IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

- - - - - - - - - - - - - - -x

MASTERCARD INCORPORATED AND :

MASTERCARD INTERNATIONAL :

INCORPORATED, : U.S. Patent No.

Petitioner, : 10,032,171

v. :

OV LOOP, INC.,

Patent Owner.

- - - - - - - - - - - - - - -x

Deposition of Stuart Fiske, PH.D.

Conducted remotely via Zoom

June 14, 2024

9:58 a.m. Eastern Standard Time

Reported By:

Alan H. Brock, RDR, CRR

Job No.: 9347

A P P E A R A N C E S

ON BEHALF OF PETITIONER:

BAKER BOTTS L.L.P.
ELIOT D. WILLIAMS, ESQ.
700 K Street NW
Washington, D.C. 20001
202.639.7700
eliot.williams@bakerbotts.com

ON BEHALF OF PATENT OWNER:

BC LAW GROUP, P.C.
SETH LINDNER, ESQ.
200 Madison Avenue, 24th Floor
New York, New York 10016
212.951.1000
slindner@bclgpc.com

Q. So if one were to look at a data item without knowing its origin, is it possible to know whether that's a cryptogram or not?

MR. WILLIAMS: Objection to form and scope.

A. So the actual value of a cryptogram without any annotation around it to say that it is a cryptogram would appear to be, for example, an 8-byte, 64-bit number. And that would be indistinguishable from any other 8-byte, 64-bit numbers that weren't cryptograms.

The way a person of ordinary skill in the art in 2012 would understand that that's handled in the context of the payment industry is to understand that the language of EMV payments includes a tag as well as a value for each data item, and it's the tag that identifies the purpose of the data item. And there would be a tag value which is associated with an application cryptogram.

Q. Would a person of skill in the art in 2012 have known how to generate a cryptogram?

A. Yes.

Q. What are some ways to generate a cryptogram that a person of skill in the art would have been familiar with in 2012?

A. The EMV standards include specifications for how cryptograms can be generated, and a person of skill in the art in 2012 would be familiar with those specifications.

Q. Are there any other ways to generate a cryptogram that a person of skill in the art would have been familiar with in 2012?

MR. WILLIAMS: Objection to form.

A. Given that a cryptogram is the result of a cryptographic calculation, which requires input data, an algorithm, and a key, there are many different cryptographic algorithms, not just the ones that are used in the payments industry.

So a person of skill in the art would understand that and know that there are alternative mechanisms for generating cryptograms to those in EMV. But they would also understand that, to have any usefulness in payments, the appropriate form would be to use the EMV standards.

Q. Would a person of skill in the art understand that MD5 is an algorithm available to generate a cryptogram?

A. They would not -- I would not accept that definition, and I don't believe a person of skill in the art in 2012 would accept that definition.

A. So if we take the example of using the triple DES algorithm to generate what the '171 patent calls a hash, what happens is you take a block of input data and a cryptographic key, and you operate on the input data using the cryptographic key to produce an output. And in some contexts that output is called a cryptogram. In other contexts it's called a MAC. But the output is an 8-byte, 64-bit value, which has come from however long the data, the input data, was. And the '171 patent, when it describes that process, calls the result a hash.

A person of ordinary skill in the art who hadn't read the '171 patent would understand that the word "hash" is the result of one of the hash algorithms. SHA is one I've already mentioned. MD5 is one that you've already mentioned. Those generate outputs which are longer than the DES algorithm.

So SHA-1, for example, will generate -- which is used in the EMV specifications -- will generate a result which is 20 bytes, 160 bits long.

Q. Would a person of skill have understood that AES could be used to generate a cryptogram?

MR. WILLIAMS: Objection to form.

A. They would have understood that the advanced encryption standard, AES, can be used to generate a

cryptographic output, which could be called a cryptogram.

However, in the context of EMV payments, because the AES standard uses a block which is 16 bytes long, it will generate a result which is 16 bytes long, whereas the DES or triple DES algorithm generates a resultant cryptogram which is 8 bytes long.

So they would have understood that without an additional step, the AES algorithm cannot generate an EMV cryptogram because an EMV cryptogram is defined to be 8 bytes long.

I think after 2012, and because the industry is moving from DES and triple DES towards AES, EMVCo have issued some guidance on how to deal with AES cryptographic results, or AES cryptograms, in the context of an EMV payment. And I think that current recommendation, from memory, is that the solution is to generate the 16-byte result and truncate it by throwing half of it away.

Q. Would a person of skill have understood that the serpent algorithm could be used to generate a cryptogram in 2012?

MR. WILLIAMS: Objection to form and scope.

A. I'm unfamiliar with the serpent algorithm, and so I would expect that a person of ordinary skill in the art in 2012 would have also been unfamiliar with the serpent algorithm.

Q. Would a person of skill have ideas that the IDEA algorithm would have been suitable for generating a cryptogram in 2012?

MR. WILLIAMS: Objection to form and scope.

A. The same answer. I'm unfamiliar with the IDEA algorithm.

Q. Would a person of skill in the art have understood that the MARS algorithm could have been used to generate a cryptogram in 2012?

MR. WILLIAMS: Same objection.

A. Same answer.

Q. Would a person of skill in the art have understand that the Camellia algorithm could have been used to generate a cryptogram in 2012?

MR. WILLIAMS: Same objection.

A. Same answer.

Q. Would a person of skill in the art have understood the term HMAC, H-M-A-C?

A. Yes.

Q. Would a person of skill in the art have been

familiar with the Federal standard FIPS Pub. 198-1?

MR. WILLIAMS: Objection to form and scope.

A. So they would have understood the FIPS range or specifications. They would have understood that at issuing banks hardware security modules have to comply with those FIPS specifications. But I confess, I'm unfamiliar with the actual number that you quoted.

Q. Is an HMAC an example of a cryptogram?

MR. WILLIAMS: Objection to form.

A. It is not an example of an EMV cryptogram, but it is the result of a cryptographic calculation.

Q. So it is a cryptogram but not an EMV cryptogram, as you are using that term?

A. Yes.

Q. Would a person of skill in the art have been familiar with the cryptographic algorithm AMAC, A-M-A-C?

MR. WILLIAMS: Objection to form.

A. I'm unfamiliar with that algorithm, and so I would say no.

Q. Would a person of skill in the art have been familiar with the term "PMAC," P M-A-C?

MR. WILLIAMS: Objection to form.

A. Same answer.

payment application together with all of its data, including the cryptographic key, would be the digital credential. And the right associated with that is the right to spend money from the account.

Q. Okay. Now's a good time for a break.

MR. WILLIAMS: Off the record.

(Recess taken.)

MR. LINDNER: Back on the record.

Q. Dr. Fiske, I'm going to ask you some questions about terms that are used in the Collinge reference, which is Exhibit 1011. Do you have a copy of Exhibit 1011?

A. Yes.

Q. And you're okay if I refer to this simply as "Collinge" during the deposition today; right?

A. Yes.

Q. Collinge uses the term "unpredictable number." Can you tell me how a person of skill in the art would have understood that term in 2012?

MR. WILLIAMS: Objection to form.

A. So there is a data item which is generated by the payment terminal and sent to the card during a payment transaction, which is called an unpredictable number, and a person of skill would identify it by its tag value, which has gone out of my head at the

diagrams.

Q. So your answer after you reviewed Fiske further was not based on something additionally that you saw in Fiske that described the cardholder verification process and the PIN or passcode. You came to that answer from just your understanding of the portion of column 15 that I directed you to earlier. Is that right?

A. Correct. So if you look in column 15 and you look in line 43, it talks about specific input from the user. And if you look in line 48, it says, "for example, in the form of password."

Q. How would a person of skill in the art have understood in 2012 the term "payment system"?

MR. WILLIAMS: Objection to form.

A. The term "payment system" is quite a broad one. In the context of what we're discussing here, the international payment brands -- examples, Visa, MasterCard -- in some cases may be called card schemes. In others they may be called payment brands. They may be called card payment networks. And in some documentation they're called payment systems.

Q. Would a person of skill in the art in 2012 have been aware of various different payment systems?

A. Yes.

Q. So in 2012 what were the mainstream contactless payment transactions?

MR. WILLIAMS: Objection to form and scope.

A. In the U.S., which in 2012 was not a country that had yet migrated to EMV, the acquiring networks that transport the transaction data from the terminal through the acquirer card network to the issuer were really only capable of transferring information in what's called Track 2 data -- sometimes Track 1 data, but Track 2 data. So there's actually very little space available.

So for that reason, in contactless at that time in the U.S. there were variants of contactless payments for each of the brand. So American Express had ExpressPay magstripe mode. Visa had legacy MSD. MasterCard had PayPass Magstripe, and Discover had Discover Zip. So those were the predominant contactless transaction methods in the U.S.

Outside the U.S., in the rest of the world, which had already migrated to EMV, they were capable of transferring the full ICC data from terminals through to issuers. And so those magnetic stripe variants of contactless were not necessary.

So in the case of MasterCard, that's

Q. And in magstripe mode, the information sent from the terminal or the POS to the acquirer and/or issuer would be different than information sent in EMV mode; right?

A. Correct.

Q. Give me one moment. I have a piece of paper I need to just grab that's out of view here.

Could I direct you to Exhibit 1020.

A. This is EMV 4.2, Book 2?

Q. Yes.

A. Security and Key Management, yes.

Q. And I'd like to direct you to Section 8, which begins on Page 99 of Exhibit 1020.

A. Application Cryptogram and Issuer Authentication.

Q. So you see that the first sentence of that section says, "The aim of this section is to provide methods for the generation of the application cryptograms"?

A. Yes.

Q. And the last sentence on this Page 99, you see that it says, "Note that the methods provided in this specification are not mandatory. Issuers may decide to adopt other methods for these functions"?

A. Yes.

Q. What does it mean when it says that "the methods provided in this specification are not mandatory"?

A. It describes a way that issuers may choose in their specifications to generate application cryptograms and perform issuer authentication. But because the issuers are in control of the application on the card -- actually, that's not quite right, but let's run with it for now.

Because the issuers are in control of the applications that run on the card and they're also in control of the logic that runs inside their host authorization systems, they may choose if they wish to do something different from what everybody else does.

As far as EMV is concerned, all it is doing is providing a globally interoperable mechanism whereby that issuer's card can interact with any EMV terminal and information can get through to the issuer. But how that information is generated could be up to the issuer.

Q. So is it accurate, then, to say that a card could be compliant and compatible with the EMV specifications without adopting the methods that are provided in Section 8 as to the generation of the application cryptogram?

A. Correct. That's what "not mandatory" means.

MR. LINDNER: We can take a break now, go off the record.

(Recess for lunch.)

MR. LINDNER: Let's go back on the record.

Q. Good afternoon, Dr. Fiske. I wanted to direct you first to Exhibit 1020. That's the one we were looking at earlier, which is Book 2, Security and Key Management.

A. Okay.

Q. On Page 142, which is Appendix A1.3 --

A. Yes.

Q. -- do you see the section there describing session key derivation?

A. Yes.

Q. And at the bottom of that section do you see it says, "Note that the session key derivation method provided in NX A1.3.1 is not mandatory. Issuers may decide to adopt another method for this function"?

A. Yep.

Q. So does that indicate that a payment application could be interoperable with the EMV specifications without deriving session keys the way that the specification provides in this section?

A. Yes.

around. I was looking for elements that were not anticipated or that I felt were not obvious, and I didn't find any. Does that answer your question?

Q. So in your analysis you found that every element within each challenged claim was anticipated by Collinge; right?

A. Yes, anticipated or obvious.

Q. We're getting the words kind of mixed up here. I apologize.

A. Okay.

Q. You said a moment ago that you didn't find any elements that were not anticipated or that were not obvious. So are you saying that you did not make a distinction between those two -- those two unpatentability theories?

A. I think the answer to that is that I didn't explicitly check each claim for anticipation on its own but instead considered whether each claim was anticipated or obvious.

Q. So in Paragraph 20 of your declaration you say that you "understand an obviousness evaluation can be based on a combination of multiple prior art references." And you also say, "I understand that the prior art references themselves may provide a suggestion, motivation, or reason to combine, but

understanding it correctly, because you seem to have identified remote-SE system 100 in one instance and then remote-SE system 110 in another instance?

A. I think that's a typo. I'm looking in Figure 7 in Collinge. I don't see, unless I've missed it, anything labeled 100. But I do see the cloud system, the remote system, being labeled as 110.

Q. Okay. So on Page 51, the quote to system 100 from Paragraph 81 of Collinge probably should have said 110 there? That's what you meant?

A. I think so. I can't see in either Figure 6 or Figure 7 an item identified with a 100. But the remote-SE system is clearly labeled 110 in both diagrams.

Q. So it is remote-SE system 110 that you are identifying as the remote computer system from the claim; right?

MR. WILLIAMS: Objection to form.

A. Yes. And in that sentence, which uses 100, it's actually talking about transmitting the generated CAP token, which will go to the authentication, so this 702, which is within 110. So yes, I'm pretty convinced that's a typo.

Q. And just for the sake of clarity, because I think that the figure in your declaration may have

some annotations that are on top of some of the original graphics in Figure 7. So if we look at the unannotated version of Figure 7, which is in Collinge page 8 --

A. Correct.

Q. So in that figure we see 110, which is essentially pointing to a sort of gray box in the lower left quadrant of Figure 7; right?

A. Yes.

Q. I'd like to point you now to Paragraph 96 of your declaration. In Paragraph 96 you say that KSUN, which is in Collinge written as capital K capital S and then subscript UN -- you say that KSUN is a non-permanent cryptographic key associated with the account, and that it's transmitted to the mobile device as part of an encrypted payload. Right?

A. Yes.

Q. Is KSUN an unpredictable number?

MR. WILLIAMS: Objection to the form and scope.

A. It's a session key. It's not an unpredictable number because it's not the result of running a random number generator. But it is a number that, without the knowledge of the issuer master key, you would be able to predict or calculate.

is why I think they've chosen to call it a session key unpredictable number.

Q. So let me make sure I got your earlier answer, because as I'm looking at what you said, it looks like when I asked if KSUN was an unpredictable number, you said that it's not an unpredictable number because it's not the result of running a random number generator, but it is a number that without the knowledge of the issuer master key you would be able to predict or calculate.

A. Correct.

Q. So how would one be able to predict or calculate the session key KSUN without the knowledge of the issuer master key?

A. You would not be able to predict the value of KSUN unless you knew the value of the issuer master key.

Q. Okay, that's what I thought maybe you were trying to say. I think your previous answer, maybe you left the word "not" out.

A. Okay.

Q. That might --

A. Let me just explain my understanding of the process of generating KSUN.

So as with EMV, you start with an issuer

master key. You drive a card-specific key by using the issuer master key and operating over the PAN and the PAN sequence number, and that's defined in EMV.

What is then defined in EMV is a mechanism where you take the card key and you operate over the application transaction counter, and that generates the session key. And that mechanism is in EMV, and it's also in Fiske.

What Collinge does is, instead of just iterating -- or encrypting the --

No, instead of deriving the session key using just the application transaction counter, they also use what they call UNCLOUD, which is the result of the random number generation. So that's why they call it a session key unpredictable number, to differentiate it from a normal EMV session key. That's how I would understand it.

Q. And is there a place in Collinge, Exhibit 1011, where you could point me to that shows this derivation of the session key that you just described?

A. No, because as I said earlier, when I read Collinge I found the use of the UNCLOUD confusing. It was only when I went back to the provisional that I found the clarity of those derivation algorithms.

Q. I see. So what you found was that Collinge,

Exhibit 1011, by itself does not describe in enough detail for you to understand it how KSUN is derived. Right?

MR. WILLIAMS: Objection to form.

A. That's correct. I needed -- in order to fully understand, I needed to refer to the provisional, which is, I think, Exhibit 1009.

Q. Does Collinge, Exhibit 1011, specify the parameters that are used to generate KSUN? And I could point you to Paragraph 94 of your declaration, which might be helpful in answering this question.

A. Yeah, I see paragraph 50, and that certainly is part of the story. But I think the whole story is best described in the provisional.

Q. Does paragraph 50 of Collinge describe how KSUN is generated?

MR. WILLIAMS: Objection to form.

A. Paragraph 50 describes how a single-use key is generated.

Q. Which portion of paragraph 50 are you referring to?

A. The generating key, which is on the fourth line.

Q. So are you talking about the sentence that says, "The single-use key may include an application

MR. WILLIAMS: Objection to form and scope.

A. So we know that the KSUN is calculated from the card-specific key, and we know that the card-specific key is calculated from a master key using part of the PAN. So when you ask for a KSUN, you need to know which PAN is being used to generate it, and that PAN is account-specific.

Q. So where in Paragraph 94 do you describe the account-specific PAN being used to generate the KSUN?

A. Sorry, could you ask the question again?

Q. Yes. Where in Paragraph 94 do you describe that KSUN is generated using the account-specific PAN or a portion of it?

A. Well, that's not described in Paragraph 94, but elsewhere, particularly in the provisional, the algorithm for deriving KSUN is described; and as part of that, the use of the PAN is described.

Q. If during communications between a mobile application and a remote computer system the remote computer system transmits a timestamp, would you consider that timestamp to be associated with the account?

MR. WILLIAMS: Objection to form and scope.

A. I think not. Now, the timestamp is being delivered as part of a communication session, which is unique to an account. But the timestamp itself would not be useful to work out which account it's associated with.

So in what you described to me, I would say that the timestamp is an attribute, which is actually more an attribute of the communication session than of the account.

Q. And you said that the timestamp would not be useful to work out which account it's associated with. Useful to whom?

A. Useful to an attacker. Useful to anybody eavesdropping on the communication.

Q. So if we look at information that is sent as part of an account-specific request but that would not be useful to work out which account it's been associated with, you would say that that information is not associated with the account; right?

MR. WILLIAMS: Objection to form and scope.

A. I would say that it's not. So I'm thinking here of an example where you might set up a session to retrieve a session key from the provisioning system, and when you receive that session key, you also

receive a timestamp.

What that would allow a mobile device to do is to implement some kind of time-to-live logic. So the mobile device could say, "I received this session key over 24 hours ago. That's too long. I can delete it rather than continue to use it."

But in that case the timestamp is not associated with the account, it's actually associated with the session key and the time it was received or transmitted.

So I think that's my answer.

Q. All right. And just for clarity, because my question -- my last question ended with the word "right" and your answer began with the phrase "I would say that it's not," let me just make sure that it's not confusing for the record.

But your testimony is that as to the information that would be sent as part of an account-specific request but that wouldn't be useful to work out which account it's been associated with, that is not associated with the account.

A. It's associated --

MR. WILLIAMS: Objection to form.

A. It's associated with the information that was synched as part of the response to that information

request. Now, if all of that information, as we would expect, is related to one account, then you might be correct in saying that that timestamp is associated with the account. But it's not an association that's like a one-to-one.

So on a second request on the same account, you would get a different timestamp. And if all you had was the timestamp, you would not be able to work out which account it was referring to.

So the direct association is not with the account, it's with the data that's being downloaded, which in the context of what we're discussing here would be the session key.

Q. Okay. I'd like to direct you to Page 53 of your declaration. Do you see that limitation 1.E-3 recites at the end of the limitation "the at least one device response communication comprising at least one response application data protocol unit"?

A. So for clarity, you actually mean Page 62 of the exhibit, which is labeled Page 53?

Q. Thank you.

A. You're welcome.

Q. So do you see the claim limitation that I read?

A. Yes, I see that.

A. But I'm going to try and answer it, if I may, by saying that I have knowledge of the PayPass card specification. So when I looked at Collinge, and in particular at some of the diagrams to show flows between card and reader, I recognized those flows as complying with the PayPass specifications.

But to follow on from that: The purpose behind being able to do payment -- contactless payments with a device which doesn't have a secure element is to expand the ability of a payment system to reach all customers or to reach customers in a different way, while still maintaining interoperability.

So in my opinion, any invention which did not comply with those specifications would be an invention which would have very little utility.

Q. I'd like to take you to Paragraph 132 of your declaration.

A. One three two?

Q. Yep, 132.

A. Okay.

Q. Is it your opinion that the issuer processing server 308 retrieves the UNCLOUD and KSUN using -- let me start again.

The first sentence in Paragraph 132 looks

like it's saying that the issuer processing server 308 validates payment CVC3 using the UNREADER, UNCLOUD, and application transaction counter by retrieving UNCLOUD and KSUN values. Can you explain that a little bit further?

A. So the detail of this is in the provisional, again. And this was one of the areas where I, in just reading Collinge, had maximum confusion, particularly around the use of UNCLOUD.

So the job of the issuer processing server at this point is to receive the CVC3 and to repeat the calculations that were performed to create it, because if you can repeat the calculations and you get the same result, then you can be satisfied that the CVC3 is correct.

So in order to repeat those calculations, you need to go through the same process of starting with the issuer master key, deriving it to the card key using the PAN and the PAN sequence number, deriving the session key from the unpredictable number -- sorry, deriving the session key using the ATC, and in this case the UNCLOUD as well, and then calculating the CVC3 using the UNREADER unpredictable number.

Q. So in looking at what you had in Paragraph

A. Yes.

Q. Does Collinge disclose itself how the CVC3 value is calculated, or is that coming from the provisional?

A. That comes from the provisional.

Q. Would you agree that the way a cryptographic key is used to generate a cryptogram depends on the particular payment system?

MR. WILLIAMS: Objection to form and scope.

A. There are parameters present in EMV cards which tell the issuer authorization systems how to repeat the calculation of the cryptograms. Different card schemes use those parameters in different ways. But a person of skill in the art would understand the principles behind the calculation and validation of a cryptogram.

From my experience there are differences in the way the cryptograms are calculated, but those really come down to two forms. One is whether a session key is used or not and how it's derived, and the other is the input data that goes into the cryptogram calculation.

EMV provides a data item, called the cryptogram version number, which cards send to issuer

ACKNOWLEDGMENT OF DEPONENT

I, Stuart Fiske, PH.D., do hereby acknowledge that I have read and examined the foregoing testimony, and the same is a true, correct and complete transcription of the testimony given by me, and any corrections appear on the attached Errata sheet signed by me.

28-6-24. _____

(Date) (Signature)

CERTIFICATE OF COURT REPORTER

I, Alan H. Brock, Registered Diplomate Reporter and Notary Public, the officer before whom the foregoing deposition was taken, do hereby certify that the foregoing transcript is a true and correct record of the testimony given; that said testimony was taken by me stenographically and thereafter reduced to typewriting under my supervision; that reading and signing was requested; and that I am neither counsel for nor related to nor employed by any of the parties to this case and have no interest, financial or otherwise, in its outcome.

IN WITNESS WHEREOF, I have hereunto set my hand and affixed my notarial seal this 15th day of June, 2024.

My commission expires March 25, 2027.

_____

Alan H. Brock, RDR, CRR