WILLIAMS: Same objections.

THE WITNESS: I have not seen -- it appears

to me from what I have read this morning and what has been explained to me that in the portion of the embodiment that we read, all four steps are done by one entity.

BY MR. GREENSPOON:

Q. Okay. I appreciate that, but the question goes one step further, which is: Have you detected any place in the '302 patent where it discloses those four steps being performed by respective different entities?

MR. WILLIAMS: Same objections.

THE WITNESS: I have not detected it, but I would need to read -- I think I probably need to read through the whole embodiment to be confident that there was no --

BY MR. GREENSPOON:

Q. By the way, the taxpayer ID number or TIN or OTIN in the abbreviation in figure 8B, that's nonsecret information in the context of these embodiments, right?

MR. WILLIAMS: Objection to form.

THE WITNESS: I don't actually see that it speaks to that issue.

BY MR. GREENSPOON:

Q. Well, turn, please, to column 11.

A. Yes.

Q. I'll just point you to line 48 to 49, I'll read it into the record "The user's TIN may also be recorded on the credential."

Do you see those words?

A. Yes.

Q. Let me direct you to another page, column 18, I'll read the words from starting line 34 into the record. "In figure 6, the file in which RN and ROC are stored is generally nonsecret because it is indexed (or addressed) by generally nonsecret user information (such as the user's TIN)."

Do you see that?

A. I apologize, you were reading line 38, however, in the embodiment shown in figure 15A?

Q. Above that, line 34.

A. Line 34.

Q. Through 37.

A. Okay.

"In figure 6, the file in which RN and ROC are stored is generally nonsecret because it is indexed (or addressed) by generally nonsecret user information (such as the user's TIN)," all right.

I'm prepared to believe it is Stambler's intention or belief the TIN is nonsecret despite what

I perceive as our current practices.

Q. Stambler was writing in 1992 when our notions of how to protect Social Security numbers may have been a little bit different, right?

MR. WILLIAMS: Objection to form, outside the scope.

THE WITNESS: Yeah, I don't know -- I'm not clear whether that's changed over that period or not.

BY MR. GREENSPOON:

Q. In any case, in the four corners of the '302 patent, the originator's TIN in the --

A. Is treated as nonsecret.

Q. Nonsecret information that was on the credential?

A. (Witness moves head up and down.)

Q. You're nodding your head.

A. I apologize. I'm happy to say yes.

Q. I need to give you a reminder to vocalize your answers.

A. Yes.

Q. So return your attention now to the verbiage in claim 51 which says it's a method for authenticating the transfer of funds.

A. I lost it in the process of finding column 18. What column? What column?

Q. We're going to go to 33 and probably go there quite a bit.

A. Thank you.

Q. The words that begin the claim, in any case, are "a method for authenticating the transfer of funds."

Do you see those words?

A. I do.

Q. And then elsewhere in the claim in the receiving step, the words begin "receiving funds transfer information."

You see that too, right?

A. That's -- yes.

Q. So the funds transfer messages in an electronic system would be relatively short messages?

MR. WILLIAMS: Objection to form and outside the scope.

BY MR. GREENSPOON:

Q. Correct?

A. I believe so, yeah.

Q. Now, let's go to claim 55. This one is short enough I will read it entirely for the record. "The method of claim 51 wherein the VAN is generated by using an error detection code derived by using at least a portion of the funds transfer information."

Do you see those words?

A. I do.

Q. So the relatively short message of claim 51 would also be a relatively short message in claim 55, right?

MR. WILLIAMS: Objection to form, outside the scope.

THE WITNESS: If the message -- if the messages are short, the messages are short.

BY MR. GREENSPOON:

Q. I apologize. Was there more?

A. No.

Q. This shouldn't be controversial in the sense that claim 55 is a dependent claim --

A. I apologize. I'm merely trying to be very careful.

The part of electronic funds transfer in which I am not expert would include knowing whether there are cases in which there might be long messages authenticated.

That's all I was hesitating about. I can easily believe that many funds transfer messages are quite short.

Q. It's mostly my fault. I'm going to do my very best not to talk when you're talking --

A. It was my error that time.

MR. WILLIAMS: You should let him finish his question before you start talking.

BY MR. GREENSPOON:

Q. So you're aware of the principle, are you not, that whatever the limitations are from the independent claim is the same --

A. Yes.

Q. -- scope in the dependent claim?

A. Yes, I am.

Q. My wife always finishes my statements, so I understand.

Back to the examination, so claim 55, that means that the VAN is generated using an error detection code, correct?

A. Yes, that's how I read it.

Q. And that claim covers using an error detection code to generate a VAN to authenticate a funds transfer message which you understand to be a relatively short message?

MR. WILLIAMS: Objection to form.

THE WITNESS: Yes.

BY MR. GREENSPOON:

Q. Let me hand you your declaration in this matter, Exhibit 1020.

A. Thank you.

Q. I did not detect within your declaration that you were making any claim that the prior art anticipates claim 55.

Would you please confirm you have no declaration statements that the prior art anticipates that claim?

MR. WILLIAMS: Objection to form.

THE WITNESS: I would have to review it to be sure of that, but I will believe you if you tell me that we have shown that claim 55 is obvious over the prior art and in the declaration have not shown anticipation.

BY MR. GREENSPOON:

Q. In any case, would you accept for me that the current status of the proceedings are that the board is allowing claim 55 to be challenged only on an obviousness theory and not on an anticipation theory?

A. That is my recollection of reading the board's decision.

Q. Okay. At the time of Mr. Stambler's invention, error detection codes were known, right?

A. Yes.

Q. And an example that you use in your declaration is Nechvatal, a document we're all calling

Nechvatal.

Do you recall that?

A. I do.

Q. N-E-C-H-V-A-T-A-L.

And in your declaration, you use the Davies reference to show the cryptographic techniques for fund transfer of claim 51 and then you combine that with Nechvatal to find a combination that also has error detection codes of claim 55?

A. Yes.

Q. I was having trouble in your declaration finding the paragraphs that hold forth reasons for combining error detection codes into the Davies technology from Nechvatal.

Would you please make an effort to point to me where that is? I'm asking you to look for any testimony on reasons to combine the teachings of Nechvatal error detection codes into the Davies technology.

A. So it appears to me my discussion of Nechvatal starts with paragraph 119 and that in paragraph 133 begins a discussion of why it would have been natural to combine Nechvatal with the other references.

Q. And that goes through what paragraph?

A. 133, 134, 135 and there may be further reference -- and there's a reference to combination in 137.

So I would say 133 on.

Q. Paragraphs 133 up through 137?

A. That's correct.

Q. All right. In these paragraphs, particularly in paragraph 135, you make the observation that Davies discloses that hash values or one-way functions on the transaction information may be used as an intermediate step in generating signatures on the messages.

You make that observation, right?

A. Yes.

Q. In your combination of claim 55 using Davies and Nechvatal, you're using Nechvatal to import the same concept, aren't you?

MR. WILLIAMS: Objection to form.

THE WITNESS: You'll have to clarify. Which -- the concept of using hash function in the process of creating a signature?

BY MR. GREENSPOON:

Q. Correct.

A. Yes.

Q. I'm confused. If Davies already had a teaching of that nature, why would a person of skill

in the art have reached out to a reference like Nechvatal to look for the exact same teaching?

A. I believe at the time I wrote this, I thought that might do that because Nechvatal explicitly refers to error detecting codes or error detection in this context and at the time I had not seen that Davies also refers to error correction at --

Q. I see. You've applied the error detection code concept onto hashes and one-way functions, though, correct?

A. Yes, I think anyone would and would have for a long time before that.

Q. So at the level of that technological description, there are hashes and one-way functions operating on the signatures in Davies just as there are hashes and one-way functions operating on signatures in Nechvatal, correct?

A. Yes.

Q. And I take it from your prior answer you were just looking for the right kind of string of words that mapped onto the claim?

MR. WILLIAMS: Objection to form.

THE WITNESS: My notion has always been that one would, of course, look at Nechvatal because it's national standards guidance and, therefore, anybody

working on the subject would look at Nechvatal.

The -- the concept that these things were error detection was well known at the time and it is, I thought, jointly expressed by these two documents very nicely.

BY MR. GREENSPOON:

Q. Do you believe -- is it your opinion that anything of substance was added when Nechvatal gave a label to that concept as an error detection code?

A. I don't know they gave a label to it as more than applied the label that it occurred to him to mention what would have been known to everyone.

Q. So if I understand correctly, if Davies had used the label error detection code to describe the one-way function hash on a signature, that would have been technologically correct for Davies to have done that?

A. Yes.

Q. I notice you didn't cite the page of Davies where this disclosure occurs.

A. I didn't see it at the time I had written this. It's on page 261.

Q. 261.

You gave me that page number without referring to anything.

A. I'm sorry, it's page 261 of Davies' book, whatever -- Davies and Price book, whatever it's called.

Q. I'm curious why was it so easy to recall the pages.

A. Because I discovered it in the process of preparing for this deposition and restudying the documents.

Q. Sure. Let me hand you the Davies reference.

It actually came to us in three different pdf files and this is the middle of the three which has the pages we're talking about so far.

This is all from --

A. Yeah, it's very hard on these copies to read the page numbers.

Q. That's the best I can do. If counsel has a hard copy of the book, I'd certainly let you use that, but I don't personally have one to show you.

MR. WILLIAMS: We do have a hard copy of the book which we could get if the witness needs it. I doubt you'll be asking about the pages that are faded.

THE WITNESS: It's finding any page, it's --

BY MR. GREENSPOON:

Q. Let me propose this.

A. Okay. The visible page numbers are 19

numbers ahead of the page numbers from the book. That is --

Q. Let's go ahead to our first break.

I'm going to ask you some questions about this section of Davies.

So if you need to, why don't we get the hard copy.

MR. WILLIAMS: I'll appreciate a break.

THE WITNESS: Which section of Davies?

BY MR. GREENSPOON:

Q. Basically pages 261 through 264.

MR. GREENSPOON: Off the record.

(Recess taken 10:33 to 10:54.)

MR. GREENSPOON: Back on the record.

BY MR. GREENSPOON:

Q. Page 264 is a page that I just asked you to refresh yourself with.

Have you had a chance to do that?

A. Yes.

Q. And on page 264 of Davies, under the heading in the middle of the page, let me read some words, actually three sentences I'll read into the record.

"The function H(M) reduces a message of arbitrary length to a number of a convenient and standard length for the purpose of signature. It

could equally well be used as a preparation for calculating an authenticator. It can even be used by itself to authenticate a large message."

Do you see those words in Davies?

A. I do.

Q. Is that the Davies disclosure you were referring to in your declaration page -- paragraph 135 where you said that Davies discloses that hash values are one-way functions on the transaction information may be used as an intermediate step in generating signatures on messages?

A. I think it was more broadly through the text than that.

Q. Would you agree that is an example that shows the proposition you state in paragraph 135?

A. Yes, that's --

Q. Okay. Now, the words of the excerpt that I just read into the record and pointed you to in that Davies suggests a one-way hash to reduce a message length, right?

A. Yes. Not to -- it does reduce a message length.

The important point is that the size of the range is fixed, not -- not so much whether it's smaller.

Q. The words that Davies uses is that the function reduces a message in terms of length, uses that word "reducing," right?

A. Convenient and standard length. He does use the term "reducing," yes.

Q. Right. Davies is not saying that a one-way hash has utility to increase a message length?

A. No, he doesn't say that there.

Q. So in Davies, he doesn't suggest that a one-way hash ought to be used to authenticate a small message?

A. I don't think the size of the -- I don't think -- and I don't think he would have thought that the size of the message is essential beyond the question of whether you could search through the messages.

Q. One of the sentences I just read was it can even be used by itself, meaning the one-way hash, to authenticate a large message.

You remember those words, right?

A. Yes.

Q. So in those words, Davies is saying or suggesting that a one-way hash can be used to authenticate a large message?

A. Yes.

Q. Those words don't suggest that a one-way hash ought to be used to authenticate a small message?

A. I don't -- I think he is taking note of the utility of this for large messages and not speaking to the issue of whether it would apply to small messages.

Q. So the Davies section on one-way hashes and signatures that you just reviewed, none of it contains any rationale or reason for using a one-way hash to authenticate small messages?

A. May I ask you a question, which is we have been using the term "small" without careful definition.

So he describes there a -- something that produces 64 bits.

Is that small? Is 128 bits small? Is 512 small? Relative to gigabyte images, of course, they're small.

So I think -- I should have asked about this before because when we first discussed small message, I thought what's small.

Q. I'll ask the question and if you need to qualify the answer, you have the freedom to do that.

All you've read in Davies about utilizing one-way hashes, is it correct that Davies does not suggest using them to authenticate small messages?

A. Without another read, I wouldn't know for certain, but I don't remember any reference -- any suggestion that small messages were to be favored with this treatment.

I didn't read his comments about large messages as anything other than informative.

I never thought of them as limiting on the messages you were authenticating.

Q. To someone of skill in the art, let's say the 1992 time frame, wouldn't the size of the message have dictated the relative usefulness of utilizing a one-way hash for authentication?

A. I don't think that consideration has changed particularly.

He states at the beginning of the section utility of using one-way hash has to do with the way you manage the message.

So by using what I call in the declaration a systematic signature, where you add an explicit signature block to the message rather than transforming the whole message as seen by the receiver, you have the advantage that you can keep the message in your files in readable form without having to do the signature verification calculation, which was expensive at that era, every time that you

consulted.

So what I read him as saying, and I think it was, by the time certainly of the second edition, received wisdom, is that it is good technique to hash the message which is inexpensive, whether it's large or small, doesn't matter if it's small, but it does matter if it's large and then apply the primitive signature mechanism to the hash.

Q. The words you just said, you said it doesn't matter if it's small, but it does matter if it's large, what do you mean by that?

A. If it is very large, it is much cheaper to do it this way.

If it is small, it will be very close in cost to having encrypted the whole message, having -- forgive me, having used the public key encryption, applied that to the whole message.

Q. You've used the language in your declaration about increasing signing efficiency.

Do you recall that?

A. No, I don't, but --

Q. Improving signing efficiency, paragraph 136.

A. Okay.

I thought you said improve the performance of cryptographic operations, is that what you're

referring to?

Q. If you read through all the way to the end of the paragraph 136 --

A. Yes, would improve the signing efficiency, yes.

Q. The improvement in signing efficiency occurs when you're dealing with a very large message, that's when the one-way hash really improves signing efficiency?

A. The efficiencies grow with the size of the message, yes.

Q. So there will become a message so small the efficiency doesn't improve and, in fact, it becomes extra overhead for the process?

A. You'd have to work at it, but yes.

Q. So for this rationale of improving signing efficiency, that's not a rationale for applying a one-way hash that would apply to a short message like fund transfer messages?

A. I think in that case, your thinking would not be dominated by the improvement in efficiency, speed, cost, yes.

Q. So Davies at least teaches no reason to combine error detection codes into a funds transfer cryptographic message because fund transfer messages

would be small, right?

MR. WILLIAMS: Objection to form.

THE WITNESS: Any authentication operation inherently is an error detection code.

If there's a modification to the message, i.e., an error, the authentication mechanism detects that.

What Davies is recommending a systematic signature when it was first proposed, and I don't know who proposed, it was instantly recognized as being, so to speak, the right way to do that. There may be corner cases where you don't want to do that, but in general, he's describing the conceptually, most straightforward way of signing things.

BY MR. GREENSPOON:

Q. You said corner cases?

A. Programming term, corner cases.

If you had a -- if you had a bunch of very small messages, you might -- and you had a high efficiency system to design, you might decide rather than using the standard techniques, you would use a primitive signature directly.

Q. Because there will come a case where you have computational overhead with no benefit by adding the one-way function hashing, right?

A. Or you might merely want to have less code.
Q. Or both reasons could be true, correct? Less code and computational overhead, right?
A. Yes, but as I say, these ...
Q. So you read claim 55 onto the references by pointing to one-way functions and hashes as the so-called error detection code, correct?
A. Yes.
Q. In your --
A. And signatures.
Q. In your declaration, you didn't apply the references to claim 55 by pointing to a mere signature as an error detection code, did you?
A. I don't recall.
Q. Can you show me anywhere in your declaration where you used the mere signature to map onto the error detection code --
A. Please forgive me.
MR. WILLIAMS: Let him finish the question.
BY MR. GREENSPOON:
Q. -- where you used a mere signature to apply to the claim languages of the error detection code?
A. So I apologize, the phrasing bothers me because I don't know what the term "a mere signature" means.

Q. I can be more precise by saying a signature without there having been a hash.

A. If you say I didn't say that, I don't, you know -- I don't remember a point at which I said it. It is certainly true the signatures, no matter how you do them, are error detection codes.

Q. Please turn to page 81 of your declaration.

Actually, let me move forward --

A. That must be in the claim charts or something. I don't have it here. Maybe it's -- maybe because I tore it apart and it's somewhere else.

The one I have ends in 66. Let's see if I cycled it. No, page 1 to page --

Q. Actually, I want to direct you to page 84.

A. Okay.

MR. WILLIAMS: Why don't you take this copy.

THE WITNESS: I found page 84.

BY MR. GREENSPOON:

Q. Between pages 84 and 85, that's your claim application on Davies in combination with Nechvatal, correct?

A. Or Meyer, yes.

Q. Or Meyer, we laboriously are taking Meyer out of the equation.

Let's focus on Davies in view of Nechvatal,

okay.

For your application of Nechvatal, you pointed to the one-way --

MR. WILLIAMS: Sorry, you're on what page?

MR. GREENSPOON: Page 85.

BY MR. GREENSPOON:

Q. You pointed to the one-way hash disclosure of Nechvatal to read on the error detection code of claim 55, right?

A. Yes, I've read that paragraph.

What were you asking?

Q. You've utilized Nechvatal's disclosure of a one-way hash to map onto the claim language in claim 55 of the error detection code, correct?

A. That appears to me to be true, yes.

Q. Let me move on to a different part of your declaration.

You have an opinion in your declaration that Davies, in combination with Meyer, renders claim 56 obvious.

Do you remember that?

A. That seems reasonable. Where is it?

Q. Let me point you to page 82.

You're free to look at where this is discussed in the more narrative section, but this

should probably do the job for my questions.

So between pages 82 and 83, that is your expression of the limitations of claim 56 with the combination of Davies in view of Meyer, correct?

A. Yes. Can you repeat your question?

Q. Yes, so pages 82 to 83 of your declaration, that's where you chart claim 56 on the combination of Davies and Meyer?

A. Yes.

Q. Okay. You've cited from page 591 of Meyer, what I've done is handed you Exhibit 1022 which is that textbook or at least the excerpts used in the exhibits.

A. I found 591.

Q. So page 591 contains the disclosure you're citing there, 591 through 92, correct.

The pending question is just: Would you confirm it's those two pages, 591 through 92?

A. Yeah, give me a moment.

Q. Sure.

A. Yes.

MR. WILLIAMS: I'm sorry. What was the question? Can you read it back to me?

THE WITNESS: I was just saying yes, I have finished reading pages 591 and looking at page 592.

BY MR. GREENSPOON:

Q. Okay. Let me go back to your charts, 82 and 83.

What I see in your charts is within Meyer; you're citing to page 591, 592 and 597 of Meyer.

Would you confirm that's correct?

A. So I assume you read the whole page, but you're actually talking about the discussion in paragraph 2.

Q. Yeah, my question is really just to establish what we're going to talk about in my next questions.

I've only asked if your chart refers to 591, 592 and 597 in Meyer for claim 56.

Would you confirm that's correct?

A. I see 591, 592. Does it refer to 597? Yes, okay, that's correct, refers to all three pages.

Q. So in claim 56, the claim language itself talks about a second variable authentication number, VAN1, being used to secure at least a portion of the credential information to the at least one party.

Do you recall that from claim 56?

A. I do.

Q. We're labeling that 56-A that I read from?

A. Yes.

Q. So for 56-A, what do you identify as the

credential information that is being secured?

A. The identity -- the public key -- the identity of the user, TIN or whatever it is, the user identifier and the user's public key.

Is that not right?

Q. Well, it's your testimony within this chart so I'm just trying to find out what it is.

Where in the chart does it show that the public key is the credential information?

MR. WILLIAMS: Objection to form.

THE WITNESS: So I see the statement Davies discloses that at least one party is previously issued a credential.

And Meyer discusses the public and private keys of users, I assume, though I don't see it here, Meyer discusses user IDs and the combination of the public key and the user identifier are the credential of the user, the customer.

BY MR. GREENSPOON:

Q. But the way you charted Davies in view of Meyer on claim 56 you're not pointing to a public key or user identifier as the credential information, are you?

MR. WILLIAMS: Objection, form.

THE WITNESS: Well, we're saying the issue

will produce a public and private key pair for each customer.

BY MR. GREENSPOON:

Q. I'm focused just --

A. You did not say that the public key was a credential, I don't see a statement public key is a credential or part of a credential.

Q. So let me go back and ask a prior question.

What is the credential information that you're reading onto claim 56 from the Davies and Meyer combination according to your chart?

A. The public key of the customer and perhaps an identifier of the customer, but explicitly the public key of the customer.

Q. And that's your testimony even though your chart doesn't say anything about a public key?

MR. WILLIAMS: Objection to form.

THE WITNESS: It does --

MR. WILLIAMS: Mischaracterizes the chart.

THE WITNESS: Says PKc SKc. PKc is the public key, public and private key pair, PKc SKc for each customer.

BY MR. GREENSPOON:

Q. I understand now.

So it's your testimony that when you referred

to PKc on page 83, we're to understand that PKc is the credential information being mapped onto claim 56?

A. It is or it is at least part of it. It would suffice, as far as I can see, for it to be all of it.

Q. So we shouldn't read your chart to communicate that a secret value is being applied to the claim language of credential information?

A. I'm sorry, a secret value for what?

Q. You're saying that it's not a secret value that you're reading on the claim language credential information?

A. I would never have said a credential was a secret value.

Q. Okay. So let's go to your reference to PKc, you're referring to PKc?

A. Yes.

Q. And you're drawing that from the disclosure of page 597, correct?

A. PKc must be referred to in quite a number of places.

I think that suffices, if you look at 591 and 592 as well.

Q. So where, according to your opinion, is PKc secured to the at least one party?

A. PKc is inseparable from SKc. There's a

unique correspondence between those two. SKc is secured to the customer by the fact that the -- by the VAN, which is SKc*, and the fact that the customer is the only one who knows the PIN.

Q. So the exclusive OR operation of the PIN onto SKc, in your opinion, is the operation you point to to reflect securing of PKc to the one party?

A. Yes.

Q. Isn't it fair to evaluate what you just pointed to as securing of a secret key to the party, not securing of a public key to the party?

A. No. It does secure a secret key to the party, but the point is to secure a public key to the party.

Q. Even though there's -- in what you've pointed to there's no cryptographic operation being performed on PKc, that's still your opinion?

MR. WILLIAMS: Objection to form.

THE WITNESS: Yes.

BY MR. GREENSPOON:

Q. If the board were to construe the securing -- the so-called securing of a portion of credential information to a party as requiring there to be a cryptographic operation on that exact information, would you agree that your reading of the claim would

no longer hold?

A. No. I think you would have to look a little deeper.

The connection between SKc and PKc is verifiable by the card which is in possession of both.

Q. By card, you're referring back to --

A. Token, whatever we're calling it that contains SKc*.

Q. We haven't mentioned this in words yet, but in the places in Meyer we're talking about there's some discussion of an intelligence smart card, right?

A. Yes, the various sources use slightly different terms for all the same thing called an intelligent token, a smart card or what was Meyer, an intelligent smart card?

Q. Intelligent secure card.

A. Intelligent secure card. It's my understanding those all designate the same type of device.

Q. A physical object --

A. A physical object with computing capacity.

Q. It's a physical object the holder would try to protect, the owner of it would try to protect physically?

A. Yes.

Q. Okay.

MR. WILLIAMS: Just remember to let him finish talking before you answer.

BY MR. GREENSPOON:

Q. Okay. So your opinion is that even if the board were to determine that the securing of claim 56 implicates some sort of cryptographic operation on the so-called credential information, you believe that is met by the Meyer disclosure you pointed to because the cryptographic operation on the secret part of the key links somehow to doing the same thing on the public part of the key?

A. Nothing is done to the public part of the key.

The public part of the key -- the public key is inseparable from the secret key.

There is a precise one-to-one correspondence between the two; for every public key there is exactly one corresponding private key and vice versa and the way in which you demonstrate that you know a public key -- you know the secret key underlying the public key is to use the secret key to generate a message that can be verified by the public key.

Q. All right. You used the term "inseparable."

What was the sense --

A. For every --

Q. Please go ahead, I finished my question.

A. For every public key, one might have to say in that case every well-formed public key, every public key, there is a unique secret key and vice versa.

That's what I meant by they're inseparable.

Q. I've shown you the Meyer textbook and you've seen at least portions of the Davies textbook -- actually, you have the whole hard copy of Davies in front of you.

You're aware that Davies actually cites to that very Meyer reference?

A. I was not.

Q. You were not.

Let's turn to page 323, if you will.

MR. WILLIAMS: The book page or the exhibit number?

BY MR. GREENSPOON:

Q. The book. I may change my mind about that.

Forget 323.

Let's turn to 339, please.

If you're at 339, let me know.

A. Yes, I am.

Q. Reference number 4, that's the very same

thing we're all calling the Meyer reference, right?

A. Yes.

Q. So Davies cites Meyer as reference?

A. I believe so. I don't know if there are multiple editions of Meyer's book, but that's certainly the right book.

Would you like me to read it to you?

Q. No, that's okay. You answered my question.

A. Since mine is legible.

Q. Sorry to do this, but please go back to page 323.

A. Yes.

Q. The last full sentence on 323 refers to a particular concept and Davies says "registration schemes based on the principles described by Matyas can be used."

Do you see that, second line from the bottom?

A. Yeah, I do see it. I was reading.

Q. So Matyas was Meyer's co-author on reference number 4 what we're calling the Meyer reference, right?

A. Yes, Matyas was.

Q. So Davies was fully aware of the content of Meyer, right?

MR. WILLIAMS: Objection to form and outside

the scope.

THE WITNESS: I don't know whether he was fully aware of it, but he was clearly aware of the book, yes.

BY MR. GREENSPOON:

Q. So Davies had every chance to incorporate teachings from the Meyer reference where he thought it appropriate?

A. I apologize, I feel uncomfortable answering that question because I don't know exactly how Davies -- he obviously was aware of Meyer's book, he cites a piece of Meyer's work, although he does not explicitly say that the thing prescribed by Matyas was prescribed in that form in the book.

So --

Q. At the very least he was able to put the Meyer and Matyas reference into his bibliography?

A. Yes.

Q. And that's his bibliography for a certain chapter on signatures and uses of keys, right?

A. Yes.

Q. Do you have any understanding of why the portion of Meyer you pointed to for claim 56 was not itself discussed in the Davies reference?

MR. WILLIAMS: Objection to form, outside the

scope.

THE WITNESS: I have no -- I don't -- please repeat that question.

BY MR. GREENSPOON:

Q. Do you know why the chunk of Meyer that you cite for claim 56 wasn't explicitly part of Davies?

A. No.

Q. Let's go back to your chart. You can set that aside.

I want to go to your very last chart on pages 86 through 89 of your declaration.

This is your chart of Davies in view of Fischer and Piosenka, correct?

A. Yes.

Q. And this is, again, against claim 56, correct?

A. Yes.

Q. So again, what you're attempting to demonstrate is the concepts of claim 56 on that combination including the concepts of VAN1 being used to secure at least a portion of the credential information to the at least one party, correct?

A. Yes.

Q. What is the purpose of bringing Fischer into that combination according to chart? Put more simply,

what do you read onto the claim from Fischer in your chart?

A. Okay, I've read through to the bottom of 87. Would you repeat your question?

Q. In your charting of the combination, what role does the citation to Fischer play?

A. Fischer is very explicit in specifying that every signature in the chain is checked and that the -- the signature is not verified unless every link in the chain is verified.

Q. You say Fischer is explicit, but that's already implicit in Davies, isn't it?

A. I'm sure it is.

Q. Turn in Davies to page 330, please.

In the very middle of the page, the first paragraph under the heading has a final sentence that reads "The merchant's terminal can verify the signatures and the merchant is sure that the checks will be accepted as genuine."

Do you see those words in Davies?

A. I do. I'm not sure over what signature is pluralized. Is it the multiple signatures on one check or signatures on various checks?

Q. I believe you'll find this is referring to the offline operation using the 16-field check of

figure 10.22.

A. Yeah, now that I read the whole thing it refers to the terminal collects the checks, plural, and so I read the plurality of signatures in the last sentence as referring back to the plurality of checks in the second sentence.

Q. I see.

A. That's why he said signatures.

Q. So were you not satisfied that that disclosure of Davies maps onto the checking of signatures according to -- that would be -- that would read on claim 56?

A. If I were concerned with the need to check the sequence of signatures, I would not have taken that part of Davies as establishing that.

Q. So can you summarize, then, what is it that Fischer adds to the combination that you didn't already have from, for example, this excerpt from Davies?

A. Fischer adds an explicit statement that you check a sequence of signatures and every signature must verify correctly for the sequence to be correct.

Q. What language of claim 56 created a need to find a sequence of signatures being checked?

MR. WILLIAMS: Objection to form.

THE WITNESS: At 56-B, authentication transfers funds being denied to the at least one party if the at least a portion of the credential information cannot be secured to the at least one party by using the VAN1.

BY MR. GREENSPOON:

Q. I see. That's only one checking of a variable authentication number in that claim, right?

A. But that is checking the variable authentication number that binds the user's credentials to the bank.

Q. What do you mean by binds the user's credentials to the bank?

A. Maybe that was a bad choice of terms.

The point of claim 56 appears to be to specify what the authentication mechanism in what Davies calls the bank section of the check in which the bank places its signature on the user's credentials.

The -- I found it less than explicit in Davies that you would check the signature of the bank on the customer credentials as well as check the signature of the customer on the transaction.

I think it's obvious, but -- and implicit in everything, but Fischer states it explicitly.

Q. Okay. And then you conclude your application of the combination by bringing Piosenka in.

What's the purpose for that?

A. It's similar. Piosenka is very clear about what happens if the verification fails, whereas although I think everybody understands if the verification fails, you go away mad and you don't pay, the -- in Davies, it is taken for granted that if the verification fails, the transaction does not go through. In Piosenka, it is called out very explicitly.

Q. So there's really no reason for a person of skill in the art to have gone to Piosenka if that person already had Davies plus Fischer to find claim 56?

MR. WILLIAMS: Objection to form.

THE WITNESS: It seemed to me that would have been natural to combine the two.

BY MR. GREENSPOON:

Q. You mean the three?

A. The three, forgive me, the three.

Q. Okay. But putting yourself in the shoes of a person of skill in the art in the beginning of 1992, with knowledge of all of these references, wouldn't your opinion be that a person of skill in the art

would only need to go to Davies plus Fischer to have all of claim 56 and wouldn't need to go to Piosenka?

A. Well, as I said, Piosenka is explicit about a point about which claim 56-B is explicit and that if all of these things weren't obvious from the start to somebody of skill in the art in 1992, this would have educated him.

Q. Now, your opinion on claim 56 presupposes that the bank's signing of the customer's public key secures the public key to the customer?

A. Yes.

Q. And your opinion also presupposes that the customer's signature on the bottom of this Davies check is the original variable authentication number of claim 51, right?

A. Yes.

Q. And in that opinion, what is the credential information and what is the credential?

A. The credential -- now, it's important to distinguish two things, the check and the filled-in check or the blank check and the filled-in check.

You can interpret the credential in several ways and the way we do it here -- I did it here, by and large, is to say that the check is the credential.

You could, if you wished, instead say that

the -- either the combination of the bank section and the customer section were the credential, instead, describing that, that's what's on the check, so to speak, when it's fresh.

Q. What's your opinion that you provide in your declaration for identifying Davies? What is the credential and what is the credential information?

A. I think I said that the credential is the check and the credential information is the information in the bank field and the customer field.

Q. And is that credential information nonsecret?

A. Yes, it is.

Q. So we will walk through that Davies check embodiment shortly.

Let's take a break.

A. Okay.

(Whereupon, a lunch recess was taken 11:51 to 12:42.)

AFTERNOON PROCEEDINGS

MR. GREENSPOON: We are on the record.

BY MR. GREENSPOON:

Q. Welcome back from lunch, Mr. Davies -- I'm sorry, Mr. Diffie.

A. You flatter me. Go on.

Q. I flatter him.

I'd like to ask you some questions about the check discussed in Davies in section 10.6, which starts on page 328.

First, I'd like to just walk through what Davies is disclosing there and I want to get your understanding on the record, okay?

A. Please.

Q. So do you understand Davies to be saying that there is a check that can be filled out by a customer with all the fields shown in figure 2. -- 10.22?

A. Yes.

Q. And when the customer first gets ahold of it, most of the fields are already filled out and the customer only needs to put in a few of them, right?

A. Well, I don't know if it's most, but certainly a lot of fields are already filled in and they are not subject to change. Doesn't have to fill them in, couldn't fill them in.

Q. Right. So what are the fields in figure 10.22 that the customer would fill in at the point in time when the customer starts the process?

A. The amount of payment, the payee identity, the date and time, transaction type, if there is one, the currency, perhaps a description of the payment and the check sequence number is probably generated automatically by the token.

Q. So let's talk about that.

So we've already had some discussion of the token.

In the case of this section of Davies, are we talking about a physical device?

A. Yes.

Q. So there comes a point in time where, through the use of a terminal under this description, the token will be plugged into the terminal in some way?

A. That's my understanding, yes.

Q. And then all of these fields that are either prepopulated or already filled in -- that are either prepopulated or filled in by the customer will eventually go in through the token through the terminal?

A. Yes, somebody in one of these references talks about the possibility the token has a keyboard,

but --

Q. We will get to that.

A. Okay.

Q. So one of the things the token might do is provide the maintenance and insertion of the check sequence number, right?

A. Yes.

Q. And then for our purposes, one of the important things that the token does is it actually signs the fields using the customer's private key, correct?

A. Yes.

Q. And what Davies is communicating is that the physically secure token is the only thing in this ecosystem that has the customer's private key in it, right?

A. Yes.

Q. Because the customer wants to keep that secret and secure, right?

A. Yes.

Q. On your point about the keyboard, do you recall there was some disclosure that the token is a physical object with a keyboard for the purpose of a customer entering a PIN code?

A. The -- I think -- I didn't pay a lot of

attention to that aspect of these references.

They refer either to data including PIN code being passed through a terminal or perhaps there being a keyboard on the token that avoids exposing the PIN in the terminal.

Q. I'll represent to you there is discussion of the customer's private token being used for keying in the PIN for the very purpose of not having someone else's equipment intercept it.

Does that refresh your memory?

A. Yes, it doesn't refresh -- if you tell me Davies says it, of course, I believe it, but that's a perfectly sensible thing to do.

Q. So some of the prepopulated items in the check embodiment are the customer identity and the customer public key, right?

A. Yes.

Q. And those are in a set of fields that I think in prior answers you've called the bank signature or bank certificate?

A. I think the three sections are called the bank section, the customer section and the transaction section.

I don't remember where I remember that from. If it isn't Davies, it's somewhere in Davies I am sure

or I think and a sensible enough term, so I took to using them.

Q. So let's say a merchant get ahold of a check such as it is in Davies -- let me finish my question.

A. Please.

Q. But it hasn't been populated with customer fields yet, it's just the prepopulated fields, not the ones that the customer has authorization to put in.

If someone provides that chunk of electronic information to the merchant, does the merchant know automatically with whom that person is dealing?

A. I'm not even sure that what you're describing can happen in this architecture because the check, in some sense before it's filled in, exists inside the token and the token has no reason to hand it out until it's filled in.

Q. Let's, then, take that instance where it's been filled in, it is a check?

A. Yes.

Q. Do you understand the filled-in check or the, let's say, the bucket of data reflecting the check is a negotiable instrument?

A. I think it has limited negotiability by comparison with a paper check because it has no mechanism for being signed on to another party, but in

the first instance, it behaves very, very much like a paper check, contains much the same information and functions in the same way.

Q. On the backend, once it's entered whatever processing it has to enter into as a filled, completed check, it can be passed from entity to entity to entity, right?

A. Yes, but not -- those passes are merely passing the data. They don't -- they have, to my mind, about the same significance as the teller takes your check and hands it to another teller to put in a file or something like that.

Q. And so --

A. Am I missing your point?

Q. No, I think you have got the point.

Let me try to make it more concrete.

Let's say a person receives -- the intended payee receives the check.

A. Yes.

Q. And the intended payee now presents the check to his own bank.

That's going to be payee bank, right, in my vocabulary I'm presenting to you.

A. Let me see if I can square that -- I think the terminology is the card issuer bank and the payer

bank.

Q. Let's go with that, okay.

You may be mixing embodiments, but with that risk, let me try to present some questions to you.

If the recipient of the check presents it, that recipient is going to be presenting it to a payer bank in the Davies vocabulary?

A. I think so, but I think that's -- you're -- I think it's misleading to anthropomorphize it quite that much.

That is to say, all of this thread goes along inside the electronics and so there really is no instance in which somebody receives the check and hands it on in exactly the way, of course, that you would with a paper check.

Q. Well --

A. Something receives it and hands it off.

Q. As between the backend entities who might pass the bucket of data which is the check, when one entity passes it to the other, those respective entities are not confirming their identities based on the data within the check, are they?

A. We have to be very careful about that and I'd have to think for a moment.

Are you counting the smart card as one of the

entities?

Q. You tell me.

A. Okay. I see several players here, yes, the smart card is a very important one.

And it, of course, generates data as opposed to merely copying and passing data or just acting on data.

However, I think there are a number of places here where the entity identities could be verified. It is not clear whether people would decide that needed to be done or not until a final verification that actually initiates a transfer of payment.

Q. Well, my question was a little more precise.

A. All right.

Q. The fields 1 through 16 --

A. Yes, of -- yes.

Q. -- on figure 10.22 --

A. Yes.

Q. -- those fields cannot allow one backend bank who received the check for payment identify itself to another backend bank who is going to effect the payment?

A. I'm sorry, I find that -- I think the answer is no, and I find this all so odd, why would one think that way.

Q. Let me put it in terms of the '302 patent.

In the '302 patent, we have a recipient's bank and an originator's bank.

If we remember how to paint the picture of '302 and its embodiments, the originator is the person who wants to initially write the check, the initial check maker and the recipient is the receiver of the check.

The recipient presents to his bank, the recipient's bank and payment is requested from the originator's bank.

Do you remember that general vocabulary of how things operate?

A. Yes.

Q. If we use that as a template to discuss the terminology of Davies, the person who fills in 10.22 would be the so-called originator, right?

A. Yes.

Q. And then the recipient or the payee for that check would be the so-called recipient?

A. Yes.

Q. So the payee will take the Davies check and at some point have to present it to his own bank, the recipient's bank, right?

A. Yes.

Q. At that moment where the payee presents that electronic check, with fields 1 through 16 to his recipient's bank, he's not using that check to identify himself with fields 1 through 16, is he?

A. I don't believe so.

Q. And then when the recipient's bank goes and presents to the originator bank to make sure that the funds can be transferred, that recipient bank is not using fields 1 through 16 to identify itself to the originator bank, right?

A. No, because there is no identification, whether reliable or not, on the check of the recipient bank, only of the recipient.

Q. So let's go to the ATM example.

By the way, before we do that, field 13 is one we've talked about payee identity.

Do you remember that?

A. Uh-huh.

Q. That's -- there's nothing in Davies that shows that that reflects an account identifier for a payee, right? That's the name of a payee?

A. You may see some discussion of how payees are identified.

I don't remember it.

Q. So it could be that in section 10.6 there's

no discussion of field 13 being information that identifies an account of a payee?

A. I believe as it is at least implicit, it is whatever identifies the payee is the same kind of data structure datum that identifies the payer.

So there's a customer identity 5 and a payee identity 13.

Q. My question is: For either one or both of those, is there any disclosure of an account number or an account identifier in connection with those fields?

A. I don't remember. I thought there was a discussion of account numbers in conjunction with the customer identity.

Q. But not payee identity?

A. I don't remember.

Q. Let's go to the ATM embodiment.

This is an embodiment where the ultimate result is going to be a cash out to --

A. Yes.

Q. And it's a cash out to the call it originator or customer?

A. Yes.

Q. So there's no second party involved in this situation, right?

A. No. I think there is a second party.

When I write a check -- I have certainly had banks which told me when I was writing a check to them for cash to specify the bank as the payee.

So I think the paying bank is the second party. The check maker is the first party.

Q. Paying bank.

So if we look at figure 10.23, who is the payee bank?

A. The one who owns the ATM.

Q. That would be the middle box of the three boxes, right, that you're talking about?

A. Well, the money comes out of the ATM and I think, yes, that would be the middle box.

Q. Okay. So you just hypothesize a way you've had to write checks to get cash from a bank.

What's the --

A. It's not a hypothesis.

It's my understanding of what the commercial practice is and how you would identify the second entity there.

Q. Let's look at the four corners of the Davies disclosure.

Isn't it the case that Davies doesn't utilize a payee field when its token is going to be used to effect this ATM process?

A. I do not remember.

Q. Some of the fields are already disclosed to be optional, right, such as description of payment, 14?

A. I believe that one's optional. I don't know if there's another optional one or not.

Transaction type, I don't know what a transaction type is.

Q. You don't? On page 331, the end of the first paragraph is actually not a full paragraph but the end of the first paragraph has this sentence "To differentiate these messages and provide for even wider use, the format of figure 10.22 includes the transaction type which denotes a customer check, ATM request, interbank payment, payment advice and so forth."

A. Thank you.

Q. Does that refresh your --

A. That refreshes my memory. It seems like it would need a transaction type.

Q. So is it fair, then, to read that field 10, the transaction type, is going to control whether the customer check is to be utilized as a person-to-person check versus an ATM request?

A. I think so.

Q. So an ATM request could be a code that goes into field 10 that indicates that some of the other fields might be optional for this usage, right?

A. Yes.

Q. Now, in the workflow of the ATM embodiment, they have a picture, figure 10.23, right?

A. Yes.

Q. And the very origin of this collection of arrows is this box under the first box which seems --

A. The keypad, that's a keypad. That appears to me to be the request comes from a keypad, which is the little box under the ATM.

Q. Yes, and the word "request" is next to those as a symbol of some sort of keypad, right.

And then that first arrow goes to what looks like a -- resembles a calculator of the era?

A. Yes.

Q. That's going to be a keypad possibly with the display?

A. That's the token.

Q. So the words next to that symbology are amount, PIN, pay.

So do you take from that that the workflow is somebody somehow electronically connects the token to the ATM machine, makes some sort of request on the ATM

machine and then the ATM machine sends a request down to the token, whereupon, the customer inputs his PIN into the token?

A. I don't know the exact time order. Might put your PIN in earlier, but that is what I see as the workflow.

The request is -- most of the request -- all the request comes in on the terminal of the ATM and it turns around to the token.

Q. Now, at this point, the magic happens and the request -- the ATM request is signed at the token by the customer private key, right?

A. In any request -- anything signed is signed in the token.

Q. And then if we follow the arrows, we now go straight up into the ATM machine with presumably whatever parts of figure 10.22 will be used for this purpose, right?

A. Whichever fields, yes.

Q. Okay. The ATM does a signature check, correct?

A. I think he says it does, yes.

Q. In fact, the first line on page 331 includes the words "the ATM checks the signature to avoid passing ineffective messages into the system," right?

A. Yes.
Q. And that's represented by circle C, yes?
A. Yes.
Q. Then there's a long arrow that goes all the way to the --
A. Card issuer bank.
Q. Right, and there's another circle C also indicating check signature, correct?
A. Yes.
Q. And then if everything works out, the workflow still at card issuer bank B says make payment to A.
Do you see that?
A. Yes.
Q. And now there's a series of hop skips, that's my terminology, but there's a signed message from card issuer bank back to payer bank, correct?
A. Yes.
Q. And if that checks out, then we go make authorization, right?
A. Yes.
Q. Make authorization happens at the payer bank A?
A. Yes.
Q. And then payer bank A now issues a signed

communication back to the ATM machine itself?

A. Yes.

Q. And then -- now near the end. At the ATM machine itself, circle C means that we check the signature, right?

A. Yes.

Q. That's the interbank communication we're checking, right?

A. Yes. It's not clear who signed that message.

Q. Well, payer bank?

A. That's what it would appear to me, yes.

Q. Good. Then, the symbology okay appears and then an arrow down money paid?

A. Yes.

Q. That's cash out to the original customer, right?

A. Yes.

Q. Okay. So what's different between the ATM workflow and the conventional customer check workflow?

A. Well, not very much. The ATM workflow looks most like a point-of-sale workflow and we have a diagram in here somewhere of sending a check to somebody else's account.

Q. I'll represent I did not locate a diagram of the kind you see in 10.23 that was a customer check

person-to-person example.

So the population of usable fields in the format of 10.22 can differ as between a customer check transaction type and ATM transaction type, correct?

A. Well, since he specifies that the transaction type field could include ATM request, I think the answer is yes.

Q. Electronic checks can be easily copied, right?

A. Yes.

Q. Okay. So let's go to your opinion on how these two transaction types described in Davies section 10.6 might read on claim 51.

A. All right.

Q. First of all, what is the so-called credential?

A. So as I said to you earlier, the credential is the unpopulated check that will be filled in inside the -- by the actions of the customer and completed inside the token.

Q. Who issues that unpopulated check?

A. The bank.

Q. So the claim language requires that the credential is issued to at least -- well, the credential is issued by a trusted party.

Is it your opinion that the bank is a trusted party?

A. It is.

Q. Why?

A. Ordinary English, that is the business relationship we have with our banks.

Q. Would you agree the bank is not a key registry in this discussion?

A. No, actually I wouldn't. It's a key registry for its customers.

Q. Do you --

A. It operates a key registry for its customers.

Q. Where do you see that disclosed?

A. I think that -- there is a statement, I believe it is disclosed here that the bank issues -- is the origin of the customer field of the check which is a component of the credential of the customer.

Q. And simply by virtue of that, your opinion is that this makes the bank a key registry?

A. I don't see any other way to view it.

Q. So what place in the workflow does the step of receiving funds transfer information occur?

A. When the token receives the funds transfer information from the -- from the ATM.

Q. From the ATM?

A. Yes. That's one place. There are multiple things that receive things that, but from the point of view of claim 51, that is the essential one.

Q. So what about for other transaction types other than ATM, do you have any opinion of --

A. They all involve the token. The token receives the information wherever it gets it from.

Q. Okay. So your opinion, then, would be if it's a customer check transaction type, then when the customer steps up to the terminal, somehow couples the token to the terminal and does that which is necessary to have a true check with a payee, that's also an instance where the token does the receiving?

A. Yes.

Q. Okay. Where in the workflow are you finding generating the VAN?

A. In the -- in the signing of the transaction information by the -- by the token.

Q. Where in the workflow are you finding the determination of authenticity, the determining step?

A. In the -- in the checking of the signature by the card issuer bank.

Q. And finally, where are you finding the transferring step in the workflow?

A. So let me have the -- let me dig up the

claims again. What column are they?

Q. 33.

A. Of course, I have 38 here.

In the arrow between the two right-hand boxes that's annotated make a payment to A.

Q. Okay. So in the lexicon of figure 10.23, that's still the card issuer bank?

A. That's the card issuer bank making a payment to the payer bank.

Q. If we map that scenario onto the way vocabulary is used in the Stambler patent, that would be the originator bank?

A. Well, let's see. Is that term used in the claims anywhere?

Q. Not the claims, but in the detailed description of the preferred embodiment?

A. And I apologize, he talks about the originator bank and the receiver bank?

Q. Right.

A. Okay. I would think in this diagram that corresponds to the card issuer bank is the originator bank and the payer bank is the receiver bank.

Q. Fair enough. So your opinions never point to any disclosure in Davies of a card issuer bank generating a VAN using a portion of the received funds

transfer information, right?

A. I wouldn't think they would.

Q. Because it would be impossible in the Davies workflow for the card issuer bank to create the same VAN because the card issuer bank will never have the customer's private key?

A. Yes, the token is the one thing that can create the VAN.

Q. And as we just went over, you've got two steps being performed in the token which is a physical thing perhaps held in the pocket of a customer and you've got two other steps being performed at a remote bank, right?

A. Yes, I didn't count. What are the two steps performed -- I mean data flow into the token and it puts a signature onto the check and returns it.

Q. I think this is just summarizing things.

A. Is that one step or two, I was trying --

Q. Well, I'll start over.

So the receiving step and the generating step --

A. These are steps as in the claims?

Q. Yes, I apologize.

A. The receiving and generating steps take place in the token, that's right.

Q. And determining and transferring take place at the remote bank, namely the one holding the customer's money?

A. Yes.

Q. And how did you come to believe it was appropriate to map claim 51 as an anticipation onto the actions performed by two different technologies or entities that are separate from one another?

A. Well, so I never followed your -- I think you've discussed that before, I, frankly, didn't follow you, just as I read claim 51, the workflow we've been discussing seems to me to satisfy its requirements.

Q. Some of the first words of claim 51 are a method for authenticating, right?

A. Yes.

Q. And so all of the steps have to be understood as a method for authenticating, right?

A. I believe you're telling me that's the way patent language is read.

Yes, I believe you.

Q. Okay. You don't have a problem with that proposition?

A. No, I don't have a problem with that.

Q. In the workflow of Davies only the card

issuer bank has the necessary capabilities to determine authenticity, right?

MR. WILLIAMS: Objection to form.

THE WITNESS: I'm actually not sure of that. Since the information in the credential is public, potentially any party to the transaction could determine the authenticity, it just may not feel it needs to.

BY MR. GREENSPOON:

Q. Well, determine the authenticity and transfer funds, there's only the customer's bank or the card issuer bank who can do that?

A. It's the only one with an obligation to transfer funds is, I think, the point.

Q. Within the four corners of the Davies disclosure section 10.6 it's the only entity that does transfer funds after performing the authentication?

A. Yes. That seems right.

Q. So I don't know if it's today or in your declaration somewhere, but you've called the middle section of the check, the part signed by the bank, you've called that a certificate of the customer, right?

A. No, I said the whole unfilled-in check was the certificate of the customer, but I said you can --

there are other ways you could describe that.

Q. How is the whole unfilled check usable -- let me back up.

Isn't it true that the unfilled-in check cannot be used to determine or establish the identity of a party?

A. The unfilled-in check is part of the filled-in check and it is the part of the filled-in check that is the credential.

Q. So maybe we're -- maybe we should be more precise.

When you said the unfilled-in check, you meant --

A. A field --

Q. A subset of fields that are fixed before the customer starts doing some kind of data entry?

A. That's what I meant, yes.

Q. The fixed fields of the check embody the certificate or the credential?

A. Yes.

Q. But you do assume that the whole check has been filled out at the point in the workflow where it's going to be used, right?

A. Yes.

Q. So isn't it correct that the fixed fields of

that check cannot be used for determining or establishing the identity of a party?

A. Well, I think your terms are for the purpose of determining or establishing the identity and yes, they play a fundamental role in determining the identity because they present the public keys that are used to verify the signatures with the secret keys.

Q. However, you agreed that electronic checks can be easily copied, right?

A. They can be perfectly copied.

Q. The person who does the presentment of such an electronic check, that person's identity cannot be determined or established by his or her presentment of that check?

A. Well, once again, you are anthropomorphizing this in a way that just isn't true to the technology because the person who presents is the person who had the token, who had the use of the token, the authority of the token and the token, effectively as the agent for that person, presents the check.

How it passes from clerk's hand to clerk's hand after that is not really part of the financial transaction, just part of the mechanism by which it's processed.

Q. So is it your opinion that if you focus on

the person who has the token, then that person, at the moment that the check leaves his or her possession, is able to use the check for the purpose of identifying himself or herself?

A. Identifying the maker -- the check identifies the maker from the point of view of the transaction, right.

Credentials are explicit to particular kinds of things. Driver's license authenticates you to the police for the right to drive.

In this case, the credential authenticates -- assisted in the authentication of the maker of the check.

Q. What do you mean by anthropomorphizing?

A. You're talking about people presenting checks as you're very much in the -- in the sense in which physical paper possession plays a role at points in human interaction that don't have a precise cognate in this workflow.

Q. Isn't this an exact analog of the check clearinghouse system that Mr. Davies is communicating, really converting the paper check into a collection of electronic data?

A. I don't know the details of the paper clearinghouse system, part of my lack of expertise in

payment systems.

I think it is an approximate analog of the normal business procedures involved in making payments by check.

Q. So in the customer check example --

A. What page are you on? The one -- the page with the diagram?

Q. The page with the diagram, 328.

A. Yes.

Q. In that case, neither the payer bank nor the card issuer bank will receive the funds transfer information before the VAN is generated, right?

A. No, they are not the ones who receive it before the VAN is generated. The token receives it before the VAN is generated.

Q. The same for the ATM example a few pages later, neither the payer nor the card issuer bank receives the funds transfer information before the VAN is generated?

A. No, it's the token that receives the funds transfer information before the VAN is generated.

Q. The token, as we've discussed, is something that would be very closely physically held by a person the way Davies describes it, right?

A. Yes.

Q. Something that that person would associate as one of its most valuable pieces of property, perhaps?

A. Depends on how much money is in the account.

Q. And the way you've explained the token receiving funds transfer information, I'm picturing the customer sits at a terminal, types the necessary information and perhaps it goes up into the terminal and then into the token, right?

A. That's -- particularly that's exactly how it looks in the diagram.

Q. Aren't you painting the picture of someone giving some information to himself?

A. The token receives the information. I don't see anything odd about that understanding. Is there something missing here?

Q. Well, it's a human being supplying some collection of data to a thing owned by the human being, right?

A. Yes.

Q. So that's giving funds transfer information to himself, right?

A. We're talking about electronic systems that involve transferring information and information is sent, in this case, by the human being, information is received by the token.

Q. It's very simple. I'm confirming the way you view the mapping of the claims.

You view it as the person receives fund transfer information from himself?

A. No, the token receives the funds transfer information.

Q. All right. Let me build that in.

So the token owned by the person receives funds transfer information from the person?

A. Yes.

Q. And you see nothing odd about that?

A. No.

Q. If you take a ball from one hand and put it into your other hand, are you receiving the ball from yourself?

A. One of my hands is receiving the ball from the other hand.

Q. But as a person with agency and an actor in the world, are you receiving a ball from yourself with that operation?

A. I don't -- I don't know. It doesn't strike me as the same thing because the token -- the token has a good deal of agency of its own. It can do things you can't do.

Q. And it does those on behalf of the person who

owns it, right?

A. It does them on behalf of the person who owns -- who owns it, yes, and just incidentally, as a consequence, might be owned by the bank. The bank would probably claim to own it.

Q. All right. You alluded to this earlier, but this is -- this is not your first version of a declaration on the Stambler patent ever, is it?

A. No.

Q. So you've submitted previous declarations related to the Stambler patent for parties other than MasterCard?

A. Yes.

Q. How many --

A. And maybe for patents other than this one.

Q. Perhaps. So how many other declarations directed to the '302 patent have you presented?

A. I think, depending how you count, it's probably three or four.

There were -- unless there was more than one -- may have been more than one for the Federal Reserve.

Then, the terminology in the Federal Reserve case was taken over by First Third Bank, right, and I think my declaration was submitted again on behalf of

First Third Bank. I don't remember any substantive changes to it, I merely remember signing it again.

Then, it was -- the case went to Visa and I -- the declaration must have changed at that point because I remember several days working with Visa's attorney discussing these issues and then it came to MasterCard about a year ago and that produced the current version.

Q. Okay. About how much time collectively have you spent on all the work leading up to the declaration we see before us today?

A. I assume it's tens of hours, but I would have to consult my logs to find out.

Q. What do you bill for your work on this matter?

A. I think it's 600 an hour. I say I think because I do not remember -- for example, I do not remember whether this moment comes under the backroom work rate or the trial rate.

So we may have as many as three different rates.

Q. Who wrote the initial draft of the declaration?

A. I would say I wrote it, but I started with a great deal of information from the attorneys for

Federal Reserve.

Q. Okay. If I walked you through the paragraphs of your declaration, would you be able to pinpoint what's changed since MasterCard retained you and asked you for a declaration?

A. Maybe. I'm not very good at that. I might, might not.

Q. Okay. We will get to some things in here in just a moment.

Let me ask you how many other times have you given testimony under oath in a patent matter, oral testimony?

A. So I've worked on let me call it two and a half cases of significance and one, there are two other little tiny things.

The case in which I have spent the most work, been deposed the most, only case in which I've ever appeared in court was a TQP case on a patent by Jones.

So I do not remember how many times I was deposed, but at least three and appeared in court once.

I do not believe I've ever been deposed before in this case or deposed in any other case I've worked on, I've worked -- done what I call backroom work, I have developed opinions for people.

Q. Other than TQP, this may be the second --
A. This is probably the second case I've been deposed as an expert witness.
I've been deposed as a percipient witness in cases of my own about public key two decades ago.
Q. You mentioned your own public key work.
Did you happen to notice that the Stambler '302 patent cites to your earlier patent with Mr. Hellman?
A. I did.
Q. And so you observe that the patent office examiner found no problem issuing the '302 patent in view of your prior inventive work on public key cryptography?
A. That I understood.
Q. You're not bringing in your patent with Mr. Hellman as any sort of invalidity theory of your declaration?
A. No.
Q. Let's turn to your declaration, paragraph 18, which is page 4.
A. That is my current declaration?
Q. Your current.
A. All right. Yes.
Q. Did you find that there's any sort of mistake

you might like to correct in paragraph 18?

A. No, I don't. If there's an error, you'll have to point it out to me.

Q. Well, just based on your expertise in cryptography, error detection code is something different from the definition you gave it, right?

A. I think I used the definition that resulted from one of the courts.

I don't see anything wrong with that definition.

Q. Wouldn't it be better if the last instance of the word "coded" was instead the word "original"?

A. No.

Q. You don't think so?

A. I don't think so.

Q. Have you been informed there was a prior claim construction by the Court that was exactly as you report it in paragraph 18, but a future court then corrected it to replace the word I just pointed to "coded" with the word "original"?

A. No, I wasn't.

Q. Let me show you page 25 of Exhibit 1016, which is a court interpretation in Stambler versus ING Bank.

A. Stambler versus whom?

Q. ING, I-N-G.

Actually starts at 24 but that's just the header.

A. 24 of what, the document that's in my hand?

Q. Yes, error detection code.

I'll read to you from this court construction.

"Plaintiff's proposed construction" meaning Mr. Stambler's, "mirrors the Court's construction in Amazon, but clarifies that an error detection code is used to detect changes to the original information, not to the resulting coded information. Plaintiff's clarification is consistent with the specification, which describes an error detection code as information coded 'in such a manner as to permit detection of changes (e.g., error detection coding) but without complete recovery of the original information.'"

You see where I've just read?

A. Yes.

Q. Do you accept the Court's correction there as a proper one to make?

A. I think either one will do.

I can live with either.

Q. Wouldn't you want to go and review your opinions if it turns out that the ING court

construction is the one that's accepted by the board?

A. Well, I would want to figure out whether it makes any difference, but as I say, as far as -- I'm not aware of a difference. I understand you could phrase it either way. I think my thinking was it is the coded information that is transmitted and received, therefore it's the coded information that could be modified.

So I think the definition as written is perfectly reasonable.

If you wish to regard it as trying to detect whether you are recovering the original information, I think the courts -- the latter court's way of putting it is reasonable.

Q. If the purpose or the issue is data integrity authentication, then the latter court's use of the word "original" is the proper way to go?

A. I find the terms "proper" and "improper" to -- there just is not enough difference here for me to want to make any strong statement about it.

Q. Fair enough.

Can you turn to your declaration, another place, paragraph 76.

A. As described in Davies.

Q. So paragraph 76 almost in its entirety is a

quotation of a Davies excerpt; is that correct?

A. I don't -- I don't doubt you.

Q. However, in the first line you have a bracket alteration to the text.

Do you see that?

A. Is a point-of-sale payment by electronic check.

Q. Let's go and find out what word or words you were replacing with that bracket alteration?

A. Please.

Q. That was on page 331 of Davies.

Actually, it's not. It's on page 330 of Davies.

A. All right.

Q. There you go, Mr. Diffie. I found an error in your declaration.

A. Do I say it's on 331? I apologize.

Q. So we agree now it's 330 --

A. I see it at the bottom of 330.

Q. So the bottom of 330, the fifth word in that sentence is the word "this."

So in other words, everything in the bracket what you were doing is replacing the word this, T-H-I-S, correct?

A. Yes.

Q. And what you put in the bracket is a point-of-sale payment by electronic check, right?

A. Yes.

Q. But if you look in the context on the bottom of page 330, that's not an accurate alteration of the text, is it?

A. I believe this is describing a -- the use of an ATM to get cash and I think my intent must have been that the -- that that transaction functions like a point-of-sale transaction in which the thing being bought is a bundle of cash.

I apologize if you found it misleading.

Q. So would you like to clarify to make that paragraph 76 in your declaration more accurate?

MR. WILLIAMS: Objection to form.

THE WITNESS: Well, I'd have to read for a moment. The "this" in Davies is referring to a previous paragraph.

BY MR. GREENSPOON:

Q. The words are --

A. The closest reference is certainly an ATM with online verification and so looking no deeper, I would incline to agree with you that it might better have said an ATM -- an ATM withdrawal by means of electronic check or something of that sort.

Q. Instead of point-of-sale?

A. But I want to emphasize that the two -- not much difference in the two.

Q. I get it. You see ties between them?

A. Right.

Q. So going back to those two workflows that we saw in section 10.6 of Davies, the customer check workflow and the ATM cash out workflow, those were each sort of self-contained systems, right? They were fully described within their own terms, right?

A. If I understand you, I think so.

Q. In other words, there was no recitation by Mr. Davies that much work needs to be done, here's a catalog of things we can add or subtract or modify or improve?

A. Well, self contained and not capable of being improved, expanded, et cetera, seem slightly different things, but I would not -- no, there's no reference here that I know to a catalog of things you might add to it.

Q. And as he wrote this up, Mr. Davies wrote each of those workflows up as a system that accomplishes this objective, right?

A. Yes.

Q. When you've taken -- when you've made your

obviousness combinations, we've gone over some of those, sometimes it's with Meyer, sometimes it's Davies with Fischer and Piosenka and Nechvatal, what have you, you've made the point in your declaration that the references are in similar subject areas?

A. Yes.

Q. So you've made the point that in each case you have a reference that accomplishes similar functions and, therefore, that gives some weight to a reason for a person of skill in the art to combine them?

A. No, they are in similar subject areas. I might even have said in conversation the same subject area, which is the use of cryptographic techniques to secure various kinds of communication and transactions on networks.

The two books are similar in that respect.

Q. And if you have a collection of references, let's call them prior art references in front of you as a person of skill in the art, and all the references independently accomplished similar functions, how could there be a reason to combine?

MR. WILLIAMS: Objection to form.

THE WITNESS: To be honest, I don't know how you cannot know that.

That is to say that by reading several references that addressed the same issues but express things in slightly different ways, you come to a more comprehensive view of the subject.

Is that not what it means to combine materials?

BY MR. GREENSPOON:

Q. They become like separate pieces of a jigsaw puzzle?

A. No, I think that's not probably -- jigsaw puzzles fit at sharp edges. These are things that overlap.

Q. All right.

MR. GREENSPOON: Let's take a break, might be ready to adjourn.

(Recess taken 1:48 to 1:55.)

MR. GREENSPOON: Pass the witness.

EXAMINATION

BY MR. WILLIAMS:

Q. Let me just ask you a question about claim 55, which -- do you have the patent in front of you?

A. I have claim 55, about error detection code, yes, I think I have the patent open to the claims, yes.

Q. In your declaration, I think you were asked

earlier about whether you had provided an opinion as to whether Davies teaches that element in your declaration.

Do you recall that?

A. Yes.

Q. Do you recall whether you provided an opinion as to whether Davies teaches that claim element in your declaration?

A. I don't remember whether I provided it, but I remember having the view that I thought in the end that it did and I merely hadn't noticed it before.

Q. So if you have your declaration in front of you, turn to page 59.

A. Yes.

Q. Does this refresh your recollection as to whether in your declaration you provided an opinion as to whether Davies teaches this element?

A. Yes.

Q. It does -- does that refresh your recollection?

A. It refreshes my memory, yes.

Q. Did you, in your declaration, provide an opinion as to whether Davies itself discloses what's recited in claim 55?

A. No, I did not.

I did not say that Davies talked about error detection.

Q. On this -- what was the intent of what's shown on the bottom of page 59 and the top of page 60 in your declaration?

A. Example 1, Davies describes the generation of a signature, et cetera.

Q. And you're comparing that to claim 55 on these two pages, correct?

A. So it appears to me that I'm saying that implicitly Davies understands that a signature is an error detection code.

MR. WILLIAMS: No further questions.

MR. GREENSPOON: Just a quick follow-up.

FURTHER EXAMINATION

BY MR. GREENSPOON:

Q. You understand that the board, in its institution decision, did not agree with you that there is a basis for unpatentability of claim 5 as anticipated by Davies?

A. Claim 5?

Q. 55.

A. Yes.

Q. So trial has been instituted on theories other than claim 55 being anticipated by Davies?

A. Yes.

MR. GREENSPOON: Okay. No further questions.

MR. WILLIAMS: Off the record.

THE REPORTER: Can you both put your orders on the record?

MR. GREENSPOON: For patentee, who is on the other side of the caption, the defense.

MR. WILLIAMS: You're the patent owner.

MR. GREENSPOON: We would like rough ASCII right away, otherwise a normal turnaround.

MR. WILLIAMS: And we will just take standard delivery on the final, please.

(the deposition of was adjourned at 2:00 p.m.)

I, , do hereby certify under penalty of perjury that I have read the foregoing transcript of my deposition taken on ; that I have made such corrections as appear noted herein in ink, initialed by me; that my testimony as contained herein, as corrected, is true and correct.

Signature: _____

Dated: _____

I, LOUISE MARIE SOUSOURES, duly authorized to administer oaths pursuant to Section 2093(b) of the California Code of Civil Procedure, do hereby certify: That the witness in the foregoing deposition was by me duly sworn to testify the truth in the within-entitled cause; that said deposition was taken at the time and place therein cited; that the testimony of the said witness was reported by me and was hereafter transcribed under my direction into typewriting; that the foregoing is a complete and accurate record of said testimony; and that the witness was given an opportunity to read and correct said deposition and to subscribe the same.

Should the signature of the witness not be affixed to the deposition, the witness shall not have availed himself or herself of the opportunity to sign or the signature has been waived.

I further certify that I am not of counsel, nor attorney for any of the parties in the foregoing deposition and caption named, nor in any way interested in the outcome of the cause named in said caption.

DATE: October 14, 2015

_____

LOUISE MARIE SOUSOURES, CSR. #3575

INDEX OF EXAMINATIONS

INDEX OF EXHIBITS

(NONE MARKED)

ERRATA SHEET FOR THE TRANSCRIPT OF:

Case Name: Mastercard International Inc.
v. Leon Stambler

Dep. Date: 10/2/2015

Deponent: Whitfield Diffie

CORRECTIONS:

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

_____
Signature of Deponent

SUBSCRIBED AND SWORN BEFORE ME
THIS____DAY OF_____, 2015.

_____

(Notary Public) MY COMMISSION EXPIRES:_____