

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

TransPerfect Legal Solutions
212-400-8845 - Depo@TransPerfect.com

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

1 INDEX OF EXHIBITS REFERRED TO

2

3 1009 79

4 1011 42

5 1012 46

6 1020 60

7 1023-1029 52

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

June 14, 2024 9:58 a.m.

P R O C E E D I N G S

STUART FISKE, PH.D.,

being first duly sworn or affirmed to testify to the truth, the whole truth, and nothing but the truth, was examined and testified as follows:

EXAMINATION

BY MR. LINDNER:

Q. Good morning, Dr. Fiske. My name is Seth Lindner. I'm with the law firm BC Law Group.

How are you today?

A. Good, thanks.

Q. Have you been deposed before?

A. Once.

Q. Was that by video or in person?

A. That was in person.

Q. All right. So I'll go over just a few sort of procedural things as far as the depo goes. So I'll be asking questions, as you know, and please wait for me to finish my question before you answer. Sometimes you might hear sort of a pause as I'm trying to get my words just right for the question, so bear with me if that happens. Does that sound good?

A. Sure.

Q. If you don't understand my question, please

1 let me know. Otherwise I will assume that you do
2 understand. Is that fair?

3 A. Yes.

4 Q. All right. And then the deposition today is
5 not being recorded by video, but the court reporter is
6 writing down all of the words that we say. So it's
7 important here to give verbal answers rather than, you
8 know, nodding your head or that kind of thing. Sound
9 good?

10 A. Okay.

11 Q. You submitted a declaration in IPR2023-01289.
12 Correct?

13 A. Yes.

14 Q. Do you have a copy of your declaration with
15 you?

16 A. I do.

17 Q. What other materials do you have with you?

18 A. So in front of me I've got the declaration,
19 the Yeager patent, the Collinge patent, the
20 provisional for the Collinge, and the Fiske patent.
21 And over here there are four large binders with an
22 awful lot of paper in it, holding the exhibits that
23 are referenced in the declaration.

24 Q. And it looks like there's some kind of a
25 computer screen or a monitor to your left there.

1 What's on that one?

2 A. That's not mine. That's Eliot's. But at the
3 moment it's showing the front page of the declaration.

4 Q. And are you controlling that computer or is
5 counsel controlling that computer?

6 A. Counsel is controlling that computer.

7 Q. Okay.

8 MR. LINDNER: Can we go off the record for
9 one second?

10 MR. WILLIAMS: Sure.

11 (Discussion off the record.)

12 MR. LINDNER: We can go back on the
13 record.

14 Q. So, Dr. Fiske, if at some point during
15 today's deposition you see a document or any notes or
16 any materials on the computer screen to your left, or
17 any other screen that you can see right now, would you
18 let me know in your response to your next question --
19 or to my next question that that's what you're seeing
20 there?

21 A. Okay.

22 Q. So some shorthand for today. When I refer to
23 this IPR or this matter, do you understand that I will
24 be talking about IPR2023-01289?

25 A. Yes. The reason why I paused in my original

1 answer to your question is that I hadn't actually
2 committed that number to memory. But I'm going with
3 the fact that you're not misquoting it.

4 Q. Okay. And your declaration concerns U.S.
5 Patent No. 10,032,171; right?

6 A. Correct, correct.

7 Q. So today you're okay if I refer to that as
8 the '171 patent?

9 A. Yes.

10 Q. And when I refer to your declaration, you'll
11 understand that to be the declaration that you
12 submitted in this IPR; right?

13 A. Yes.

14 Q. When were you first contacted by counsel for
15 MasterCard regarding this IPR?

16 A. I guess I don't remember the date.

17 Q. Can you give me an approximate date range?

18 A. I think I'd need to check my work records to
19 give you a proper answer on that.

20 Q. Have you worked for MasterCard previously?

21 A. I have been assigned to MasterCard projects
22 in the past, yes.

23 Q. What was the nature of those projects?

24 A. There were several projects, going all the
25 way back to 2003 intermittently. Those early projects

1 concerned the use of contactless payment cards.

2 Q. And in what capacity were you employed by
3 MasterCard during those projects?

4 MR. WILLIAMS: Objection to form.

5 A. I wasn't employed by MasterCard. I've always
6 been employed by my -- the company that I work for
7 now. These were consulting assignments.

8 Q. By "consulting assignments," do you mean that
9 you were serving as an expert witness, or were you
10 consulting in a different capacity?

11 A. I was -- in those cases I was acting as a
12 technical consultant.

13 Q. Were you a technical consultant regarding a
14 matter before MasterCard that was a legal matter, or
15 something else?

16 A. At that time these were all technical
17 assignments, not legal assignments.

18 Q. And over the period of time from when you
19 first worked for MasterCard, approximately how much
20 money did you earn through that work, prior to the
21 current IPR?

22 A. So, again, I am actually employed by my
23 company, and so the salary I draw from my company are
24 my earnings.

25 MasterCard would pay my company consulting

1 fees for the work that I and my colleagues did.

2 Q. And can you give me an approximate value for
3 how much MasterCard paid your company during all of
4 that consulting work prior to this IPR?

5 A. I really can't. I'm sorry. But it would
6 have been over something like 20 years.

7 Q. Can you approximate how many hours or what
8 percentage of your time during that period you were
9 working on matters on behalf of MasterCard?

10 A. Again, to answer that question I'd need to
11 consult my work records.

12 Q. So you have no idea, sitting here today, even
13 roughly how much work you have done on behalf of
14 MasterCard over the past 20 years?

15 MR. WILLIAMS: Object to form.

16 A. I can't give you a realistic number at all.

17 If you look in the declaration and look at
18 my CV, you'll see that most of my time over that
19 period was actually spent working on assignments for
20 American Express. Over that period I've worked on
21 assignments for American Express, MasterCard, Visa,
22 and Discover. But what proportion of my time was
23 spent on which payment brands and which other
24 customers, I can't tell you.

25 Q. Would you say that during any of those years

1 you spent more than 10 percent of your time on
2 MasterCard as compared to your other work?

3 A. I would say not.

4 Q. More than 5 percent of your time?

5 A. I'm sorry, I can't -- I can't answer that
6 question.

7 Q. More than 1 percent of your time?

8 A. There would probably have been some years
9 where I would have spent more than 20 days in the year
10 working on assignments for MasterCard, but it
11 certainly wouldn't have been every year. And again, I
12 would need to go back to my work records to give you
13 an accurate answer on that.

14 Q. How many years would you say you had
15 somewhere around 20 or more days that you spent
16 working on behalf of MasterCard?

17 A. Again, I can't remember. I would need to
18 consult my work records.

19 Q. More than one year?

20 A. I'd be guessing if I answered that question.
21 So again, I would need to consult my work records.

22 Q. And are you still employed by the same
23 company that you were employed with when you did this
24 prior work for MasterCard?

25 A. Yes.

1 Q. So what is the nature of that company's
2 business?

3 A. So the company is called Hyperion Systems
4 Limited. We trade under the name Consult Hyperion.
5 We're based in Guilford in the UK, and we are a
6 technical consultancy, consulting in payments,
7 identity, and fare collection, transit fare
8 collection.

9 Our customers as well as the major
10 international card schemes that I've already listed
11 include acquiring banks, issuing banks, and transit
12 agencies, together with a large number of technology
13 companies who wish to design and build products to
14 sell to those organizations.

15 The core skills that I have and that we
16 offer are specifying solutions, assisting in the
17 implementation of those solutions, and then testing
18 those solutions once they've been implemented.

19 Q. Is your company currently doing work for
20 MasterCard outside of this IPR?

21 A. I don't believe so, no.

22 Q. Do you expect that your company in the future
23 would do work for MasterCard outside of the expert
24 consulting in a legal matter?

25 A. Yes, given that we're a technical consultancy

1 setting to the payments industry, I would hope that we
2 would be able to win work with Visa, American Express,
3 MasterCard, Discover, JCB. China Union Pay may be a
4 bit of a stretch.

5 Q. If you could estimate the relative earnings
6 by your company from the various clients or customers
7 that you serve, what would that look like?

8 MR. WILLIAMS: Objection to form and
9 relevance.

10 A. I think our billings for the last year were
11 on the order of 5.4 million pounds sterling. That's
12 across the whole range of customers that we have.

13 Q. And across that range of customers, what are
14 the largest customers and what percentage of earnings
15 comes from those entities, approximately?

16 A. I would need to consult my financial
17 controller to get a realistic answer to that.

18 Q. Are the entities that you listed -- Visa,
19 American Express, MasterCard, Discover, JCB -- what
20 you would consider to be your company's top customers?

21 A. Of those that you've listed that I mentioned,
22 I would say American Express is in our top ten. The
23 others are not. The remaining top ten customers are
24 predominantly U.S. banks and transit agencies.

25 Q. Did you review the '171 patent before being

1 retained in this matter?

2 A. No.

3 Q. Did you review any of the exhibits filed in
4 this IPR before being retained?

5 MR. WILLIAMS: Objection to form.

6 A. Well, as I was involved in reviewing the Visa
7 patent, or the Fiske patent, the answer is yes to that
8 one.

9 A lot of the exhibits here are references
10 to EMV specifications, and those are things that I've
11 been reading for several years now.

12 Q. Did you speak to anyone at MasterCard about
13 this matter prior to being retained?

14 A. No.

15 Q. Are you aware that OV Loop and MasterCard are
16 involved in a patent infringement lawsuit in Federal
17 Court?

18 A. Yes. Counsel informed me of that.

19 Q. Are you involved in that lawsuit in any way?

20 A. No.

21 Q. So you have not been engaged to assist in --
22 as either a consultant or a testifying expert in the
23 OV Loop v. MasterCard lawsuit; correct?

24 A. Correct.

25 Could I just clarify my answer there?

1 Inasmuch as I say that on the assumption that what
2 we're discussing today does not form part of that
3 lawsuit.

4 Q. Fair enough. Would you consider yourself an
5 expert programmer?

6 A. I have been writing computer programs for --
7 oh, I can't do this. Let me think about this.

8 I started programming at school. That
9 would be back in the late '60s, early '70s. And I
10 have been writing code ever since. I am sure that
11 there are many more expert coders than me.

12 Q. Would you consider yourself an expert in
13 application development?

14 MR. WILLIAMS: Objection to form.

15 A. There are particular types of application
16 that I have been involved with over the years, and I
17 would claim expertise in those areas.

18 Q. Which areas have you been involved in where
19 you'd claim expertise?

20 A. In payment applications, both applications
21 that run inside smart cards and applications that run
22 inside readers that communicate with smart cards.

23 Q. I'd like to ask you some questions about your
24 understanding of a couple of legal terms. So I'll
25 direct you to Pages 13 through 14 of your declaration.

1 A. So when you say Pages 13 and 14, in the copy
2 I'm looking at, for example, at the foot it says
3 "MasterCard, Ex1006, p. 13," but it's actually labeled
4 in the center as Page 4.

5 Q. Yes, that's a good point, and we'll have to
6 deal with that issue throughout the deposition today.
7 When I'm referring to page numbers, just for
8 consistency, throughout our time here, I'm always
9 going to use the page number that follows the
10 MasterCard and then the exhibit number in the bottom
11 right corner of the page.

12 A. Okay. So in this case you're looking at
13 Page -- near the bottom says "Understanding of the
14 Law."

15 Q. That's right. So in Paragraph 13 you say
16 that you understand that "a prior art reference
17 anticipates a challenged claim, and thus renders the
18 claim invalid, if all limitations of the claim are
19 disclosed in that prior art reference, either
20 explicitly or inherently (i.e., necessarily present or
21 implied), as arranged or combined in the claim." Do
22 you see that?

23 A. I do.

24 Q. And is that the understanding that you
25 applied when you rendered your opinions as to

1 anticipation in this IPR?

2 A. Yes.

3 Q. Are there instances where your opinion is
4 based not on an explicit disclosure in the prior art
5 but on an implied disclosure?

6 MR. WILLIAMS: Objection to form.

7 A. Are you asking that question in the context
8 of anticipation?

9 Q. Yes.

10 A. And I think the answer is no.

11 Q. I'll now direct you to the following section,
12 which is on Page 14 and continues on for several
13 pages, regarding the legal standard for obviousness.
14 Do you see that?

15 A. Yes.

16 Q. And in Paragraph 18 you say, "I also
17 understand that an obviousness determination includes
18 the consideration of various factors such as (1) the
19 scope and content of the prior art, (2) the
20 differences between the prior art and the challenged
21 claims, (3) the level of ordinary skill in the
22 pertinent art, and (4) the existence of secondary
23 considerations, also referred to as objective
24 considerations, of non-obviousness." Do you see that?

25 A. Yes.

1 Q. When you rendered your opinions as to
2 obviousness of the claims of the '171 patent in your
3 declaration, is this methodology here in Paragraph 18
4 the one that you applied?

5 A. Yes.

6 Q. Were there any instances where in forming
7 your opinion as to obviousness that your opinion
8 changed based on the fourth factor here, regarding
9 secondary considerations?

10 MR. WILLIAMS: Objection to form.

11 A. I don't think so, no.

12 Q. All right, I'm going to ask you about some
13 terms that appear either in the '171 patent or in one
14 of the exhibits that you relied on for your
15 declaration. And when I ask you about these terms,
16 I'm going to be asking about how a person of skill in
17 the art in 2012 would have understood these terms.
18 Does that sound fair?

19 A. Yes.

20 Q. Would a person of skill in the art in 2012
21 have been familiar with the term "associated with an
22 account"?

23 MR. WILLIAMS: Objection to form.

24 A. I believe they would, yes.

25 Q. How would a person of skill in the art have

1 understood the plain meaning of that term?

2 MR. WILLIAMS: Objection to form.

3 A. So the context here is making payments using
4 a payment card. Someone who understands the payments
5 industry would know that there are payment accounts
6 from which to pay funds to make purchases, and there
7 are payment cards, and that a funding account or a
8 payment account could have multiple cards associated
9 with it -- for example, a primary cardholder and a
10 supplementary cardholder.

11 So, that said, they would understand the
12 phrase "associated with an account," in my view.

13 Q. So in your opinion, a person of skill would
14 understand that "associated with an account" refers to
15 a payment card that is associated with a payment
16 account?

17 MR. WILLIAMS: Objection to form.

18 A. That's kind of a circular definition. But
19 yes. There are payment cards and there are funding
20 accounts, and a payment card grants you access to make
21 payments from that funding account.

22 Q. So if we wanted to know whether a particular
23 piece of information is associated with an account,
24 how would a person of skill in the art determine that?

25 MR. WILLIAMS: Objection to form and

1 scope.

2 A. So, first of all, you would need to
3 understand what the data item is representing, in
4 order to understand whether it was representing
5 something that linked to a payment card or to the
6 account of the payment card or to the funding account.
7 So it would depend on the particular data item.

8 Q. So can you give me some examples of
9 information that a person of skill in the art would
10 understand to be associated with an account.

11 A. Sure. So the simplest example would be the
12 card number that at that time was embossed on the
13 front of the card, called the primary account number,
14 or generically we call it the PAN.

15 So the PAN identifies the card account
16 that the payments will be taken from. Those card
17 accounts will be associated with funding accounts. So
18 when, for example, with a credit card purchase you buy
19 something with your credit card, then an amount is
20 debited from your credit card account and at the end
21 of the month, when you pay your bill, you pay the
22 money into the funding account.

23 Q. Did you say earlier that a "payment account"
24 or a "funding account" are interchangeable terms?

25 MR. WILLIAMS: Objection to form.

1 A. I think I used those terms interchangeably,
2 because your question was actually about an account,
3 without specifying what type of account.

4 So to be more precise, I would say that
5 there are card accounts and there are funding
6 accounts, and you make payments from the card account,
7 and when you pay off your bill at the end of the
8 month, you pay it into the funding account. The
9 issuing bank will manage the linkage or the
10 associations between those.

11 Q. So would a person of skill in the art in 2012
12 understand that all of the information on a physical
13 credit card is associated with either a payment
14 account or a funding account?

15 MR. WILLIAMS: Objection to form.

16 A. In my head I'm running through all the
17 information that at that time you would see on a
18 payment card.

19 Are we talking about a U.S. payment card
20 or another payment card? The reason why I ask that
21 question is that at that time there were very few, if
22 any, U.S. payment cards that contained a chip, whereas
23 in Europe, for example, the predominant number of
24 payment cards included a chip on them.

25 Q. So I think I'm asking about the printed

1 information that one would see on the card, just
2 holding it in your hand and looking at it.

3 A. Okay. So there is some information which is
4 not specific to the account -- the bank name, the
5 logo, for example. But there is other information
6 that is specific to the account, so the card number,
7 the expiry date. If you turn the card over, you would
8 see a three-digit number, the card security code.
9 Those would be unique to the card account.

10 If you had two cards operating off the
11 same funding account, then that information on the
12 cards would be different, but the transactions would
13 still get posted through to the funding account, and
14 you would make one payment at the end of the month to
15 pay off any outstanding debt.

16 Q. So you said that there's some information on
17 a card that is, for example, the bank name or the logo
18 for Visa or MasterCard that are not unique to the card
19 account and therefore are not associated with the
20 account. Is that right?

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

23 A. That's correct. Another example might be, if
24 you were to look at the back of your payment card, you
25 may find a customer service number, which would not be

1 unique to your account.

2 Q. Would a person of skill in the art have
3 understood that the '171 patent uses the term
4 "associated with an account" according to the plain
5 meaning that we've just been discussing?

6 MR. WILLIAMS: Objection to form.

7 A. Yes.

8 Q. How would a person of skill in the art in
9 2012 have understood the term "account identifier"?

10 MR. WILLIAMS: Objection to form.

11 A. They would have understood "account
12 identifier" as a data item which identifies a card
13 account and would almost certainly have taken that to
14 mean the PAN, or the card number.

15 Q. When you say a data item which identifies a
16 card account, does that mean it uniquely identifies a
17 particular card account?

18 MR. WILLIAMS: Objection to form and
19 scope.

20 A. The card number will identify the card
21 account. You can have multiple cards on the same
22 account. For example, when a card expires at the end
23 of its three- or maybe five-year lifetime, you would
24 have a second card, but those cards would have the
25 same card number. So it's kind of a one-to-many

1 relationship.

2 Q. But for each account number, it would only --
3 sorry, let me go back.

4 You mentioned a scenario where there could
5 be over time more than one card that are associated
6 with a particular payment account. Right?

7 A. Correct.

8 Q. Is there an instance where a particular card
9 number would be associated with multiple payment
10 accounts?

11 A. No.

12 Q. So if we were to look at a bank's database or
13 records for a particular payment account, we would see
14 a card number within those records that is unique to
15 that payment account; right?

16 MR. WILLIAMS: Objection to form and
17 scope.

18 A. So I've thought of a situation, which I'm
19 unclear about, which I think happens in some
20 countries, where you present a card to make a payment,
21 and the terminal asks you whether you want to pay from
22 your savings account or from your checking account.
23 And I don't know whether, when you make that decision,
24 the transaction happens with a different card number,
25 with a different PAN.

1 Q. Is the three-digit code that you mentioned
2 that's printed on the back of a credit card unique to
3 a particular account, or are those codes potentially
4 the same between unrelated cards and accounts?

5 A. They would be -- well, a three-digit code
6 gives you a thousand possibilities. If you have more
7 than 1,000 accounts, then you will inevitably have two
8 accounts that have the same three-digit code.

9 Q. Would you consider that three-digit code to
10 be an account identifier?

11 A. No.

12 Q. Why not?

13 A. Because it doesn't identify an account.

14 Q. Is the three-digit code associated with an
15 account?

16 MR. WILLIAMS: Objection to form.

17 A. A three-digit code can be used as part of the
18 data that's considered by the issuer when deciding
19 whether to authorize a transaction or not. That's
20 what it's there for.

21 Q. Would a person of skill in the art have
22 understood that the '171 patent uses the term "account
23 identifier" according to the plain meaning that we've
24 just discussed?

25 MR. WILLIAMS: Objection to form.

1 A. I believe so. I think I already said that
2 they would have understood the account identifier to
3 be the PAN.

4 Q. Would a person of skill in the art in 2012
5 have been familiar with the term "computer system"?

6 A. Yes.

7 Q. How would a person of skill in the art have
8 understood the plain meaning of "computer system"?

9 MR. WILLIAMS: Objection to form and
10 scope.

11 A. They would have understood it to mean a
12 system which has a central processing unit; storage,
13 both transient and nonvolatile storage; and input/
14 output capability as well.

15 Q. Can a computer system include more than one
16 computer?

17 MR. WILLIAMS: Objection to form, scope.

18 A. I'm not sure I understand the question here.
19 If there are two computers, then there would be two
20 computer systems.

21 It's possible, of course, to network
22 computers together and to design an overall solution
23 where different elements or different computers
24 undertake different but coordinated tasks.

25 Q. And if one were to design such a network of

1 computers, a person of skill in the art would consider
2 that to be more than one computer system; right?

3 MR. WILLIAMS: Objection to form and
4 scope.

5 A. The word "system" is actually quite loose in
6 its definition. It could encompass multiple
7 computers, or at some level of detail you might refer
8 to that collection of computers as a single system.

9 Q. In what context would a person of skill in
10 the art refer to a collection of computers as a single
11 system, as opposed to separate systems?

12 MR. WILLIAMS: Objection to form and
13 scope.

14 A. So in the context of payments, let's consider
15 an issuing bank. When a transaction arrives at an
16 issuing bank looking for authorization, there are a
17 number of steps that need to be undertaken before the
18 issuing bank can decide whether to authorize the
19 transaction or not. That may well include, first of
20 all, authenticating the transaction on the transaction
21 data to establish that the card is genuine, and
22 potentially to also establish that the cardholder is
23 the genuine cardholder for that card.

24 There would be an authorization component
25 to establish whether the account from which the

1 transaction is to be funded has enough money in it to
2 fund the transaction.

3 Then there will be a fraud management
4 system which looks at transactions as they come in to
5 determine whether a transaction is likely to be
6 fraudulent or not. And there may also be a customer
7 service system, that looks at the transactions that
8 are deemed to be potentially fraudulent and to
9 override those, in some cases to approve a transaction
10 when that transaction would otherwise be declined.

11 Now, all of those may be one or multiple
12 computer systems each, but the whole thing could be
13 described as an issuing host authorization system.

14 Q. Would a person of skill in the art in 2012
15 have been familiar with the term "communications
16 channel"?

17 MR. WILLIAMS: Objection to form.

18 A. Yes.

19 Q. How would a person of skill in the art have
20 understood the plain meaning of "communications
21 channel"?

22 A. So they would understood that communications
23 involves sending data or messages between two end
24 points, to, in our case, two different computer
25 systems. The word "channel" can be used quite loosely

1 as well. So you might, for example, define
2 communications over wifi as over one channel, whereas
3 over a mobile network as over a different channel.

4 If you go down one level of detail, you
5 may discover that within one particular communications
6 medium it operates at different frequencies, and those
7 often are called channels as well.

8 Q. Would a person of skill in the art have
9 understood that the '171 patent uses the term
10 "communications channel" in a way that's consistent
11 with the plain meaning that you've just described?

12 A. Yes.

13 Q. Would a person of skill in the art in 2012
14 have been familiar with the term "cryptogram"?

15 A. Yes.

16 Q. What would a person of skill in the art have
17 understood as the plain meaning of "cryptogram"?

18 A. A cryptogram is the result of a cryptographic
19 calculation.

20 Q. What's a cryptographic calculation?

21 A. A cryptographic calculation is a calculation
22 that's done over a set of input data using a
23 cryptographic algorithm and a cryptographic key. So
24 an example would be the data encryption algorithm,
25 DEA, or sometimes called DES.

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

4 MR. WILLIAMS: Objection to form and
5 scope.

6 A. So the actual value of a cryptogram without
7 any annotation around it to say that it is a
8 cryptogram would appear to be, for example, an 8-byte,
9 64-bit number. And that would be indistinguishable
10 from any other 8-byte, 64-bit numbers that weren't
11 cryptograms.

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

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

22 A. Yes.

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

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

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

8 MR. WILLIAMS: Objection to form.

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

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

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

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

1 Q. Why not?

2 A. Because the MD5 algorithm is a hash
3 algorithm, and it doesn't use a key.

4 Q. So an algorithm that is a hash algorithm
5 cannot be used to generate a cryptogram; is that
6 right?

7 MR. WILLIAMS: Objection to form and
8 scope.

9 A. No, that's not correct, either. An algorithm
10 that is used to generate a cryptogram can involve a
11 one-way mechanism, such that, given the output, you
12 cannot go back to determine what the inputs were. And
13 in the '171 patent it's that definition that is used
14 to define a hash.

15 Q. So how would a person of ordinary skill have
16 understand the plain meaning of a "hash" in 2012?

17 MR. WILLIAMS: Objection to form.

18 A. They would have understood the plain meaning
19 of a "hash" to be a calculation which takes data and
20 truncates or digests it down to a smaller amount of
21 data in such a way that you cannot then go back from
22 that smaller amount of data to the original data.

23 They would have understood that the secure
24 hash algorithm suite, at that time particularly SHA-1,
25 but growing in popularity, SHA-2 or SHA256, were

1 examples of secure hash algorithms.

2 They would also know that MD5 was a hash
3 algorithm but it had weaknesses which were such that
4 it wasn't of use in the payments industry.

5 They would have also understood the
6 concept of a message authentication code, which is
7 another way of generating an output from which you
8 cannot go back to the inputs. And in the '171 patent
9 it's that message authentication code concept which is
10 called a hash.

11 Q. Would a person of skill in the art have
12 understood that the '171 patent uses the term "hash"
13 according to the plain meaning that you just
14 described?

15 A. They would have understood, having read the
16 '171 patent, that it's using the word "hash" in the
17 way that you would normally use the word "MAC."

18 Q. Is that different from how a person of skill
19 would have understood the ordinary meaning of "hash"
20 in 2012?

21 MR. WILLIAMS: Objection to form.

22 A. Yes.

23 MR. WILLIAMS: Go ahead.

24 A. Yes.

25 Q. Can you explain that, the difference, please?

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

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

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

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

23 MR. WILLIAMS: Objection to form.

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

1 cryptographic output, which could be called a
2 cryptogram.

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

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

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

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

24 MR. WILLIAMS: Objection to form and
25 scope.

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

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

8 MR. WILLIAMS: Objection to form and
9 scope.

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

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

15 MR. WILLIAMS: Same objection.

16 A. Same answer.

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

20 MR. WILLIAMS: Same objection.

21 A. Same answer.

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

24 A. Yes.

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

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

2 MR. WILLIAMS: Objection to form and
3 scope.

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

9 Q. Is an HMAC an example of a cryptogram?

10 MR. WILLIAMS: Objection to form.

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

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

15 A. Yes.

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

19 MR. WILLIAMS: Objection to form.

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

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

24 MR. WILLIAMS: Objection to form.

25 A. Same answer.

1 Q. Would a person of skill in the art have been
2 familiar with the term "UMAC," U-M-A-C?

3 MR. WILLIAMS: Same objection.

4 A. Same answer.

5 Q. How would a person of skill in the art in
6 2012 have understood the term "cryptographic key"?

7 MR. WILLIAMS: Objection to form.

8 A. They would have understood a cryptographic
9 key to be a value which is used as input to a
10 cryptographic algorithm, and in the context of what
11 we're discussing here, they would have understood that
12 to be a triple DES key as input to the triple DES
13 algorithm.

14 Q. And when you say "in the context of what
15 we're discussing here," are you referring to the way
16 that EMV creates cryptographic keys using the triple
17 DES algorithm?

18 A. Yes.

19 Q. Would a person of skill in the art have
20 understood the term "cryptographic key" outside of its
21 use in EMV?

22 A. Yes.

23 Q. So if a person of skill in the art were to
24 look at a particular data item, would they be able to
25 determine whether or not that data item was a

1 cryptographic key outside of the context of how it is
2 used or derived?

3 MR. WILLIAMS: Objection to form and
4 scope.

5 A. In some circumstances within the context of
6 EMV, there are mechanisms that address cryptographic
7 keys in a way that they can be identified as
8 cryptographic keys. But in the general case, a
9 cryptographic key is just a long binary number, and
10 without any context around it, you wouldn't be able to
11 know that it is a cryptographic key.

12 MR. WILLIAMS: Seth, when you get a
13 chance -- we've been going about an hour -- I'd like
14 to take a break.

15 MR. LINDNER: Let me finish a couple of
16 questions here, and we'll do that.

17 Q. How would a person of skill in the art have
18 understood the term "permanent cryptographic key"?

19 MR. WILLIAMS: Objection to form.

20 A. A permanent cryptographic key would be
21 understood to be a key that doesn't change from the
22 point at which it's created and associated with a
23 payment account to the point at which the card that
24 it's in expires.

25 So it would be a value which is injected

1 into a payment card and is used for the lifetime of
2 that payment card.

3 Q. You say that a permanent cryptographic key
4 would be injected into a payment card. Can you
5 explain that?

6 A. A payment card with a chip in it contains a
7 payment application, and before it's issued to the
8 cardholder, it goes through a process called
9 personalization. And during personalization, data is
10 loaded into the chip and into the payment application.
11 Some of that data is available during a payment
12 transaction in the clear, like the card number, for
13 example. But some of that information is put into the
14 secure chip and is never -- although it's used in the
15 secure chip, it is never emitted from that secure
16 chip.

17 Examples there would be the cryptographic
18 keys that are used to secure a payment transaction.
19 And in the UK, for example, the PIN that's used to
20 prove that the cardholder is genuine is also a
21 confidential piece of information which is
22 personalized into the payment application on the card.

23 Q. You also said in response to my question
24 about the term "permanent cryptographic key," that it
25 does not change from the point at which it's created

1 and associated with a payment account to the point at
2 which the card expires -- or the card that it's in
3 expires, excuse me.

4 A. Correct.

5 Q. How is a permanent cryptographic key
6 associated with a payment account?

7 MR. WILLIAMS: Objection to form and
8 scope.

9 A. It's -- two ways. First of all, it's
10 personalized into a payment card along with the card
11 number, which identifies or associates the payment
12 account. But secondly, if you follow the EMV
13 specifications, the cryptographic key is actually
14 calculated from what's called an issuer master key
15 using data, and the data that's used to derive that
16 cryptographic key includes the most part of the PAN --
17 includes most of the PAN.

18 Q. So associating the permanent cryptographic
19 key with the account is, in your view, the result of
20 generating the key using the PAN or a portion of the
21 PAN?

22 MR. WILLIAMS: Objection to form.

23 A. Correct.

24 Q. Is it possible to recover the PAN or the
25 portion of the PAN that was used to generate a

1 cryptographic key using the cryptographic key?

2 MR. WILLIAMS: Objection to form and
3 scope.

4 A. No.

5 Q. How would a person of skill in the art have
6 understood the term "wireless network" in 2012?

7 A. There are a number of wireless communications
8 technologies which are used. A person of skill in the
9 art would certainly be aware that wifi is a wireless
10 network, that the mobile phone network is a wireless
11 network as well. They may also consider technologies
12 such as Bluetooth to be wireless networks.

13 Q. How would a person of skill have understood
14 the term "digital credential" in 2012?

15 MR. WILLIAMS: Objection to form. And I
16 really would like that break soon, Seth.

17 MR. LINDNER: This is my last one.

18 MR. WILLIAMS: Okay.

19 A. So a person of skill in the art in 2012 would
20 understood that a digital credential is a collection
21 of data items which together provide the recipient of
22 the credential with an identity and a right and
23 probably a proof that the credential is genuine.

24 So in the context that we're talking about
25 here, a payment card would be the credential. The

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

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

6 MR. WILLIAMS: Off the record.

7 (Recess taken.)

8 MR. LINDNER: Back on the record.

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

13 A. Yes.

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

16 A. Yes.

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

20 MR. WILLIAMS: Objection to form.

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

1 moment. I was trying to remember the actual value of
2 the tag. It's 9F37. And that would tell a person of
3 skill in the art that the four bytes following it
4 would be the terminal unpredictable number.

5 Collinge uses other unpredictable numbers
6 as well, but those are not EMV unpredictable numbers.

7 Q. So my question is actually slightly broader
8 than just the particular unpredictable number that you
9 were describing. I'm asking just as a general term
10 what an unpredictable number is as that would have
11 been understood by a person of skill in the art?

12 A. They would have understood that to be the
13 result of a random number generator.

14 Q. What are the characteristics of an
15 unpredictable number?

16 MR. WILLIAMS: Objection to form and
17 scope.

18 A. When a -- when an unpredictable number is
19 generated by a random number generator, there are a
20 number of statistical tests that can be applied to
21 determine whether the resulting number is sufficiently
22 random to be useful in a subsequent calculation.

23 The tests are quite -- or can be quite
24 extensive. I'm aware that one of the tests involves
25 looking at the number of consecutive bits which are

1 all zero, and if the number of bits which are all zero
2 is longer than a certain length, then the number can
3 be deemed to be insufficiently random and would be
4 rejected and another random number would be generated.

5 Q. So are you saying that a person of skill in
6 the art would understand that you could look at a
7 particular data item and perform some tests on that
8 item without knowing its origin and determine whether
9 or not it was an unpredictable number?

10 MR. WILLIAMS: Objection to form and
11 scope.

12 A. No, that's not what I said, or at least
13 that's not what I meant.

14 So if you are generating what you know to
15 be an unpredictable number, then you can apply those
16 statistical tests to determine whether it's a useful
17 unpredictable number or not.

18 Because an unpredictable number is just a
19 stream of 1's and 0's, you cannot look at any stream
20 of 1's and 0's and say that is an unpredictable
21 number, in the same way that you couldn't look at a
22 6 -- a stream of 64 1's and 0's and say that is an
23 application cryptogram. You need the context.

24 Q. Is that the same for a random number, that
25 you need context to determine if a number is random?

1 MR. WILLIAMS: Objection to form and
2 scope.

3 A. The terms "random number" and "unpredictable
4 number" are used interchangeably, although the phrase
5 "unpredictable number" has a very specific meaning in
6 EMV.

7 Q. So I'm not sure that that answered my
8 question, because my question is whether a person of
9 skill in the art would be able to look at a number --
10 so, for example, a 4-byte-long stream of digits -- and
11 determine whether that number is random.

12 MR. WILLIAMS: Objection to form and
13 scope.

14 A. I think the answer to your question is no,
15 because without the context, it's just a 4-byte
16 number, and there is a probability, albeit a low one,
17 that if all of those 4 bytes were 0, it could still be
18 a number that was generated randomly. It could still
19 be unpredictable. If it were always four 0's, it
20 wouldn't be unpredictable. But without the context
21 you can't look at a sequence of 4 bytes and say that
22 is a random number.

23 Q. So a number that is generated randomly is
24 what a person of skill would understand to be a random
25 number?

1 MR. WILLIAMS: Objection to form and
2 scope.

3 A. A person of skill would understand that a
4 number which is the result of running a random number
5 generator would be a random number.

6 Q. Do you agree with the disclosure in Collinge
7 in Paragraph 83 that methods and systems for the
8 generation of unpredictable numbers would have been
9 apparent to a person of skill in the art?

10 A. Sorry, did you say Paragraph 83?

11 Q. I did.

12 A. Okay, sorry, I've got it.

13 Yes, I would agree with that statement.

14 Q. I'd like to turn to Exhibit 1012. Do you
15 have a copy of that?

16 A. That's the Fiske patent?

17 Q. Correct. And hopefully we don't confuse
18 anyone, but I'm going to refer to that as "Fiske"
19 today. Is that all right?

20 A. Sure.

21 Q. I'll try to refer to you as "Dr. Fiske," if
22 that's okay.

23 As the terms are used within Fiske, how
24 are payment keys different from ICC session keys?

25 MR. WILLIAMS: Objection to form.

1 A. Can you give me a reference for where the
2 term "payment keys" is used?

3 Q. I'll direct you to, for example, column 15,
4 line 50 through 55.

5 A. In that paragraph, "payment key" means the
6 key that's used to calculate the cryptogram.

7 Q. And how is that different from a session key
8 or an ICC session key?

9 A. So I'm reading that paragraph, and I see that
10 there is a difference in the paragraph between the
11 stored ICC session keys and the remaining payment
12 keys. But at this instant I'm unclear what purpose
13 the remaining payment keys have if they are not ICC
14 session keys.

15 Q. Do you also see within the portion of Fiske
16 that you're reviewing in column 15 that it discloses
17 "decrypt two separately encrypted data portions" on
18 line 53, or 54?

19 A. Yes.

20 Q. Does that disclosure help you better
21 understand the difference between payment keys and ICC
22 session keys?

23 A. Can I have some time to read further back
24 into the document?

25 Q. Yes.

1 A. Thank you.

2 Okay, I think I understand what this
3 paragraph is saying now. So in this paragraph we are
4 discussing the idea that, rather than just storing the
5 ICC session keys, which are used to make the payment,
6 we may additionally encrypt them with a value which is
7 known to the user and not to an attacker.

8 So the idea here is that there would be
9 one set of session keys which are used for
10 transactions where cardholder verification is not
11 required and there will be another set of session keys
12 which are used when cardholder verification is
13 required. The cardholder verification is achieved by
14 entering the PIN or passcode, which, if it's entered
15 correctly, can be used to successfully decrypt the
16 encrypted payment key to recover the key, which can
17 then be used to conduct an EMV transaction.

18 In both cases the key that is used to
19 conduct the EMV transaction is a session key.

20 Q. Is there a particular portion of Fiske that
21 you reviewed that led you to this understanding?

22 A. Other than what I was just reading?

23 Q. Yes.

24 A. There may be somewhere else a clearer
25 description of that process, but it's not in the

1 diagrams.

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

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

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

15 MR. WILLIAMS: Objection to form.

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

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

25 A. Yes.

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

3 MR. WILLIAMS: Objection to form and
4 scope.

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

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

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

25 So in the case of MasterCard, that's

1 called MasterCard M/ChIp. In the case of Visa it's
2 called QVSDC. In the case of American Express it's
3 ExpressPay EMV mode. And in the case of Discover it
4 was D-PAS Contactless.

5 Q. You've named a bunch of different contactless
6 payment systems. What makes one payment system
7 different from another?

8 MR. WILLIAMS: Objection to form and
9 scope.

10 A. So I mentioned a number of different payment
11 methods or payment products, rather than payment
12 systems, because one of the definitions of "payment
13 system" was the card networks.

14 The things that made those things
15 different were the individual card specifications,
16 which describe the information flowing between card
17 and terminal, and also describe the internal
18 processing of the card applications.

19 Q. So a person of skill in the art would have
20 been aware of different specifications that have
21 different communication protocols between the terminal
22 and the card?

23 MR. WILLIAMS: Objection to form.

24 A. No. The communication protocols between
25 terminal and card were common, in that all of the card

1 schemes adopted the same communications protocol.

2 The things that differed were the
3 application messages that flew across that
4 communications protocol.

5 Q. Okay, maybe I was using the word "protocol"
6 incorrectly there. Let me ask my question again.

7 A person of skill in the art would have
8 been aware of different specifications that have
9 different information flowing between the card and the
10 terminal; is that right?

11 A. That's correct. So the different card
12 schemes implemented contactless in different ways,
13 partly for the magstripe situation that I described,
14 but also for EMV-based contactless transactions as
15 well.

16 And on the terminal side those
17 specifications are defined and referenced in the EMVCo
18 contactless specifications, which are Exhibits 1023
19 through 1029, and in particular the Book C kernels.

20 Q. Would the different payment specifications
21 have also included different information sent between
22 the card and the issuer?

23 MR. WILLIAMS: Objection to form and
24 scope.

25 A. The individual payment brands -- Visa,

1 MasterCard, et cetera -- have their own specifications
2 for the information that flows between their acquirers
3 and their issuers. And so in that context the answer
4 is yes.

5 In terms of the information flowing
6 between the contactless card and the contactless
7 reader, there are a number of data items which are
8 common to all of the specifications, because those are
9 EMV data items. But there are a range of data items
10 where the individual card schemes may choose to use
11 the same tag for different information.

12 So tags 9F01 through 9F7F are owned by
13 EMVCo, and all of the card schemes represent the same
14 data using those tags. But from 9F50 upwards the
15 meaning of those tags is determined by the individual
16 card schemes.

17 So a 9F50 for Amex may represent a
18 completely different thing to a 9F50 for MasterCard,
19 et cetera.

20 Q. You said that the information flowing between
21 the contactless card and the contactless reader
22 includes some common data items because those are EMV
23 data items. Can you explain why in a contactless
24 payment system in the United States at that time that
25 is not compliant with EMV why the data items would be

1 the same and why you called them EMV data items?

2 A. So the communication between the cards and
3 the contactless terminals for all the card schemes
4 were based on EMV specifications, EMV logic. The
5 messaging between the terminal and the acquirer and on
6 through the network to the issuer were determined by
7 the capabilities of those networks to carry the EMV
8 data. And in the U.S. at that time the majority of
9 the networks were not able to carry that data because
10 the U.S. at that time was still a predominantly
11 magstripe acquiring market. It hadn't yet migrated to
12 EMV.

13 So although EMV data items were flowing
14 between the card and the terminal, when the message
15 left the terminal, the EMV data items either had to be
16 discarded or transformed in some way to fit within the
17 space available in the messaging between the terminal,
18 the acquirer, and the issuer.

19 Q. So which data items would have been discarded
20 or transformed to fill the available space between the
21 terminal and the acquirer and the issuer?

22 A. There are a number of those data items, and
23 which ones were discarded or transformed and the
24 method of transformation differed from specification
25 to specification, from card scheme to card scheme.

1 Q. Did each of the contactless specifications
2 available in 2012 use cryptograms?

3 A. Sorry, someone's just entered the room.

4 MR. WILLIAMS: It's lunch. If you want to
5 keep going, that's fine.

6 A. Could you repeat the question? Sorry, Seth.

7 Q. Do each of the contactless payment systems
8 that a person of skill in the art would have been
9 aware of in 2012 use cryptograms?

10 A. Yes.

11 Q. And were the cryptograms used throughout the
12 entire system, or would those be a piece of
13 information that's discarded potentially?

14 A. So in the case of a magstripe acquiring
15 market, like the U.S. at that time, there is no room
16 in the messages that fly through the terminal -- there
17 is no room in the messages that fly from the terminal
18 through the acquirer and payment network to the issuer
19 to carry the full value of the cryptogram and to carry
20 the full value of the application transaction counter,
21 the ATC.

22 So the card schemes transformed the
23 cryptogram and the ATC into a smaller number of digits
24 that could be carried in the space available. The
25 card schemes did that in different ways.

1 Q. Did each of the card schemes or contactless
2 payment systems available in 2012 calculate
3 cryptograms in the same way?

4 MR. WILLIAMS: Objection, form.

5 A. Each of the card schemes had a specification
6 which described how the cryptograms were to be
7 calculated. In all cases the cryptograms were
8 calculated using the same algorithm and using the same
9 type of cryptographic key, but they varied in the
10 amount of input data that was used to generate the
11 cryptogram.

12 Q. All right, I'd like to direct you to Exhibit
13 1026.

14 A. C-2: Kernel?

15 Q. Yes.

16 A. Okay.

17 Q. And I'll ask you to go to Page 28.

18 A. This is the page that starts with heading
19 1.5.4 Terminal?

20 Q. That's right.

21 A. Okay.

22 Q. In Section 1.5.7, titled Magstripe Mode, what
23 is this referring to when it discloses the magnetic
24 stripe infrastructure?

25 A. So the magnetic stripe infrastructure is the

1 capability of the terminals to transmit the data that
2 you would normally see on the physical magstripe on
3 the back of a payment card through to the acquirer,
4 the network, and the issuer. This mode allows them to
5 conduct a contactless transaction and transfer
6 information in the same container, the same message.

7 So magstripe mode here is what you would
8 use in the U.S. because it isn't an EMV-acquiring
9 infrastructure yet, whereas in 1.5.6, EMV mode, that's
10 what we would use in Europe.

11 Q. So does this mean that a card could be used
12 for contactless payment that is compliant with the EMV
13 4.2 standard that utilizes magstripe mode instead of
14 EMV mode?

15 MR. WILLIAMS: Objection to form.

16 A. So I think I need to take a step back and
17 just clarify the background of these specifications.

18 EMV gives you the ability to have global
19 interoperability, so any bank card in any EMV terminal
20 in the world will be able to conduct a transaction.
21 EMVCo achieves that by providing specifications for
22 terminals. The EMV 4.2 specifications referenced here
23 are actually about what happens when you insert a
24 payment card into a slot in a payment terminal. So
25 these are contact transactions. The EMV contactless

1 transactions from 1023 through 1029 are what happens
2 when you wave an EMV-capable contactless card at a
3 contactless terminal.

4 In both cases, for contact and for
5 contactless, the internal processing of the chip
6 application are not defined -- with one exception,
7 which I'll come to -- they're not defined by the EMVCo
8 specifications. They're actually defined by the
9 specifications provided by the individual payment
10 schemes.

11 So, to take an example, a MasterCard card
12 would comply with MasterCard specifications but would
13 be able to interoperate globally with an EMV terminal.
14 And similarly, a Visa card would comply to Visa
15 specifications but be able to interoperate with an EMV
16 kernel.

17 So this specification, Kernel 2 spec, is
18 about what goes on in a contactless terminal when it
19 needs to deal with a Kernel 2 card, which is a
20 MasterCard.

21 Q. So, then, going back to my question: The EMV
22 specification 4.2 supports transactions that operate
23 in magstripe mode; right?

24 A. No. The EMV 4.2 specifications are about
25 what happens over the contact interface, and magstripe

1 mode in the context of the document you pointed me to
2 here are what happens over the contactless interface.

3 Q. I'm sorry, that's -- I must be missing
4 something here. That's confusing, because we're
5 looking at a document that's part of EMV 4.2; right?

6 A. No. This document that you pointed me to is
7 EMV contactless Book C-2, and it's Kernel 2 specs,
8 Version 2.1. So EMV publishes contactless
9 publications, which it calls Books 1, 2, 3, 4, and it
10 publishes contactless specifications, which it calls
11 Books A, B, C, D -- actually and now E, but back then
12 it was A, B, C, D. And within the C range, there's
13 C-1, C-2, C-3, C-4, which are the contactless
14 definitions for the individual card schemes, because
15 in contactless the card schemes chose to do things
16 differently, whereas in contact they elected to all do
17 the same thing.

18 Q. Okay, thank you for that clarification. I
19 think I was using EMV 4.2 as a proxy for both of the
20 sets of specifications that were submitted as those
21 exhibits. Let me ask my question again, hopefully a
22 bit more precisely this time.

23 The EMV contactless specifications
24 supported transactions in magstripe mode?

25 A. Correct.

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

5 A. Correct.

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

8 Could I direct you to Exhibit 1020.

9 A. This is EMV 4.2, Book 2?

10 Q. Yes.

11 A. Security and Key Management, yes.

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

14 A. Application Cryptogram and Issuer
15 Authentication.

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

20 A. Yes.

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

25 A. Yes.

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

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

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

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

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

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

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

4 (Recess for lunch.)

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

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

10 A. Okay.

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

12 A. Yes.

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

15 A. Yes.

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

20 A. Yep.

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

25 A. Yes.

1 Q. I would like to now direct you to your
2 analysis of the Collinge reference. We can put the
3 EMV specs away for the moment.

4 A. Okay.

5 Q. So you have offered your opinions that the
6 challenged claims of Collinge -- or, sorry, let me say
7 that again.

8 You've offered your opinion that the
9 challenged claims of the '171 patent are both
10 anticipated and rendered obvious. Right?

11 A. Yes.

12 Q. Have you endeavored to determine which claims
13 are anticipated, which are obvious, based on Collinge?

14 MR. WILLIAMS: Objection to form.

15 A. I don't think I identified any claims which I
16 felt were not both anticipated and obvious.

17 Q. So is it your opinion, then, that all of the
18 challenged claims are anticipated by Collinge?

19 A. I think it's my opinion that all of the
20 challenged claims are anticipated or obvious.

21 Q. My question is: Is it your opinion that all
22 of the challenged claims are anticipated by Collinge?

23 A. I think I would need to go through each of
24 them in turn, because I was looking for --

25 I was kind of doing it the other way

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

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

7 A. Yes, anticipated or obvious.

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

10 A. Okay.

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

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

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

1 other times the nexus linking two or more prior art
2 references may be the background knowledge of one of
3 ordinary skill in the art or simple common sense." Do
4 you see that?

5 A. Yes.

6 Q. So when you analyzed Collinge, is it fair to
7 say that you looked at Collinge and the EMV
8 specifications as you've defined them as separate
9 prior art references and that you determined that they
10 would be -- there would be a motivation to combine
11 them?

12 MR. WILLIAMS: Objection to form, scope.

13 A. Collinge references the EMV specifications,
14 and a person of skill in the art would understand
15 Collinge because they understand the EMV
16 specifications.

17 I'm a bit unclear as to your question
18 about combining the two, because if Collinge
19 references EMV, then in my mind Collinge still stands
20 on its own. But I may be wrong.

21 Q. So were there instances where the Collinge
22 disclosure was in some way incomplete as to a
23 particular limitation and you determined that that
24 limitation would have been obvious because whatever
25 incompleteness was there would have been filled in by

1 disclosures within the EMV specifications?

2 MR. WILLIAMS: Objection to form.

3 A. When I analyzed Collinge, there was one part
4 of it which I frankly didn't understand, to do with
5 the data item that he called UNCLOUD. It wasn't clear
6 to me from reading Collinge what the purpose of
7 UNCLOUD was, or indeed how it was used.

8 But there is a provisional application,
9 which goes into a lot more detail and explains the
10 purpose of UNCLOUD, to the point where I was able to
11 understand what Collinge was about. And my
12 understanding from counsel is that provisional
13 application can be counted as part of the Collinge
14 patent.

15 Q. Okay, I'd like to direct you to Page 53 of
16 your declaration. It contains Paragraph 88. Are you
17 there?

18 A. Yep.

19 Q. So on Page 53 you have an annotated figure,
20 which you note is Figure 7 from Collinge; right?

21 A. Yes.

22 Q. All right. So there's a red box in that
23 figure. Is that an annotation that you added?

24 A. I don't remember it being in the actual
25 Collinge patent. Can I just check?

1 Q. Sure.

2 A. Okay, so the boxes aren't present, so I must
3 have added them.

4 Q. And what is the significance of the red box
5 that you added?

6 A. It highlights the communications channel
7 between the mobile device and the merchant's payment
8 reader.

9 Q. And the blue box?

10 A. Highlights the communications channel between
11 the mobile device and Collinge's provisioning system.

12 Q. And the orange box?

13 A. Is highlighting that the interaction between
14 the mobile device and the provisioning system is
15 initiated by a request from the mobile device to the
16 provisioning system.

17 Q. So within Figure 7 could you identify what
18 you understand would be the claimed mobile device?

19 MR. WILLIAMS: Objection to form.

20 A. It's the box that's labeled Mobile Payment
21 Application and includes the mobile device with a
22 picture of a smartphone.

23 Q. And could you identify what would be the
24 claimed electronic reader in Figure 7?

25 A. It's in the box that's labeled 306. It's

1 the, I call it, it looks like a payment reader, just
2 above the word "merchant."

3 Q. So just for clarity, you're referring to the
4 box that has the payment reader graphic above the word
5 "merchant," and it also sort of includes within the
6 top of that box a little drawing of a shopping cart?

7 A. Yep. But to answer your question
8 specifically, the device that communicates with the
9 mobile device is not the whole of that. It is the
10 device, the icon just above "merchant."

11 Q. What is in Figure 7 the claimed first
12 communication channel?

13 MR. WILLIAMS: Objection to form.

14 A. It's the box highlighted in blue.

15 Actually, let me just double-check that.

16 Could you give me a reference to the
17 phrase "first communication channel"?

18 Q. "First communication channel" is a limitation
19 recited in 1.A-2 as the claims are numbered in the
20 petition and in your declaration.

21 A. Okay, right. So I misspoke. The first
22 communication channel referred to in 1.A-2 is the
23 channel between the mobile device and the merchant
24 POS. And so it's the one that's highlighted in red.

25 Q. Can a wireless network have more than one

1 channel?

2 MR. WILLIAMS: Objection to form and
3 scope.

4 A. Again, the word "channel" is a very broad
5 term. But yes, a wireless network can have different
6 channels.

7 Q. So in Paragraph 87 of your declaration, on
8 the second page of that paragraph, which is Page 43,
9 you say, "Further, as shown in Collinge Figure 7, the
10 communication between the remote/cloud system to the
11 phone is a different (second) communication channel
12 (e.g., SSL/TLS) from the channel used to communicate
13 with the POS reader/merchant (first communication
14 channel, shown by the near-field communication
15 symbols)." Do you see that?

16 A. Yes.

17 Q. So you're saying here that SSL/TLS are
18 examples of a different communication channel from the
19 channel that's used with the POS reader/merchant; is
20 that right?

21 A. So the channel that is used between the
22 mobile device and the merchant's POS is a contactless
23 technology. The channel that's used between the
24 mobile device and the provisioning system would be a
25 different technology, which could, for example, be

1 over the Internet, in which case, if it was secured,
2 you would see secure socket layer, SSL, or transport
3 layer security, TLS. But it's essentially running
4 over an IP network, and that IP network could be wifi
5 or it could be a mobile data network.

6 Q. After the sentence that I just read, you have
7 a citation to Paragraph 43 of Collinge, and you
8 include in parentheses "regarding dual channel
9 communication between the mobile device and remote
10 system." Do you see that?

11 A. Yes.

12 Q. So how is Collinge's disclosure in Paragraph
13 43 regarding the dual-channel communication relevant
14 to your opinion that the connection between the remote
15 cloud system to the phone is different -- or a
16 different channel from the channel used to communicate
17 with the POS?

18 A. So at the end of 43 there's a sentence which
19 says, "The mobile device may communicate using
20 dual-channel communication, discussed in more detail
21 below." But at this instant I can't find that more
22 detail below. Do you have a reference to it?

23 Q. Well, I'm just asking -- you cited this
24 paragraph, so I'm just trying to understand how this
25 paragraph supported your opinion about the channels

1 that we've been discussing.

2 A. I'm not sure how to articulate my answer to
3 this, other than to say that the provisioning system,
4 which we're talking about here, is sending information
5 to the mobile device, and there is no mechanism to do
6 that over the NFC channel between a point-of-sale
7 terminal and the mobile device. And indeed, you
8 wouldn't need that because the mobile device has its
9 own network connections, which will allow it to
10 communicate with the provisioning system.

11 So on that basis, I think this shows that
12 the communication channel to the provisioning system
13 is different to the communication channel between the
14 mobile device and the merchant POS. But I'm still
15 unclear about this term "dual-channel communication."

16 Q. I also wanted to point you to your citation
17 to Paragraph 58, where, on Page 43 of your
18 declaration, you have the parentheses "dual-channel
19 communication" as part of your citation there. Do you
20 see that?

21 A. Yes.

22 Q. So I guess I would ask the same question as
23 to Paragraph 58: How does the disclosure there of
24 dual-channel communication relate to your opinion as
25 to the first communication channel between the mobile

1 device and the POS and what you've described as a
2 second communication channel between the mobile device
3 and the payment system?

4 MR. WILLIAMS: Objection to form.

5 A. So one communication channel is clearly the
6 connection between the mobile device and the merchant
7 POS, and that is clearly separate and different from
8 the second communication channel, which is between the
9 mobile device and the provisioning system.

10 What Paragraph 58 illustrates is that over
11 that second communication channel you can in fact have
12 two different mechanisms for transferring information.
13 One is called -- where's the actual term? This is
14 Paragraph 59. One is called remote notification,
15 which is the mechanism whereby the provisioning system
16 can send a message unsolicited to the mobile device.
17 And the other alternative is a mutually authenticated
18 channel, where the mobile device places a request to
19 the provisioning system.

20 So "dual-channel communication" is
21 actually talking about two different ways of
22 communicating over that second channel, which is the
23 IP network.

24 Q. Looking back to Figure 7: Could you identify
25 which component would be the remote computer system

1 that you're relying on for claim 1?

2 MR. WILLIAMS: Objection to form.

3 Q. And if it's helpful, the remote computer
4 system is first recited in limitation 1.A-3.

5 A. Do you have a page number for that? Hold on.
6 I think I'm there. 1.A.1. 1.A.1 refers to a mobile
7 device executing an application in the operating
8 system of the mobile device. Is that what you meant?

9 Q. Sorry, you may have misheard me. Let me just
10 state my question again. If we look at Page 42 of
11 your declaration -- sorry, Page 51, Paragraph 87.

12 A. Right.

13 Q. And do you see that in the second-to-last
14 line on Page 51 you say, "Further, the mobile payment
15 application 106 may transmit the generated CAP token
16 to the remote-SE system 100"?

17 A. Right.

18 Q. And a few lines up from there, somewhere
19 around halfway down Paragraph 87, you also quote
20 Collinge, and you say, "The method 500 may return to
21 step 510, where connection may be made with the remote
22 system 110 and a new single-use key 118 provisioned to
23 the mobile device 104"?

24 A. Yep.

25 Q. So for clarity, I wanted to make sure I'm

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

4 A. I think that's a typo. I'm looking in Figure
5 7 in Collinge. I don't see, unless I've missed it,
6 anything labeled 100. But I do see the cloud system,
7 the remote system, being labeled as 110.

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

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

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

18 MR. WILLIAMS: Objection to form.

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

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

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

5 A. Correct.

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

9 A. Yes.

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

17 A. Yes.

18 Q. Is KSUN an unpredictable number?

19 MR. WILLIAMS: Objection to the form and
20 scope.

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

1 Q. So let me point you to Paragraph 9 of
2 Collinge, on Page 21. Do you see about halfway down
3 the phrase that says "generating by a processing
4 device a session key unpredictable number (KSUN)"?

5 A. Yes.

6 Q. So is it your opinion that a person of skill
7 in the art reading that description of a session key
8 unpredictable number would not understand that KSUN is
9 an unpredictable number?

10 MR. WILLIAMS: Objection to form.

11 A. The term "session key unpredictable number,"
12 which they've labeled as KSUN, is a confusing term. I
13 would agree with you there.

14 If you look at how KSUN is calculated, it
15 is clear that it's calculated in the way that EMV
16 describes key derivation. It is a session key, but I
17 believe the reason that they've labeled it as a
18 session key unpredictable number is because in the key
19 derivation data you not only have the application
20 transaction counter, which is the thing that makes it
21 a session key, but you also have an unpredictable
22 number, which is UNCLOUD.

23 So if you look at how the session key is
24 generated, it's generated using both the transaction
25 counter and the unpredictable number, UNCLOUD, which

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

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

11 A. Correct.

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

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

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

21 A. Okay.

22 Q. That might --

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

25 So as with EMV, you start with an issuer

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

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

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

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

18 Q. And is there a place in Collinge, Exhibit
19 1011, where you could point me to that shows this
20 derivation of the session key that you just described?

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

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

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

4 MR. WILLIAMS: Objection to form.

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

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

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

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

17 MR. WILLIAMS: Objection to form.

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

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

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

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

1 transaction counter and a generating key 208"?

2 A. Yes.

3 Q. So what does that tell you about how --

4 A. Well, that maps -- to me that maps onto the
5 EMV mechanism, which says that once you've got the
6 card key you can generate a session key by using the
7 ATC and its key derivation data.

8 Q. So you're interpreting this, when it says
9 that "the single-use key may include an application
10 transaction counter and a generating key" to mean that
11 the application transaction counter and the generating
12 key are what's used to create the single-use key?

13 A. Correct.

14 Q. And that's in your opinion how a person of
15 skill in the art would understand that the single-use
16 key includes the ATC and the generating key?

17 A. Because a person of skill in the art would be
18 conversant with the EMV specs and the session key
19 derivation therein, I think yes.

20 Q. So is it your opinion, then, that when a key
21 is used to generate another key -- so, in this
22 example, the generating key being used to generate a
23 single-use key -- a person of skill would understand
24 that it's appropriate in that context to say that the
25 single-use key includes the generating key?

1 MR. WILLIAMS: Objection to form.

2 A. Given that a person of skill in the art would
3 understand how EMV suggests that you generate single-
4 use or session keys, I think the answer to that is
5 yes.

6 Q. Would a person of skill in the art be able to
7 determine the PAN from the KSUN value?

8 A. No.

9 Q. Would a person of skill in the art be able to
10 determine any of the account information using the
11 KSUN value?

12 MR. WILLIAMS: Objection to form.

13 A. No.

14 Q. In the same paragraph we were looking at,
15 Paragraph 96 of your declaration, you describe that
16 "KSUN is a non-permanent cryptographic key associated
17 with the account," and you say that "KSUN is
18 transmitted to the mobile device as part of an
19 encrypted payload." Do you see that?

20 A. Yes.

21 Q. What is the encrypted payload in Collinge?

22 A. It's the data that flows from the provision
23 system to the mobile device over the wireless network.

24 Q. And what data is included in the encrypted
25 payroll?

1 A. Well, certainly the KSUN. And in the
2 early -- in the early part of the life cycle it would
3 be the other digital credential data, including the
4 PAN and the PAN sequence number and so on.

5 And with each KSUN you would also include
6 the ATC appropriate to that KSUN.

7 In fact, at the bottom of 96 it includes
8 Cloud_CVC3TRACK1/2 as well?

9 Q. So that portion you just pointed to there
10 came from the Collinge provisional; right?

11 A. Yes.

12 Q. So was that disclosure in the Collinge
13 provisional that you pointed to regarding what's part
14 of the encrypted payload -- was that carried forward
15 into Collinge, or is it just in the Collinge
16 provisional?

17 MR. WILLIAMS: Objection to form.

18 A. The closest I can find in Collinge is
19 paragraph 83.

20 Q. So does something in paragraph 83 show that
21 the Cloud_CVC3TRACK1/2 data is part of the encrypted
22 payload?

23 MR. WILLIAMS: Objection to form.

24 A. So paragraph 83 says "There is at least one
25 CVC3 key, the KSUN, and the application transaction

1 counter that may be generated using a derived CVC3
2 key." But the actual details of how those data items
3 are used is in the provisional.

4 MR. LINDNER: Can we take a short break?

5 MR. WILLIAMS: Sure. Off the record.

6 (Recess taken.)

7 MR. LINDNER: Back on the record.

8 Q. In Paragraph 94 of your declaration, at the
9 end of that paragraph you say that, "KSUN is
10 associated with the account because it is generated in
11 response to an account-specific request and uses the
12 account-specific ATC in its generation." Do you see
13 that?

14 A. Yep.

15 Q. So can you explain what you mean by it being
16 generated in response to an account-specific request?

17 A. So a mobile device that wants a new KSUN will
18 in this description request that and will need to
19 identify which account it's requesting the KSUN for.
20 So that would be the account-specific request.

21 Q. So you're saying that if information is
22 requested by the mobile application as part of
23 communications that involve a particular account, that
24 information would be considered associated with the
25 account?

1 MR. WILLIAMS: Objection to form and
2 scope.

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

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

11 A. Sorry, could you ask the question again?

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

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

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

24 MR. WILLIAMS: Objection to form and
25 scope.

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

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

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

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

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

20 MR. WILLIAMS: Objection to form and
21 scope.

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

1 receive a timestamp.

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

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

11 So I think that's my answer.

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

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

22 A. It's associated --

23 MR. WILLIAMS: Objection to form.

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

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

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

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

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

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

21 Q. Thank you.

22 A. You're welcome.

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

25 A. Yes, I see that.

1 Q. And you're okay if I refer to that as APDU?

2 A. Yes.

3 Q. Does Collinge specify that responses from the
4 application are formulated as APDUs?

5 A. Inasmuch as all communications between
6 contactless cards and payment terminals are
7 encapsulated in ISO 7816 APDUs, a person of skill in
8 the art would understand that. But you asked if
9 Collinge explicitly uses the term "APDU," which I
10 would need to search through the document to check.

11 Q. So in Paragraph 106 you say, "As explained in
12 1.E and 1.E-1, the card (or device) being interrogated
13 would respond to a command APDU from the POS terminal
14 with response APDU." Do you see that?

15 A. That's correct, yes.

16 Q. So if we look back at Paragraph 95, you again
17 discuss the APDUs, and you say there, "It is well
18 known in the art that during the interrogation
19 commands issued by the terminal and responses from the
20 'Card' are communicated in command- and response-
21 application protocol data units." Right?

22 A. Correct.

23 Q. And then you said that "It would be obvious
24 to implement Collinge in this way to ensure
25 interoperability with EMV-standardized devices."

1 Right?

2 A. Right.

3 Q. So you have put in Paragraph 95 the word
4 "Card" in quotes with a capital C. Is that something
5 that came from Collinge?

6 A. That may have been something that I
7 introduced. The -- because we started with physical
8 cards, the device that's the payment credential is
9 usually referred to as a card, even if it's not. So
10 in the case of a mobile device, the phone acting as
11 the payment credential, you might still refer to it as
12 a card instead of a mobile device. The double quotes
13 is probably an intent to indicate that it may not just
14 be a physical card.

15 Q. And the capitalization there, is that what
16 Collinge does with the word "card" whenever it's used?

17 A. I don't know. Probably not. It's not what I
18 would normally do.

19 Collinge in paragraph 38 has a definition
20 of terms as a payment card. "Payment Card" is
21 capitalized. But then the explanation says "a card or
22 data associated with a payment account," and "card"
23 there is in lower case.

24 Q. So you're referring to the heading of
25 paragraph 38 that says capital-P Payment, capital-C

1 Card, similar to Paragraph 37, which says Capital-P
2 Payment, Capital-A Account. Right?

3 And this Paragraph 95 of your declaration
4 you do not cite to any disclosure in Collinge; right?

5 A. Right.

6 Q. So instead you're citing to Exhibit 1037 and
7 1021 at the end of Paragraph 95.

8 A. The 1021 is the EMV Book 3 application
9 specification. And 1037 is a document which talks in
10 general terms about implementing card payment systems.

11 Q. So your contention here in Paragraph 95 is
12 that communicating using APDUs would have been
13 obvious -- would have been an obvious way to implement
14 Collinge to ensure interoperability with
15 EMV-standardized devices. Right?

16 A. Correct.

17 Q. So put in a different way, a person of skill
18 in the art reading Collinge would have looked to the
19 EMV disclosures where APDUs are utilized and
20 implemented Collinge in a way that also used APDUs.

21 A. That's right. In fact, APDUs are not an EMV
22 concept. EMV itself uses the concept from an
23 international standard, ISO 7816, which defines how
24 chip card readers interact with chip cards.

25 Q. I'd like to turn you to Paragraph 105 of your

1 declaration.

2 A. Okay.

3 Q. And do you see that the claim limitation
4 above Paragraph 105 recites a device response
5 communication comprising the response cryptogram and
6 an account identifier?

7 A. It says "the at least one device response
8 communication comprising at least one response APDU
9 containing the response cryptogram and an account
10 identifier."

11 Q. So in your analysis of Collinge, what is the
12 response cryptogram?

13 A. The response cryptogram in Collinge is the
14 cryptogram that's generated using the KSUN and synched
15 through the terminal to the issuer.

16 Now, Collinge covers both EMV and
17 magstripe, and in magstripe the cryptogram is further
18 distilled down into the CVC3. So in Collinge, when it
19 describes magstripe mode, the response cryptogram is
20 the CVC3. But when it's describing EMV mode, it is
21 the EMV cryptogram.

22 Q. Okay. So if we look at Collinge, is there a
23 particular wording used for those two different types
24 of cryptogram?

25 A. So in Collinge, paragraph 7, they describe

1 generating a payment cryptogram valid for a single
2 financial transaction.

3 Q. Okay. My question was actually maybe
4 slightly different. Maybe I didn't word it too
5 precisely there.

6 I'm just trying to understand: You
7 mentioned two different types of cryptogram, and I'm
8 wondering what wording Collinge uses to separately
9 describe each of those. And I would maybe point you
10 to your Paragraph 102, if that is helpful here.

11 A. Okay. So let's have a look at 64. That's
12 not right.

13 Sorry, it's in the provisional again,
14 paragraph 64 of the provisional.

15 Sorry, I'm getting confused between them.
16 Let's go back to Collinge, Exhibit 1011, and let's
17 have a look at paragraph 77. Are you there?

18 Q. Yes. Sorry. I thought you were still
19 answering my question.

20 A. Oh, right. If you look in paragraph 77 of
21 Collinge, about eight lines down it says, "The payment
22 cryptogram may be, for example, an application
23 cryptogram or a dynamic card validation code (CVC3)."
24 So the payment cryptogram being an application
25 cryptogram is what you would get if you were operating

1 in EMV mode, and the dynamic CVC, CVC3, is what you
2 would get if you were operating in magstripe mode.

3 Q. Okay. If I'm understanding you correctly,
4 you're saying that when Collinge references an
5 application cryptogram, a person of skill would
6 understand that to be referring to an EMV mode
7 transaction; and when Collinge uses the term "CVC3," a
8 person of skill would understand that is referring to
9 a magstripe mode transaction. Is that right?

10 A. Correct.

11 Q. Let's go back to where we were, with
12 limitation 1.E-3. And we've discussed what the
13 response cryptogram is. What is the account
14 identifier in Collinge that you're pointing to to
15 satisfy this limitation?

16 A. That would be the PAN.

17 Q. I'd like to direct you to Paragraph 117 of
18 your declaration.

19 A. Okay.

20 Q. So what is the PayPass card specification
21 that you mentioned in Paragraph 117?

22 A. That's the card specification offered by
23 MasterCard to describe how MasterCard contactless chip
24 cards should work.

25 Q. So how does the PayPass card specification

1 relate, if at all, to the EMV specifications?

2 A. The EMV specifications describe processing
3 inside the payment terminal and the commands that the
4 payment terminal may make of the card and the
5 responses that the terminal may expect back from the
6 card.

7 The card specification -- in this case,
8 for MasterCard, the PayPass card specification --
9 defines the other end. So it defines the commands
10 that the card may expect to receive from the terminal,
11 the responses that the card should send back to the
12 terminal, and also it defines the processing that the
13 card application would perform between receiving the
14 command and returning the response.

15 Q. So you have at the bottom of Paragraph 17,
16 you say that Collinge refers to M/ChIp payment
17 transactions, and you cite to paragraph 44 of
18 Collinge. Could you show me where in paragraph 44
19 Collinge makes reference to M/ChIp payment
20 transactions?

21 A. So I don't see it in 44. I've read around to
22 see if 44 is a typo, which I suspect it is. But I
23 haven't found a reference to M/ChIp or the term
24 "M/ChIp payment transaction."

25 Q. So a person of skill in the art --

1 A. Sorry, I was going to say: Which is not to
2 say it's not there; I just can't find it at this
3 instant.

4 Q. So if we look at Paragraph 117, you're
5 pointing to the PayPass card specification, which you
6 identify as coming from the Collinge provisional,
7 Exhibit 1009, and then the M/ChIp payment transactions
8 coming from Exhibit 1011, which is Collinge itself.

9 Are those two things different, PayPass
10 and M/ChIp?

11 MR. WILLIAMS: Objection to form.

12 A. So "PayPass" is the term for MasterCard
13 contactless, and PayPass comes in two forms. It comes
14 in PayPass Magstripe and PayPass M/ChIp. And PayPass
15 Magstripe is the full EMV formulation. PayPass
16 Magstripe is the magnetic stripe.

17 But I am confused about this reference.

18 Q. So just for clarity, you're saying that the
19 term "PayPass" would be understood to refer to the
20 magstripe implementation, and "M/ChIp" would be
21 understood as referring to the EMV formulation?

22 A. No. "PayPass" is the term to identify
23 MasterCard contactless. Then you have "PayPass
24 Magstripe," which is the magstripe formulation, and
25 "PayPass M/ChIp," which is the EMV formulation.

1 Q. So claim 4 recites "wherein the interrogation
2 conforms to a card specification, the set of inputs as
3 specified by the card specification and the at least
4 one device response is formulated according to the
5 card specification."

6 So what you've said here in Paragraphs 117
7 and 118 indicates that a person of skill would
8 understand that Collinge's reference to M/ChIp and
9 PayPass, which were known payment systems, and that it
10 would have been obvious for the Collinge system to
11 comply with these known specifications to expand their
12 market opportunity by allowing interoperability with
13 existing and expected future payment infrastructure.
14 Did I get that right?

15 A. That's right.

16 Q. So when you analyzed Collinge with respect to
17 claim 4, did you look at each of the interrogation
18 steps described in Collinge to see if those match the
19 card specification, or were you simply opining here
20 that it would have been obvious if not disclosed in
21 Collinge to make the payment process in Collinge
22 compliant with the specifications?

23 MR. WILLIAMS: Objection to form.

24 A. That question kind of went on a bit.

25 Q. Let me try again.

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

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

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

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

19 A. One three two?

20 Q. Yep, 132.

21 A. Okay.

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

25 The first sentence in Paragraph 132 looks

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

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

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

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

25 Q. So in looking at what you had in Paragraph

1 132, there's a couple of terms that you mentioned in
2 your answer that I'm not seeing there. So I'm curious
3 as to where we would find that disclosure. For
4 example, I don't see in Paragraph 132 any mention of
5 the issuer master key.

6 A. But you do see that the issuer process server
7 has to determine the KSUN, and we know that in
8 determining the KSUN you need to start from the issuer
9 master key.

10 Q. So is that coming from Collinge that we know
11 that, or is that coming from the provisional 1009 --

12 A. That's described in more detail in the
13 provisional.

14 Q. Is it described in Collinge at all?

15 MR. WILLIAMS: Objection to form.

16 A. Well, it's certainly not described in the
17 same detail. Again, I would need to read through
18 Collinge to see where it is mentioned.

19 Q. Okay. So I see that you've cited here to
20 paragraph 87 of Collinge, and I don't see any
21 additional cites to Collinge in Paragraph 132. So is
22 paragraph 87 the place we should look in Collinge to
23 see these disclosures?

24 MR. WILLIAMS: Objection to form.

25 A. So in 87 it does describe the process of

1 validating the cryptogram -- or the CVC3, rather. But
2 it doesn't explicitly describe how the KSUN is
3 derived.

4 Q. So Collinge doesn't describe that the issuer
5 master key is used in this.

6 A. Not at that point.

7 Q. And also, Collinge also doesn't describe that
8 the PAN and the PAN sequence number are used to derive
9 the session key from the unpredictable number; right?

10 MR. WILLIAMS: Objection to form.

11 A. The PAN and the PAN sequence number are used
12 to derive the permanent cryptographic key from the
13 issuer master key. In Collinge the transaction
14 counter and the cloud unpredictable number are used to
15 derive the session key, KSUN. And that is used with
16 the reader unpredictable number to generate the CVC3.

17 Q. Okay. Let me make sure I'm understanding
18 your answer. Are you pointing to a disclosure in
19 Collinge that shows that the PAN and the PAN sequence
20 number are used to derive the permanent cryptographic
21 key from the issuer master key?

22 A. I'm pretty sure that's disclosed in the
23 provisional. Let me take a look.

24 Q. It looks like in Paragraph 132 you're citing
25 to paragraph 61 of the Collinge provisional, Exhibit

1 1009. Is that where we would see this description of
2 the PAN and the PAN sequence number?

3 A. You actually see it in paragraph 68. Let's
4 have a look at 61 and see if it's there.

5 It's not in paragraph 61; it's in
6 paragraph 68.

7 Sorry, paragraph 71.

8 Q. So what are we looking at specifically there?

9 A. So the derivation from the issuer master key
10 to the permanent cryptographic key is described in
11 1009, which is the provisional, and its description
12 starts at paragraph 69. And the actual calculation is
13 in paragraph 71.

14 Q. So paragraph 71 of the Collinge provisional,
15 Exhibit 1009, shows how the PAN and the PAN sequence
16 number are used to derive the permanent cryptographic
17 key from the issuer master key?

18 A. Yeah, the description of using the PAN and
19 the PAN sequence number starts at paragraph 69, but
20 the actual generation is in 71.

21 Q. So can you point me to where the actual
22 generation uses the PAN and the PAN sequence number?

23 A. Okay. So in 69 we start the process by
24 concatenating the PAN with the PAN sequence number.
25 And in 70, if the result is less than 16 digits, we

1 pad to the left with 0's.

2 In 71, if it's at least 16 digits long,
3 then we take the rightmost 16 digits and we encrypt
4 with the issuer master key, which is third line from
5 the bottom, which gets us the left-hand half of the
6 permanent cryptographic key.

7 Then we perform another triple DES
8 operation to get the right-hand half, and we put them
9 together to end up with the permanent cryptographic
10 key.

11 Q. And what's the nomenclature for the permanent
12 cryptographic key?

13 A. KD CVC3.

14 Q. And so you're saying that IMK CVC3 in
15 paragraph 71 of the Collinge provisional is the issuer
16 master key?

17 A. Correct.

18 Q. And this disclosure in the Collinge
19 provisional of how the PAN and the PAN sequence number
20 are used to derive the permanent cryptographic key
21 from the issuer master key is not carried forward into
22 Collinge itself; right?

23 MR. WILLIAMS: Objection to form.

24 A. I wasn't able to find it.

25 Q. And you also said in your previous answer

1 that in Collinge the transaction counter and the cloud
2 unpredictable number are used to derive the session
3 key KSUN.

4 A. That's correct.

5 Q. Is that a disclosure that's in Collinge, or
6 are we again looking at the provisional?

7 A. Again we're looking at the provisional, and
8 we are still in paragraph 71, but we are two pages on,
9 on page 28, which is actually labeled page 22.

10 Q. Okay. So that disclosure of using the
11 transaction counter and the cloud unpredictable number
12 to derive the session key KSUN is in the Collinge
13 provisional but not carried forward into Collinge;
14 right?

15 MR. WILLIAMS: Objection to form.

16 A. I didn't see it.

17 Q. In Paragraph 132 you say in the last sentence
18 that verifying would involve comparing whether the two
19 CVC3 values are the same. Correct? Does Collinge
20 disclose this comparison?

21 A. It mentions validating the generated CVC3,
22 but I haven't yet found an explicit mention of
23 comparing the CVC3 that it receives against the CVC3
24 that it calculates.

25 In paragraph 45 of Collinge it describes a

1 payment network submitting an authorization response
2 to the acquirer and/or merchant. It finishes with
3 "methods and systems suitable for the processing of
4 financial transactions will be apparent to persons of
5 skill in the relevant art." But I can't see anything
6 that explicitly talks about comparison.

7 Q. In Paragraph 133 you then say that a person
8 of skill in the art "would find it obvious to
9 implement Collinge in the manner described above
10 because these are standardized operations in secure
11 payment transactions and are therefore applying a
12 known technique to yield predictable results."

13 A. Well, that is certainly true. The generation
14 of a cryptogram by the host and comparing that to the
15 cryptogram generated by the card is the way every EMV
16 transaction is authenticated.

17 Q. So when you describe standardized operations
18 in secure payment transactions, you mean specifically
19 that a person of skill would look to the EMV standard
20 or specifications and see how this operation was done
21 and that it would be obvious to implement Collinge
22 that way?

23 A. Yes.

24 MR. WILLIAMS: Objection to form.

25 THE WITNESS: Sorry.

1 A. Yes.

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

5 A. That comes from the provisional.

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

9 MR. WILLIAMS: Objection to form and
10 scope.

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

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

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

1 hosts to tell the issuer host how to repeat the
2 calculation.

3 MR. LINDNER: I think it's been about an
4 hour since the last break. Do you want to take
5 another short break?

6 THE WITNESS: Okay.

7 MR. LINDNER: Off the record.

8 (Recess taken.)

9 MR. LINDNER: We can go back on the
10 record.

11 Q. Given that you're trying to get out this
12 evening, I'll try to get us onto the home stretch as
13 quickly as I can here.

14 A. That's fine. My flight's not until 10 to
15 11:00 tonight, so I'm okay.

16 Q. All right. I may or not have a happy hour I
17 should be going to myself, so that might motivate me
18 to get through it quicker.

19 I would like to turn your attention now to
20 your analysis of the Fiske reference, Exhibit 1012.
21 If you look at Exhibit 1012, in column 2, beginning at
22 the very bottom, around line 65: Could you review the
23 first few sentences, running over onto the next page,
24 and tell me what "offline data authentication" refers
25 to.

1 A. So what we've been discussing so far with
2 Collinge and cryptograms is what's called online card
3 authentication, where the card generates a cryptogram,
4 which can only be verified or validated by the issuer.
5 So the transaction has to be sent online to the issuer
6 before the issuer can say "This card is genuine" and
7 return that to the terminal and the merchant.

8 There are a couple of circumstances in
9 which online card authentication is not appropriate.
10 So the first one, which is something that was quite
11 prevalent in Europe but is now, with the improvements
12 in networking technology, is now being -- sorry,
13 brain's gone.

14 So there used to be a circumstance in
15 which it made sense for payment terminals to be able
16 to approve transactions themselves without going
17 online to the issuer. And there's a feature in EMV to
18 allow cards to make that decision as well. So if it's
19 a low-value transaction, for example, a few cents or a
20 small number of dollars, if the card and the terminal
21 agree that the transaction should be approved, then
22 the transaction will be approved and there is no need
23 to go online to the issuer to check whether the
24 consumer has enough money or not.

25 So that's called an offline transaction,

1 and it is extremely useful as part of that for the
2 terminal to know that the card is genuine.

3 The second use case is in transit, as we
4 were just discussing before we went back on the
5 record, where it's now possible to wave a contactless
6 card at a payment -- at a transit gate and for the
7 gate to open and for you to get on the subway. There
8 is not enough time for the payment gate to receive
9 your cryptogram, go online to your issuer, get an
10 approval from the issuer. So instead, the payment
11 gate determines that the card is genuine and allows
12 you to ride on the subway on the basis that you have a
13 genuine card.

14 In London, where this happens, and in fact
15 in most cases where this mode is used, while you're
16 actually riding the subway the system will go online
17 to the issuer and find out if you do in fact have
18 enough money. If you do, everything's fine. If you
19 don't, then you'll be allowed out of the transit
20 network, but your card number will be sent to all the
21 transit operator's terminals, and you won't be able to
22 get on again.

23 So those are the two use cases, and as I
24 say, the most important one these days is traveling on
25 transit.

1 How do you prove that the card is genuine?

2 You use a process within EMV called offline data
3 authentication. So as well as the session keys or the
4 permanent cryptographic keys that we've been talking
5 about, it's also possible to place an asymmetric
6 cryptographic key in the payment device, which
7 generates a digital signature, and it is possible for
8 the payment terminals or transit gates to verify that
9 digital signature themselves, without needing to go
10 online.

11 So that's what data authentication is
12 about here. It's about proving that a card is genuine
13 without needing to go online to its issuer. And it is
14 a relatively complex process, which I'm happy to talk
15 you through if you like.

16 Q. So does offline data authentication, as it's
17 described here in Fiske, use cryptographic keys?

18 A. Yes.

19 Q. Does it use cryptograms?

20 A. It uses the cryptographic keys to generate a
21 result, but these are usually termed digital
22 signatures rather than cryptograms.

23 Q. And are those cryptograms ever sent to a
24 system beyond the point of sale?

25 A. No.

1 Q. I'd like to direct you to Paragraph 182 of
2 your declaration. So is it your opinion that the READ
3 RECORD command is what satisfies the limitation that
4 recites at least one POS command communication?

5 A. It goes in part to satisfying it, yes. So I
6 guess if the term is "at least one," then the READ
7 RECORD is a way of satisfying that.

8 Q. You said it goes in part. Is there more to
9 it than that?

10 A. Well, the READ RECORD command will respond
11 with an amount of data. Typically in an EMV
12 transaction you would issue multiple READ RECORD
13 commands, because there is too much data and some of
14 it is too big to actually be sent back in a single
15 response APDU.

16 But you also get data coming back in other
17 commands, traditionally in -- there's data that comes
18 back in the GET PROCESSING OPTIONS command and there's
19 data that comes back in the GENERATE AC command.

20 Q. So is the response to the READ RECORD command
21 a response that includes a response cryptogram and an
22 account identifier in one response APDU?

23 MR. WILLIAMS: Objection to form.

24 A. No. So let's talk about in a bit more
25 detail.

1 The account identifier, we said earlier,
2 would be the PAN, the card number. Now, in some card
3 specifications that card number will be returned in
4 response to a READ RECORD command. Indeed, it can be
5 returned in two places: as part of the Track 2
6 equivalent data and as a PAN in its own right.

7 The cryptogram, the response cryptogram,
8 is not returned in a READ RECORD command. It's
9 returned, depending on the card specification, in
10 either the GET PROCESSING OPTIONS command or in the
11 GENERATE AC command, or indeed, for PayPass Magstripe,
12 it's returned in the COMPUTE CRYPTOGRAPHIC CHECKSUM
13 command.

14 Q. And you say in Paragraph 182 that the mobile
15 device -- this is kind of in the middle of the
16 paragraph -- "the mobile device would return an
17 Application Cryptogram in response to a GENERATE AC
18 command."

19 A. Correct.

20 Q. And you've cited quite a few different
21 portions of Fiske there. Could you point me to which
22 of those shows that the application cryptogram is
23 returned in response to a GENERATE AC command?

24 A. So as an example, if you look in column 7,
25 look at line 35, you can see that the GENERATE AC

1 command is used to request different types of
2 cryptogram, and the cryptogram is returned in response
3 to the GENERATE AC command.

4 Q. So you pointed to column 7, line 35, which in
5 that sentence says, "If the terminal decides to
6 decline transaction offline, the GENERATE AC command
7 requests application authentication cryptogram (AAC)
8 in step 304."

9 A. Right. So that's an example of when the
10 GENERATE AC command is used to generate a cryptogram.
11 The terminal can ask for three different types of
12 cryptogram to be generated. A decline is an AAC. An
13 ARQC, which is at line 38, is a request to go online.
14 And if the terminal and the card are configured that
15 they can approve the transaction without going online,
16 then you have the option of requesting a transaction
17 certificate, a TC, which is at lines 40 and 41.

18 So those paragraphs describe the GENERATE
19 AC command. And then if we read further down column
20 7, we can see that at, for example, line 56, 57, the
21 ICC may decide to respond with an ARQC. So round
22 about lines 55, 56, 57, you have response to the
23 GENERATE AC command being returned with the
24 cryptogram.

25 Q. Does Fiske describe how the ICC session key

1 is generated?

2 A. Yes. If you look in column 8, starting line
3 49; and that runs through to line 63.

4 Q. Is an ICC session key a permanent
5 cryptographic key?

6 A. It's a temporary cryptographic key. It's
7 only valid for one transaction.

8 Q. Is the ICC session key different from a PAN?

9 MR. WILLIAMS: Objection to form.

10 A. PAN is the card number that identifies the
11 account. The ICC session key is the triple DES key
12 that's used to create the cryptogram for that one
13 transaction.

14 Q. Is an ICC an account -- sorry, is an ICC
15 session key an account identifier?

16 MR. WILLIAMS: Objection to form.

17 A. No.

18 Q. In Paragraph 183 -- and I'm looking on Page
19 94 of your declaration, at the top -- you refer to
20 "for the same reasons stated in 1.E-3 above." What
21 are you citing to there?

22 A. So 1.E-3 when I read it was interpretable by
23 me, I think, in two ways. The first way is to say
24 there are at least one and multiple response APDUs.
25 Your account identifier is sent in one of those

1 response APDUs, and the response is sent in a
2 different response APDU. And that's consistent with
3 the PAN being sent as the response to a READ RECORD
4 command and the cryptogram being sent as the response
5 to a GENERATE AC command.

6 The other way that I read it was that
7 there would be a single response APDU, which would
8 contain both the account identifier and the
9 cryptogram. And there is an example in the Visa
10 contactless transactions where the cryptogram and the
11 Track 2 equivalent data are both returned in the
12 response to the GET PROCESSING OPTIONS command.

13 So my conclusion was that, whichever way
14 you read 1.E-3, there is existing examples of how
15 transactions handle that already.

16 Q. Okay. So I'm trying to understand, because
17 you've given a very thorough explanation just now, but
18 in this portion of your declaration I'm not seeing
19 that, and I wanted to make sure I'm looking in the
20 right place -- because you just said "as stated in
21 1.E-3 above," which is that referring to the
22 immediately above Paragraph 182 or something else?

23 A. That's referring to the paragraph in bold at
24 the top of Page 93 and is a quotation from the '171
25 patent.

1 Q. So you are just referring back to the claim
2 language when you are saying "for the same reasons
3 stated in 1.E-3 above"?

4 A. Yes. So what I'm saying is, whichever of the
5 two possible constructions you place on the language
6 in 1.E-3, there are existing examples of how that
7 language is satisfied -- either, in the case of
8 MasterCard, with the account identifier and the
9 cryptogram being present but in different response
10 APDUs; and in the Visa case, where they are present in
11 the same response APDU.

12 Q. All right. And in Paragraph 183 I don't see
13 any citation to a source for your explanation as to
14 how MasterCard or Visa transactions would operate. So
15 where would one find that explanation for evidence?

16 A. You would look at the -- you would look at
17 Kernel 2 and Kernel 3 specifications. That's Exhibits
18 1026 and 1027, where those circumstances would be
19 described.

20 Q. So you're saying that within the EMV
21 specifications there's a description of these
22 differences between a MasterCard and a Visa
23 transaction?

24 A. Correct.

25 Q. And are those --

1 To comply with the EMV specifications,
2 does a payment application need to choose between the
3 MasterCard or Visa transaction, or are there other
4 options as well?

5 MR. WILLIAMS: Objection to form.

6 A. So if you have a Visa card, then when you
7 wave that at an EMV contactless reader, the
8 contactless reader will know, because it knows that
9 you're dealing with an EMV card -- you're dealing with
10 a Visa card, sorry, to run the logic that's described
11 in Kernel 3. If you wave a MasterCard, the terminal
12 knows to apply the logic that's described in Kernel 2.

13 So Kernel 2 is MasterCard, Kernel 3 is
14 Visa, Kernel 4 is American Express. And the
15 contactless terminal interrogates the card to work out
16 which card scheme and then switches to the appropriate
17 kernel to conduct the rest of the transaction.

18 Q. How would a person of skill in the art
19 understand the term "remote payment authorization
20 process," as used in claims 14 and 31 of the '171
21 patent?

22 MR. WILLIAMS: Objection to form.

23 A. In '171?

24 Q. Yes.

25 A. Could you repeat the claims again, please?

1 Q. Claims 14 and 31, and the term I was asking
2 about is "remote payment authorization process."

3 A. Sorry, could you give me a page reference?

4 Q. You can see those terms in the claims which
5 are at the very end of the '171 patent.

6 A. Yeah, so I found the claims. You say 14?

7 Q. Yes, claim 14, and I was asking about the
8 "remote payment authorization process."

9 A. So somebody who is a person of skill in the
10 art would recognize that that would be the
11 authorization system operated by the issuing bank.

12 MR. LINDNER: That's all the questions I
13 have for now. So subject to recross, I'll pass the
14 witness.

15 MR. WILLIAMS: Let's go off the record for
16 five minutes. Let me just see if there's anything.

17 MR. LINDNER: Sounds good.

18 MR. WILLIAMS: Off the record.

19 (Recess taken.)

20 MR. WILLIAMS: We can go on the record.
21 We have no redirect. The witness will read and sign.
22 That's all we have.

23 (The deposition concluded at 4:14 p.m.)
24
25

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.

(Date)

(Signature)

1 CERTIFICATE OF COURT REPORTER
2

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

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

17 My commission expires March 25, 2027.
18
19
20

21 _____
22 Alan H. Brock, RDR, CRR
23
24
25

1 *** ERRATA SHEET ***
 2 CASE: Mastercard Inc. v. OV Loop Inc.
 3 DATE: June 14, 2024
 4 WITNESS: Stuart Fiske, Ph.D.
 5 JOB NO.: 9347

6 PAGE/LINE CHANGE REASON

7 _____
 8 _____
 9 _____
 10 _____
 11 _____
 12 _____
 13 _____
 14 _____
 15 _____
 16 _____
 17 _____
 18 _____
 19 _____

20
 21 _____
 Stuart Fiske, Ph.D.

22 Subscribed and sworn to before me
 23 this ____ day of _____, 20__.

24 _____
 25 Notary Public

A	84:8,10,13 85:16	31:4,9,24 32:3	answers 5:7	116:16
A-M-A-C 36:18	accounts 18:5,20	33:2,17 34:6,10	anticipated 63:10	approval 108:10
a.m 1:16 4:1	19:17,17 20:5,6	34:22 35:1,4,6,11	63:13,16,18,20,22	approve 27:9
A1.3 62:11	23:10 24:4,7,8	35:13,18 36:17,20	64:2,5,7,12,19	107:16 112:15
A1.3.1 62:18	accurate 10:13	37:10,13,17 56:8	anticipates 15:17	approved 107:21
AAC 112:7,12	61:21	84:17	anticipation 16:1,8	107:22
ability 57:18 97:10	achieved 48:13	algorithms 30:12	64:17	approximate 7:17
able 12:2 37:24	achieves 57:21	32:1 33:15 78:24	anybody 85:13	9:2,7
38:10 45:9 54:9	acknowledge 118:4	allow 71:9 86:2	APDU 88:1,9,13,14	approximately
57:20 58:13,15	ACKNOWLED...	107:18	91:8 110:15,22	8:19 12:15
66:10 75:25 77:9	118:1	allowed 108:19	114:2,7 115:11	areas 14:17,18 98:7
77:12,15 81:6,9	acquirer 50:8 54:5	allowing 96:12	APDUs 88:4,7,17	ARQC 112:13,21
87:8 97:8 102:24	54:18,21 55:18	allows 57:4 108:11	90:12,19,20,21	arranged 15:21
107:15 108:21	57:3 60:2 104:2	alternative 30:15	113:24 114:1	arrives 26:15
AC 110:19 111:11	acquirers 53:2	72:17	115:10	art 15:16,19 16:4
111:17,23,25	acquiring 11:11	AMAC 36:17	apologize 64:9	16:19,20,22 17:17
112:3,6,10,19,23	50:6 54:11 55:14	American 9:20,21	apparent 46:9	17:20,25 18:24
114:5	acting 8:11 89:10	12:2,19,22 50:15	104:4	19:9 20:11 22:2,8
accept 30:23,25	actual 29:6 36:8	51:2 116:14	APPEAL 1:2	24:21 25:4,7 26:1
access 18:20	43:1 66:24 72:13	Amex 53:17	appear 17:13 29:8	26:10 27:14,19
account 17:22 18:7	83:2 101:12,20,21	amount 19:19	118:7	28:8,13,16 29:13
18:8,12,14,16,21	added 66:23 67:3,5	31:20,22 56:10	Appendix 62:11	29:20,24 30:3,6
18:23 19:6,6,10	additional 34:10	110:11	application 14:13	30:14,20,25 32:11
19:13,15,20,22,23	99:21	analysis 63:2 64:4	14:15 29:19 39:7	33:12 35:3,12,17
19:24 20:2,3,6,8	additionally 48:6	91:11 106:20	39:10,22 42:1	35:22,25 36:16,22
20:14,14 21:4,6,9	49:3	analyzed 65:6 66:3	44:23 52:3 55:20	37:1,5,19,23
21:11,13,19,20	address 38:6	96:16	58:6 60:14,18	38:17 41:5,9,19
22:1,4,9,11,13,16	adopt 60:24 62:19	and/or 60:2 104:2	61:5,7,25 62:22	42:19 43:3,11
22:17,21,22 23:2	adopted 52:1	annotated 66:19	66:8,13 67:21	44:6 45:9 46:9
23:6,13,15,22,22	adopting 61:23	annotation 29:7	73:7,15 76:19	49:13,23 51:19
24:3,10,13,15,22	advanced 33:24	66:23	78:6,12 79:25	52:7 55:8 64:22
25:2 26:25 38:23	AES 33:22,25 34:4	annotations 75:1	80:9,11 82:25	64:24 65:1,3,9,14
40:1,6,12,19 42:4	34:10,15,16,16	answer 4:20 7:1,19	83:22 84:20 87:18	76:7 80:15,17
75:15 81:10,17	affirmed 4:4	9:10 10:5,13	88:4,21 90:8	81:2,6,9 88:8,18
83:10,19,23,25	affixed 119:15	12:17 13:7,25	92:22,24 93:5	90:18 94:25 104:5
84:23 85:3,4,9,11	afternoon 62:6	16:10 35:10,16,21	94:13 98:3 111:17	104:8 105:15
85:17,19 86:8,20	agencies 11:12	36:25 37:4 45:14	111:22 112:7	116:18 117:10
86:21 87:2,4,7,9	12:24	49:2,6 53:3 64:3	116:2	articulate 71:2
87:11 89:22 90:2	ago 64:11 86:5	64:16 68:7 71:2	applications 14:20	asked 77:5 88:8
91:6,9 93:13	agree 46:6,13 76:13	77:4,19 81:4	14:20,21 51:18	asking 4:19 16:7
110:22 111:1	105:6 107:21	86:11,14 97:1	61:11	17:16 20:25 43:9
113:11,14,15,25	ahead 32:23	99:2 100:18	applied 15:25 17:4	70:23 117:1,7
114:8 115:8	aim 60:17	102:25	43:20	asks 23:21
account- 86:18	Alan 1:24 119:3,22	answered 10:20	apply 44:15 116:12	assigned 7:21
account-specific	albeit 45:16	45:7	applying 104:11	assignments 8:7,8
83:11,12,16,20	algorithm 28:23,24	answering 79:11	appropriate 30:18	8:17,17 9:19,21
	30:11,21 31:2,3,4	92:19	80:24 82:6 107:9	10:10

assist 13:21 assisting 11:16 associated 17:21 18:8,12,14,15,23 19:10,17 20:13 21:19 22:4 23:5,9 24:14 29:18 38:22 40:1,6 42:3 75:14 81:16 83:10,24 84:22 85:5,11,18 85:19 86:8,8,20 86:21,22,24 87:3 89:22 associates 40:11 associating 40:18 association 87:4,10 associations 20:10 assume 5:1 assumption 14:1 asymmetric 109:5 ATC 55:21,23 80:7 80:16 82:6 83:12 98:22 attached 118:7 attacker 48:7 85:13 attention 106:19 attribute 85:7,8 authenticated 72:17 104:16 authenticating 26:20 authentication 32:6,9 60:15 61:6 74:21 106:24 107:3,9 109:3,11 109:16 112:7 authorization 26:16,24 27:13 61:13 104:1 105:12 116:19 117:2,8,11 authorize 24:19 26:18 available 30:21 39:11 50:12 54:17 54:20 55:2,24 56:2	Avenue 2:13 aware 13:15 41:9 43:24 49:24 51:20 52:8 55:9 awful 5:22 B B 59:11,12 back 6:12 7:25 10:12 14:9 21:24 23:3 24:2 31:12 31:21 32:8 42:8 47:23 57:3,16 58:21 59:11 62:5 72:24 78:23 83:7 88:16 92:16 93:11 94:5,11 106:9 108:4 110:14,16 110:18,19 115:1 background 57:17 65:2 BAKER 2:3 bank 20:9 21:4,17 26:15,16,18 57:19 117:11 bank's 23:12 banks 11:11,11 12:24 36:6 based 11:5 16:4 17:8 49:3 54:4 63:13 64:22 basis 71:11 108:12 BC 2:11 4:10 bear 4:22 began 86:14 beginning 106:21 begins 60:13 behalf 2:2,10 9:9 9:13 10:16 believe 11:21 17:24 25:1 30:24 76:17 best 79:14 better 47:20 beyond 109:24 big 110:14 bill 19:21 20:7 billings 12:10	binary 38:9 binders 5:21 bit 12:4 59:22 65:17 96:24 98:5 110:24 bits 33:20 43:25 44:1 block 33:3 34:4 blue 67:9 68:14 Bluetooth 41:12 BOARD 1:2 bold 114:23 Book 52:19 59:7 60:9 62:8 90:8 Books 59:9,11 bottom 15:10,13 62:16 82:7 94:15 102:5 106:22 BOTTS 2:3 box 66:22 67:4,9,12 67:20,25 68:4,6 68:14 75:7 boxes 67:2 brain's 107:13 brand 50:15 brands 9:23 49:18 49:20 52:25 break 38:14 41:16 42:5 62:2 83:4 106:4,5 broad 49:16 69:4 broader 43:7 Brock 1:24 119:3 119:22 build 11:13 bunch 51:5 business 11:2 buy 19:18 bytes 33:20 34:5,6 34:7,12 43:3 45:17,21 C C 2:1 4:2 52:19 59:11,12,12 89:4 C-1 59:13 C-2 56:14 59:7,13	C-3 59:13 C-4 59:13 calculate 47:6 56:2 75:25 77:10,13 calculated 40:14 56:7,8 76:14,15 84:3,5 105:3,19 calculates 103:24 calculating 98:23 calculation 28:19 28:20,21,21 30:10 31:19 36:12 43:22 101:12 105:13,16 105:23 106:2 calculations 98:12 98:13,16 call 19:14 68:1 77:1 78:13,15 called 11:3 19:13 28:7,25 32:10 33:6,7 34:1 39:8 40:14 42:23 49:19 49:20,21,22 50:10 51:1,2 54:1 66:5 72:13,14 105:24 107:2,25 109:2 calls 33:2,10 59:9 59:10 Camellia 35:18 CAP 73:15 74:21 capabilities 54:7 capability 25:14 57:1 capable 50:9,22 capacity 8:2,10 capital 75:12,12 89:4 Capital-A 90:2 capital-C 89:25 capital-P 89:25 90:1 capitalization 89:15 capitalized 89:21 card 11:10 18:4,15 18:20 19:5,6,12 19:13,15,16,18,19	19:20 20:5,6,13 20:18,19,20 21:1 21:6,7,8,9,17,18 21:24 22:12,14,16 22:17,20,20,22,24 22:25 23:5,8,14 23:20,24 24:2 26:21,23 38:23 39:1,2,4,6,12,22 40:2,2,10,10 41:25 42:22 49:19 49:21 50:8 51:13 51:15,16,18,22,25 51:25 52:9,11,22 53:6,10,13,16,21 54:3,14,25,25 55:22,25 56:1,5 57:3,11,19,24 58:2,11,14,19 59:14,15 61:8,11 61:17,21 78:5 80:6 88:12 89:4,9 89:12,14,16,20,20 89:21,22 90:1,10 90:24 92:23 93:20 93:22,25 94:4,6,7 94:8,10,11,13 95:5 96:2,3,5,19 97:2,5 98:18 104:15 105:14 107:2,3,6,9,20 108:2,6,11,13,20 109:1,12 111:2,2 111:3,9 112:14 113:10 116:6,9,10 116:15,16 Card' 88:20 card- 84:4 card-specific 78:1 84:4 cardholder 18:9,10 26:22,23 39:8,20 48:10,12,13 49:4 cards 8:1 14:21,22 18:7,8,19 20:22 20:24 21:10,12 22:21,24 24:4
--	--	---	--	--

54:2 88:6 89:8 90:24 93:24 105:11,25 107:18 carried 55:24 82:14 102:21 103:13 carry 54:7,9 55:19 55:19 cart 68:6 case 15:12 27:24 38:8 50:25 51:1,2 51:3 55:14 70:1 86:7 89:10,23 94:7 98:22 108:3 115:7,10 119:12 120:2 cases 8:11 27:9 48:18 49:19 56:7 58:4 108:15,23 center 15:4 central 25:12 cents 107:19 certain 44:2 certainly 10:11 22:13 41:9 79:12 82:1 99:16 104:13 certificate 112:17 119:1 certify 119:6 cetera 53:1,19 challenged 15:17 16:20 63:6,9,18 63:20,22 64:5 chance 38:13 change 38:21 39:25 120:6 changed 17:8 channel 27:16,21 27:25 28:2,3,10 67:6,10 68:12,17 68:18,22,23 69:1 69:4,11,12,14,18 69:19,21,23 70:8 70:16,16 71:6,12 71:13,25 72:2,5,8 72:11,18,22 channels 28:7 69:6 70:25	characteristics 43:14 check 7:18 64:17 66:25 88:10 107:23 checking 23:22 CHECKSUM 111:12 China 12:3 chip 20:22,24 39:6 39:10,14,15,16 58:5 90:24,24 93:23 choose 53:10 61:4 61:13 116:2 chose 59:15 chosen 77:1 circular 18:18 circumstance 107:14 circumstances 38:5 107:8 115:18 citation 70:7 71:16 71:19 115:13 cite 90:4 94:17 cited 70:23 99:19 111:20 cites 99:21 citing 90:6 100:24 113:21 claim 14:17,19 15:17,18,18,21 64:5,17,18 73:1 74:17 87:23 91:3 96:1,17 115:1 117:7 claimed 67:18,24 68:11 claims 16:21 17:2 63:6,9,12,15,18 63:20,22 68:19 116:20,25 117:1,4 117:6 clarification 59:18 clarify 13:25 57:17 clarity 68:3 73:25 74:24 78:24 86:12	87:19 95:18 clear 39:12 66:5 76:15 clearer 48:24 clearly 72:5,7 74:13 clients 12:6 closest 82:18 cloud 70:15 74:6 100:14 103:1,11 Cloud_CVC3TR... 82:8,21 code 14:10 21:8 24:1,5,8,9,14,17 32:6,9 92:23 coders 14:11 codes 24:3 colleagues 9:1 collection 11:7,8 26:8,10 41:20 Collinge 5:19,20 42:10,15,17 43:5 46:6 63:2,6,13,18 63:22 64:6 65:6,7 65:13,15,18,19,21 66:3,6,11,13,20 66:25 69:9 70:7 73:20 74:5,9 75:3 75:12 76:2 78:9 78:18,22,25 79:8 79:15 81:21 82:10 82:12,15,15,18 88:3,9,24 89:5,16 89:19 90:4,14,18 90:20 91:11,13,16 91:18,22,25 92:8 92:16,21 93:4,7 93:14 94:16,18,19 95:6,8 96:10,16 96:18,21,21 97:3 98:8 99:10,14,18 99:20,21,22 100:4 100:7,13,19,25 101:14 102:15,18 102:22 103:1,5,12 103:13,19,25 104:9,21 105:2	107:2 Collinge's 67:11 70:12 96:8 column 47:3,16 49:7,9 106:21 111:24 112:4,19 113:2 combination 64:22 combine 64:25 65:10 combined 15:21 combining 65:18 come 27:4 33:8 58:7 105:20 comes 12:15 95:13 95:13 105:5 110:17,19 coming 95:6,8 99:10,11 105:3 110:16 command 88:13 94:14 110:3,4,10 110:18,19,20 111:4,8,10,11,13 111:18,23 112:1,3 112:6,10,19,23 114:4,5,12 command- 88:20 commands 88:19 94:3,9 110:13,17 commission 119:17 committed 7:2 common 51:25 53:8,22 65:3 communicate 14:22 69:12 70:16 70:19 71:10 communicated 88:20 communicates 68:8 communicating 72:22 90:12 communication 51:21,24 54:2 68:12,17,18,22 69:10,11,13,14,18 70:9,13,20 71:12	71:13,15,19,24,25 72:2,5,8,11,20 85:2,8,14 87:17 91:5,8 110:4 communications 27:15,20,22 28:2 28:5,10 41:7 52:1 52:4 67:6,10 83:23 84:19 88:5 companies 11:13 company 8:6,23,23 8:25 9:3 10:23 11:3,19,22 12:6 company's 11:1 12:20 compared 10:2 comparing 103:18 103:23 104:14 comparison 103:20 104:6 compatible 61:22 complete 118:6 completely 53:18 complex 109:14 compliant 53:25 57:12 61:22 96:22 comply 36:6 58:12 58:14 96:11 97:15 116:1 complying 97:6 component 26:24 72:25 comprising 87:17 91:5,8 COMPUTE 111:12 computer 5:25 6:4 6:5,6,16 14:6 25:5 25:8,15,16,20 26:2 27:12,24 72:25 73:3 74:16 84:20,21 computers 25:19 25:22,23 26:1,7,8 26:10 concatenating 101:24 concept 32:6,9
---	---	---	---	--

90:22,22 concerned 8:1 61:15 concerns 7:4 concluded 117:23 conclusion 114:13 conduct 48:17,19 57:5,20 116:17 Conducted 1:14 confess 36:7 confidential 39:21 configured 112:14 conforms 96:2 confuse 46:17 confused 92:15 95:17 confusing 59:4 76:12 78:22 86:16 confusion 98:8 connection 70:14 72:6 73:21 connections 71:9 consecutive 43:25 consider 12:20 14:4 14:12 24:9 26:1 26:14 41:11 84:22 consideration 16:18 considerations 16:23,24 17:9 considered 24:18 64:18 83:24 consistency 15:8 consistent 28:10 114:2 constructions 115:5 consult 9:11 10:18 10:21 11:4 12:16 consultancy 11:6 11:25 consultant 8:12,13 13:22 consulting 8:7,8,10 8:25 9:4 11:6,24 consumer 107:24 contact 57:25 58:4	58:25 59:16 contacted 7:14 contactless 8:1 50:2 50:13,14,19,24 51:4,5 52:12,14 52:18 53:6,6,21 53:21,23 54:3 55:1,7 56:1 57:5 57:12,25 58:2,3,5 58:18 59:2,7,8,10 59:13,15,23 69:22 88:6 93:23 95:13 95:23 97:8 108:5 114:10 116:7,8,15 contain 114:8 contained 20:22 container 57:6 containing 91:9 contains 39:6 66:16 content 16:19 contention 90:11 context 16:7 18:3 26:9,14 29:14 34:3,17 37:10,14 38:1,5,10 41:24 44:23,25 45:15,20 49:17 53:3 59:1 80:24 87:12 contexts 33:6,7 continue 86:6 continues 16:12 control 61:7,10,12 controller 12:17 controlling 6:4,5,6 conversant 80:18 convinced 74:23 coordinated 25:24 copy 5:14 15:1 42:11 46:15 core 11:15 corner 15:11 correct 5:12 7:6,6 13:23,24 21:23 23:7 31:9 40:4,23 46:17 49:9 52:11 59:25 60:5 62:1 75:5 77:11 79:5	80:13 87:3 88:15 88:22 90:16 93:10 98:15 102:17 103:4,19 111:19 115:24 118:5 119:7 corrections 118:7 correctly 48:15 74:1 93:3 counsel 6:5,6 7:14 13:18 66:12 119:11 counted 66:13 counter 55:20 76:20,25 78:6,12 80:1,10,11 83:1 98:3 100:14 103:1 103:11 countries 23:20 country 50:5 couple 14:24 38:15 99:1 107:8 course 25:21 court 5:5 13:17 119:1 covers 91:16 create 80:12 98:12 113:12 created 38:22 39:25 creates 37:16 credential 41:14,20 41:22,23,25 42:3 82:3 89:8,11 credit 19:18,19,20 20:13 24:2 CRR 1:24 119:22 cryptogram 28:14 28:17,18 29:3,6,8 29:19,21,23 30:6 30:9,22 31:5,10 33:7,22 34:2,7,11 34:11,23 35:7,14 35:19 36:9,11,13 36:14 44:23 47:6 55:19,23 56:11 60:14 61:25 91:5	91:9,12,13,14,17 91:19,21,24 92:1 92:7,22,23,24,25 93:5,13 100:1 104:14,15 105:7 105:17,23,25 107:3 108:9 110:21 111:7,7,17 111:22 112:2,2,7 112:10,12,24 113:12 114:4,9,10 115:9 cryptograms 29:11 30:2,16 34:16 55:2,9,11 56:3,6,7 60:19 61:6 105:13 105:19 107:2 109:19,22,23 cryptographic 28:18,20,21,23,23 30:10,12 33:4,5 34:1,16 36:12,17 37:6,8,10,16,20 38:1,6,8,9,11,18 38:20 39:3,17,24 40:5,13,16,18 41:1,1 42:2 56:9 75:14 81:16 100:12,20 101:10 101:16 102:6,9,12 102:20 105:6 109:4,6,17,20 111:12 113:5,6 curious 99:2 current 8:21 34:18 currently 11:19 customer 21:25 27:6 customers 9:24 11:9 12:6,12,13 12:14,20,23 97:11 97:11 CV 9:18 CVC 93:1 CVC3 82:25 83:1 91:18,20 92:23 93:1,7 98:2,11,14	98:23 100:1,16 102:13,14 103:19 103:21,23,23 105:2 cycle 82:2 D D 2:4 4:2 59:11,12 D-PAS 51:4 D.C 2:6 data 19:3,7 22:12 22:15 24:18 26:21 27:23 28:22,24 29:1,16,17 30:10 31:19,21,22,22 33:3,5,9,9 37:24 37:25 39:9,11 40:15,15 41:21 42:1,21 44:7 47:17 50:7,10,10 50:11,22 53:7,9,9 53:14,22,23,25 54:1,8,9,13,15,19 54:22 56:10 57:1 66:5 70:5 76:19 80:7 81:22,24 82:3,21 83:2 87:11,18 88:21 89:22 105:22,24 106:24 109:2,11 110:11,13,16,17 110:19 111:6 114:11 database 23:12 date 7:16,17 21:7 109:16 118:12 120:3 day 119:15 120:23 days 10:9,15 108:24 DEA 28:25 deal 15:6 34:15 58:19 dealing 116:9,9 debited 19:20 debt 21:15 decide 26:18 60:24
---	--	--	--	--

62:19 112:21 decides 112:5 deciding 24:18 decision 23:23 107:18 declaration 5:11,14 5:18,23 6:3 7:4,10 7:11 9:17 14:25 17:3,15 64:20 66:16 68:20 69:7 71:18 73:11 74:25 75:11 79:10 81:15 83:8 87:15 90:3 91:1 93:18 97:18 110:2 113:19 114:18 decline 112:6,12 declined 27:10 decrypt 47:17 48:15 deemed 27:8 44:3 define 28:1 31:14 defined 34:11 52:17 58:6,7,8 65:8 78:3,4 defines 90:23 94:9 94:9,12 definition 18:18 26:6 30:24,25 31:13 89:19 definitions 51:12 59:14 delete 86:6 delivered 85:2 depend 19:7 depending 111:9 depends 105:7 depo 4:18 DEPONENT 118:1 deposed 4:13 deposition 1:13 5:4 6:15 15:6 42:15 117:23 119:5 derivation 62:14,17 76:16,19 78:20,24 80:7,19 101:9 derive 40:15 100:8	100:12,15,20 101:16 102:20 103:2,12 derived 38:2 79:2 83:1 100:3 105:21 deriving 62:23 78:11 84:17 98:18 98:20,21 DES 28:25 33:2,17 34:6,6,14,14 37:12,12,17 102:7 113:11 describe 51:16,17 79:1,15 81:15 84:9,12 91:25 92:9 93:23 94:2 99:25 100:2,4,7 104:17 112:18,25 described 27:13 28:11 32:14 49:4 52:13 56:6 72:1 78:20 79:14 84:15 84:17,18 85:6 96:18 99:12,14,16 101:10 104:9 109:17 115:19 116:10,12 describes 33:10 61:4 76:16 79:18 91:19 103:25 describing 43:9 62:13 91:20 description 48:25 76:7 83:18 101:1 101:11,18 115:21 design 11:13 25:22 25:25 detail 26:7 28:4 66:9 70:20,22 79:2 98:6 99:12 99:17 110:25 details 83:2 determination 16:17 determine 18:24 27:5 31:12 37:25 43:21 44:8,16,25	45:11 63:12 81:7 81:10 99:7 determined 53:15 54:6 65:9,23 determines 108:11 determining 99:8 development 14:13 device 67:7,11,14 67:15,18,21 68:8 68:9,10,23 69:22 69:24 70:9,19 71:5,7,8,14 72:1,2 72:6,9,16,18 73:7 73:8,23 75:16 76:4 81:18,23 83:17 86:2,4 87:17 88:12 89:8 89:10,12 91:4,7 96:4 97:9 109:6 111:15,16 devices 88:25 90:15 diagrams 49:1 74:14 97:4 differed 52:2 54:24 difference 32:25 47:10,21 differences 16:20 105:18 115:22 different 8:10 21:12 23:24,25 25:23,23,24 27:24 28:3,6 30:11 32:18 46:24 47:7 49:24 51:5,7,10 51:15,20,21 52:8 52:9,11,12,20,21 53:11,18 55:25 60:3 61:14 69:5 69:11,18,25 70:15 70:16 71:13 72:7 72:12,21 87:7 90:17 91:23 92:4 92:7 95:9 97:12 105:13,14 111:20 112:1,11 113:8 114:2 115:9 differentiate 78:16	differently 59:16 digests 31:20 digital 41:14,20 42:2 82:3 109:7,9 109:21 digits 45:10 55:23 101:25 102:2,3 Diplomate 119:3 direct 14:25 16:11 47:3 56:12 60:8 60:12 62:7 63:1 66:15 87:10,14 93:17 110:1 directed 49:7 discarded 54:16,19 54:23 55:13 disclose 103:20 105:2 disclosed 15:19 96:20 100:22 discloses 47:16 56:23 disclosure 16:4,5 46:6 47:20 65:22 70:12 71:23 82:12 90:4 99:3 100:18 102:18 103:5,10 disclosures 66:1 90:19 99:23 discover 9:22 12:3 12:19 28:5 50:17 50:18 51:3 discuss 88:17 discussed 24:24 70:20 93:12 discussing 14:2 22:5 37:11,15 48:4 49:17 71:1 87:12 107:1 108:4 Discussion 6:11 distilled 91:18 distinction 64:14 document 6:15 47:24 59:1,5,6 88:10 90:9 documentation 49:22	doing 11:19 61:16 63:25 dollars 107:20 double 89:12 double-check 68:15 downloaded 87:11 Dr 4:9 6:14 42:9 46:21 62:6 draw 8:23 drawing 68:6 drive 78:1 dual 70:8 dual-channel 70:13 70:20 71:15,18,24 72:20 duly 4:4 dynamic 92:23 93:1 E E 2:1,1 4:2,2 59:11 e.g 69:12 earlier 19:23 49:8 62:8 77:3 78:21 111:1 early 7:25 14:9 82:2,2 earn 8:20 earnings 8:24 12:5 12:14 Eastern 1:16 eavesdropping 85:14 eight 92:21 either 13:22 15:19 17:13 20:13 31:9 54:15 74:11 111:10 115:7 elected 59:16 electronic 67:24 element 64:5 97:10 elements 25:23 64:1,12 ELIOT 2:4 Eliot's 6:2 eliot.williams@b...
---	---	---	---	--

2:8	encryption 28:24 33:25	excuse 40:3	fact 7:3 72:11 82:7 90:21 108:14,17	46:23 47:15 48:20 49:2,4 62:6 78:8 106:20 109:17 111:21 112:25 118:3 120:4,21
embossed 19:12	endeavored 63:12	executing 73:7	factor 17:8	fit 54:16
emitted 39:15	ended 86:13	exhibit 15:10 42:11 42:12 46:14 56:12 60:8,13 62:7 78:18 79:1,7,8 87:20 90:6 92:16 95:7,8 100:25 101:15 106:20,21	factors 16:18	five 117:16
employed 8:2,5,6 8:22 10:22,23 119:12	engaged 13:21	exists 106:20,21	fair 5:2 14:4 17:18 65:6	five-year 22:23
EMV 13:10 29:15 30:1,16,19 33:19 34:3,11,11,17 36:11,13 37:16,21 38:6 40:12 43:6 45:6 48:17,19 50:6,21 51:3 53:9 53:22,25 54:1,4,4 54:7,12,13,15 57:9,12,14,18,19 57:22,25 58:13,15 58:21,24 59:5,7,8 59:19,23 60:3,9 61:15,17,22 62:22 63:3 65:7,13,15 65:19 66:1 76:15 77:25 78:3,4,7,16 80:5,18 81:3 90:8 90:19,21,22 91:16 91:20,21 93:1,6 94:1,2 95:15,21 95:25 104:15,19 105:11,24 107:17 109:2 110:11 115:20 116:1,7,9	ensure 88:24 90:14	exhibits 3:1 5:22 13:3,9 17:14 52:18 59:21 115:17	flight's 106:14	flowing 51:16 52:9 53:5,20 54:13
EMV-acquiring 57:8	entered 48:14 55:3	existence 16:22	familiar 17:21 25:5 27:15 28:14 29:25 30:3,7 36:1,17,23 37:2	flows 53:2 81:22 97:4,5
EMV-based 52:14	entering 48:14	existing 96:13 114:14 115:6	far 4:18 61:15 107:1	fly 55:16,17
EMV-capable 58:2	entire 55:12	expand 96:11 97:10	fare 11:7,7	follow 40:12 97:7
EMV-standardiz... 88:25 90:15	entities 12:15,18	expect 11:22 35:2 87:2 94:5,10	feature 107:17	following 16:11 43:3
EMVCo 34:15 52:17 53:13 57:21 58:7	equivalent 111:6 114:11	expected 96:13	Federal 13:16 36:1	follows 4:6 15:9
encapsulated 88:7	Errata 118:8 120:1	experience 105:18	fees 9:1	foot 15:2
encompass 26:6	ESQ 2:4,12	expert 8:9 11:23 13:22 14:5,11,12	felt 63:16 64:2	foregoing 118:5 119:5,6
encrypt 48:6 102:3	essentially 70:3 75:7	expertise 14:17,19	figure 66:19,20,23 67:17,24 68:11 69:9 72:24 74:4 74:11,12,25 75:2 75:3,6,8	form 8:4 9:15 12:8 13:5 14:2,14 16:6 17:10,23 18:2,17 18:25 19:25 20:15 21:21 22:6,10,18 23:16 24:16,25 25:9,17 26:3,12 27:17 29:4 30:8 30:18 31:7,17 32:21 33:23 34:24 35:8 36:2,10,19 36:24 37:7 38:3 38:19 40:7,22 41:2,15 42:20 43:16 44:10 45:1 45:12 46:1,25 49:12,15 50:3 51:8,23 52:23 56:4 57:15 63:14 65:12 66:2 67:19 68:13 69:2 72:4 73:2 74:18 75:19 76:10 79:4,17 81:1,12 82:17,23
encrypted 47:17 48:16 75:16 81:19 81:21,24 82:14,21	establish 26:21,22 26:25	expires 22:22 38:24 40:2,3 119:17	filed 13:3	
encrypting 78:10	estimate 12:5	expiry 21:7	fill 54:20	
	et 53:1,19	explain 32:25 39:5 53:23 77:23 83:15 98:4	filled 65:25	
	Europe 20:23 57:10 107:11	explained 88:11	financial 12:16 92:2 104:4 119:13	
	evaluation 64:21	explains 66:9	find 21:25 64:3,11 70:21 82:18 95:2 99:3 102:24 104:8 108:17 115:15	
	evening 106:12	explanation 89:21 114:17 115:13,15	fine 55:5 106:14 108:18	
	everybody 61:14	explicit 16:4 103:22	finish 4:20 38:15	
	everything's 108:18	explicitly 15:20 64:17 88:9 100:2 104:6	finishes 104:2	
	evidence 115:15	Express 9:20,21 12:2,19,22 50:15 51:2 116:14	FIPS 36:1,4,7	
	Ex1006 15:3	ExpressPay 50:16 51:3	firm 4:10	
	EXAMINATION 4:7	extensive 43:24	first 4:4 7:14 8:19 19:2 26:19 40:9 60:16 62:7 68:11 68:17,18,21 69:13 71:25 73:4 97:25 106:23 107:10 113:23	
	examined 4:6 118:4	extremely 108:1	Fiske 1:13 4:3,9 5:20 6:14 13:7 42:9 46:16,18,21	
	example 15:2 18:9 19:11,18 20:23 21:5,17,23 22:22 28:1,24 29:8 33:1 33:18 36:9,11 39:13,19 45:10 47:3 49:12 58:11 69:25 80:22 85:23 92:22 99:4 107:19 111:24 112:9,20 114:9	F		
	examples 19:8 32:1 39:17 49:18 69:18 114:14 115:6			
	exception 58:6			

84:1,24 85:20 86:23 95:11 96:23 99:15,24 100:10 102:23 103:15 104:24 105:9 110:23 113:9,16 116:5,22 forming 17:6 forms 95:13 105:20 formulated 88:4 96:4 formulation 95:15 95:21,24,25 forward 82:14 102:21 103:13 found 64:4 78:22 78:24,25 94:23 103:22 117:6 four 5:21 43:3 45:19 fourth 17:8 79:22 frankly 66:4 fraud 27:3 fraudulent 27:6,8 frequencies 28:6 front 5:18 6:3 19:13 full 50:22 55:19,20 95:15 fully 79:6 function 62:19 functions 60:24 fund 27:2 funded 27:1 funding 18:7,19,21 19:6,17,22,24 20:5,8,14 21:11 21:13 funds 18:6 further 47:23 49:3 69:9 73:14 91:17 98:5 112:19 future 11:22 96:13	gates 109:8 general 38:8 43:9 90:10 generate 29:21,23 30:5,21 31:5,10 33:2,16,18,20,22 33:25 34:5,10,19 34:22 35:14,19 40:25 56:10 61:5 79:9 80:6,21,22 81:3 84:7,10 100:16 105:7 109:20 110:19 111:11,17,23,25 112:3,6,10,10,18 112:23 114:5 generated 30:2 42:21 43:19 44:4 45:18,23 61:19 73:15 74:20 76:24 76:24 79:16,19 83:1,10,16 84:13 91:14 103:21 104:15 112:12 113:1 generates 34:7 78:6 107:3 109:7 generating 30:16 32:7 35:6 40:20 44:14 76:3 77:24 79:22 80:1,10,11 80:16,22,25 92:1 generation 46:8 60:18 61:24 78:14 83:12 101:20,22 104:13 generator 43:13,19 46:5 75:23 77:8 generically 19:14 genuine 26:21,23 39:20 41:23 107:6 108:2,11,13 109:1 109:12 getting 64:8 92:15 give 5:7 7:17,19 9:2 9:16 10:12 19:8 47:1 60:6 68:16	117:3 given 11:25 30:9 31:11 81:2 106:11 114:17 118:6 119:7 gives 24:6 57:18 global 57:18 globally 58:13 61:16 go 4:17 6:8,12 10:12 23:3 28:4 31:12,21 32:8,23 56:17 62:2,5 63:23 74:21 92:16 93:11 98:17 106:9 107:23 108:9,16 109:9,13 112:13 117:15,20 goes 4:18 39:8 58:18 66:9 105:22 110:5,8 going 7:2,24 15:9 17:12,16 38:13 42:9 46:18 55:5 58:21 95:1 97:1 106:17 107:16 112:15 good 4:9,12,23 5:9 15:5 42:5 62:6 117:17 grab 60:7 grants 18:20 graphic 68:4 graphics 75:2 gray 75:7 Group 2:11 4:10 growing 31:25 guess 7:16 71:22 110:6 guessing 10:20 guidance 34:15 Guilford 11:5	halfway 73:19 76:2 hand 21:2 119:15 handle 114:15 handled 29:13 happens 4:23 23:19 23:24 33:3 57:23 58:1,25 59:2 108:14 happy 106:16 109:14 hardware 36:6 hash 31:2,4,14,16 31:19,24 32:1,2 32:10,12,16,19 33:3,11,14,14 head 5:8 20:16 42:25 heading 56:18 89:24 hear 4:21 help 47:20 helpful 73:3 79:11 92:10 hereunto 119:14 highlighted 68:14 68:24 highlighting 67:13 highlights 67:6,10 HMAC 35:23 36:9 Hold 73:5 holding 5:22 21:2 home 106:12 hope 12:1 hopefully 46:17 59:21 host 27:13 61:12 104:14 106:1 hosts 106:1 hour 38:13 106:4 106:16 hours 9:7 86:5 Hyperion 11:3,4	50:22 112:21,25 113:4,8,11,14,14 icon 68:10 idea 9:12 35:6,11 48:4,8 ideas 35:5 identified 38:7 63:15 74:2,12 identifier 22:9,12 24:10,23 25:2 91:6,10 93:14 110:22 111:1 113:15,25 114:8 115:8 identifies 19:15 22:12,15,16 29:17 40:11 113:10 identify 22:20 24:13 42:24 67:17 67:23 72:24 83:19 95:6,22 identifying 74:16 identity 11:7 41:22 illustrates 72:10 IMK 102:14 immediately 114:22 implement 86:3 88:24 90:13 104:9 104:21 implementation 11:17 95:20 implemented 11:18 52:12 90:20 implementing 90:10 implied 15:21 16:5 important 5:7 108:24 improvements 107:11 Inasmuch 14:1 88:5 include 11:11 25:15 26:19 30:1 70:8 79:25 80:9 82:5 included 20:24
--	---	--	---	--

52:21 81:24 includes 16:17 29:15 40:16,17 53:22 67:21 68:5 80:16,25 82:7 110:21 including 42:2 82:3 incomplete 65:22 incompleteness 65:25 INCORPORAT... 1:4,6 incorrectly 52:6 INDEX 3:1 indicate 62:21 89:13 indicates 96:7 indistinguishable 29:9 individual 51:15 52:25 53:10,15 58:9 59:14 industry 12:1 18:5 29:14 30:13 32:4 34:14 inevitably 24:7 information 18:23 19:9 20:12,17 21:1,3,5,11,16 39:13,21 50:9 51:16 52:9,21 53:2,5,11,20 55:13 57:6 60:1,3 61:18,19 71:4 72:12 81:10 83:21 83:24 85:15,18 86:18,24,25 87:1 informed 13:18 infrastructure 56:24,25 57:9 96:13 infringement 13:16 inherently 15:20 initiated 67:15 injected 38:25 39:4 input 28:22 30:10 33:3,4,9 37:9,12	49:10 56:10 105:22 input/ 25:13 inputs 31:12 32:8 96:2 insert 57:23 inside 14:21,22 61:12 94:3 instance 23:8 74:2 74:3 instances 16:3 17:6 65:21 instant 47:12 70:21 95:3 insufficiently 44:3 intent 89:13 interact 61:17 90:24 interaction 67:13 interchangeable 19:24 interchangeably 20:1 45:4 interest 119:13 interface 58:25 59:2 intermittently 7:25 internal 51:17 58:5 international 1:5 11:10 49:18 90:23 Internet 70:1 interoperability 57:19 88:25 90:14 96:12 97:13 interoperable 61:16 62:22 interoperate 58:13 58:15 interpretable 113:22 interpreting 80:8 interrogated 88:12 interrogates 116:15 interrogation 88:18 96:1,17 introduced 89:7 invalid 15:18	invention 97:14,16 involve 31:10 83:23 103:18 involved 13:6,16,19 14:16,18 involves 27:23 43:24 IP 70:4,4 72:23 IPR 6:23 7:12,15 8:21 9:4 11:20 13:4 16:1 IPR2023-01289 5:11 6:24 ISO 88:7 90:23 issue 15:6 110:12 issued 34:15 39:7 88:19 issuer 24:18 40:14 50:8 52:22 54:6 54:18,21 55:18 57:4 60:3,14 61:6 61:19,20 75:24 77:9,14,16,25 78:2 91:15 97:22 98:1,10,18 99:5,6 99:8 100:4,13,21 101:9,17 102:4,15 102:21 105:12,25 106:1 107:4,5,6 107:17,23 108:9 108:10,17 109:13 issuer's 61:17 issuers 50:23 53:3 60:23 61:4,7,10 62:18 issuing 11:11 20:9 26:15,16,18 27:13 36:6 117:11 item 19:3,7 22:12 22:15 29:1,16,17 37:24,25 42:21 44:7,8 66:5 74:12 105:24 items 41:21 53:7,9 53:9,22,23,25 54:1,13,15,19,22 83:2	iterating 78:10 J JCB 12:3,19 job 1:25 98:10 120:5 June 1:15 4:1 119:16 120:3 K K 2:5 75:12 KD 102:13 keep 55:5 kernel 56:14 58:16 58:17,19 59:7 115:17,17 116:11 116:12,13,13,14 116:17 kernels 52:19 key 28:23 30:11 31:3 33:4,5 37:6,9 37:12,20 38:1,9 38:11,18,20,21 39:3,24 40:5,13 40:14,16,19,20 41:1,1 42:2 47:5,6 47:7,8 48:16,16 48:18,19 56:9 60:11 62:9,14,17 73:22 75:14,21,24 76:4,7,11,16,16 76:18,18,21,23 77:1,9,13,14,17 78:1,1,2,5,7,11,15 78:16,20 79:18,22 79:25 80:1,6,6,7,9 80:10,12,12,16,16 80:18,20,21,22,23 80:25,25 81:16 82:25 83:2 84:4,5 84:5 85:24,25 86:5,9 87:13 98:18,19,20,21 99:5,9 100:5,9,12 100:13,15,21,21 101:9,10,17,17 102:4,6,10,12,16	102:20,21 103:3 103:12 105:7,21 109:6 112:25 113:4,5,6,8,11,11 113:15 keys 37:16 38:7,8 39:18 46:24,24 47:2,11,12,13,14 47:21,22 48:5,9 48:11 62:23 81:4 109:3,4,17,20 kind 5:8,24 18:18 22:25 63:25 64:8 86:3 96:24 111:15 knew 77:16 know 4:19 5:1,8 6:18 18:5,22 23:23 29:2 30:15 32:2 38:11 44:14 84:3,4,7 89:17 99:7,10 108:2 116:8 knowing 29:2 44:8 knowledge 65:2 75:24 77:9,13 97:2 known 29:21 48:7 88:18 96:9,11 104:12 knows 116:8,12 KSUN 75:11,13,18 76:4,8,12,14 77:5 77:13,16,24 79:2 79:9,16 81:7,11 81:16,17 82:1,5,6 82:25 83:9,17,19 84:3,6,10,13,17 91:14 97:23 98:4 99:7,8 100:2,15 103:3,12 L L.L.P 2:3 labeled 15:3 67:20 67:25 74:6,7,13 76:12,17 87:20 103:9
--	---	--	---	--

language 29:15 115:2,5,7 large 5:21 11:12 largest 12:14 late 14:9 law 2:11 4:10,10 15:14 lawsuit 13:16,19,23 14:3 layer 70:2,3 led 48:21 left 5:25 6:16 54:15 75:8 77:20 102:1 left-hand 102:5 legacy 50:16 legal 8:14,17 11:24 14:24 16:13 length 44:2 let's 26:14 61:9 62:5 92:11,16,16 93:11 101:3 110:24 117:15 level 16:21 26:7 28:4 life 82:2 lifetime 22:23 39:1 limitation 65:23,24 68:18 73:4 87:15 87:16,23 91:3 93:12,15 110:3 limitations 15:18 Limited 11:4 Lindner 2:12 4:8 4:10 6:8,12 38:15 41:17 42:8 62:2,5 83:4,7 106:3,7,9 117:12,17 line 47:4,18 49:10 49:11 73:14 79:23 102:4 106:22 111:25 112:4,13 112:20 113:2,3 lines 73:18 92:21 112:17,22 linkage 20:9 linked 19:5 linking 65:1	listed 11:10 12:18 12:21 little 50:11 68:6 97:16 98:5 loaded 39:10 logic 54:4 61:12 86:3 116:10,12 logo 21:5,17 London 108:14 long 33:9,20 34:5,6 34:8,12 38:9 86:5 102:2 longer 33:17 44:2 look 9:17,17 12:7 21:24 23:12 29:1 37:24 44:6,19,21 45:9,21 49:9,10 49:11 73:10 75:2 76:14,23 85:15 88:16 91:22 92:11 92:17,20 95:4 96:17 99:22 100:23 101:4 104:19 106:21 111:24,25 113:2 115:16,16 looked 65:7 90:18 97:3 looking 15:2,12 21:2 26:16 43:25 59:5 62:8 63:24 64:1 72:24 74:4 77:4 81:14 98:25 101:8 103:6,7 113:18 114:19 looks 5:24 27:4,7 68:1 77:5 97:25 100:24 Loop 1:9 13:15,23 120:2 loose 26:5 loosely 27:25 lot 5:22 13:9 66:9 low 45:16 low-value 107:19 lower 75:8 89:23 lunch 55:4 62:4	M M-A-C 36:23 M/ChIp 51:1 94:16 94:19,23,24 95:7 95:10,14,20,25 96:8 MAC 32:17 33:7 Madison 2:13 magnetic 50:23 56:23,25 95:16 magstripe 50:16,17 52:13 54:11 55:14 56:22 57:2,7,13 58:23,25 59:24 60:1 91:17,17,19 93:2,9 95:14,15 95:16,20,24,24 111:11 mainstream 50:1 maintaining 97:12 major 11:9 majority 54:8 making 18:3 manage 20:9 management 27:3 60:11 62:9 mandatory 60:23 61:3 62:1,18 manner 104:9 maps 80:4,4 March 119:17 market 54:11 55:15 96:12 MARS 35:13 master 40:14 75:24 77:9,14,16 78:1,2 84:5 98:18 99:5,9 100:5,13,21 101:9 101:17 102:4,16 102:21 MasterCard 1:4,5 7:15,20,21 8:3,5 8:14,19,25 9:3,9 9:14,21 10:2,10 10:16,24 11:20,23 12:3,19 13:12,15	13:23 15:3,10 21:18 49:19 50:17 50:25 51:1 53:1 53:18 58:11,12,20 93:23,23 94:8 95:12,23 115:8,14 115:22 116:3,11 116:13 120:2 match 96:18 materials 5:17 6:16 matter 6:23 8:14,14 11:24 13:1,13 matters 9:9 maximum 98:8 MD5 30:21 31:2 32:2 33:15 mean 8:8 22:14,16 25:11 57:11 61:1 80:10 83:15 87:19 104:18 meaning 18:1 22:5 24:23 25:8 27:20 28:11,17 31:16,18 32:13,19 45:5 53:15 means 47:5 62:1 meant 44:13 73:8 74:10 mechanism 31:11 61:16 71:5 72:15 78:4,7 80:5 mechanisms 30:16 38:6 72:12 medium 28:6 memory 7:2 34:18 mention 99:4 103:22 mentioned 12:21 23:4 24:1 33:15 33:16 51:10 92:7 93:21 99:1,18 mentions 103:21 merchant 68:2,5,10 68:23 71:14 72:6 104:2 107:7 merchant's 67:7 69:22	message 32:6,9 54:14 57:6 72:16 messages 27:23 52:3 55:16,17 messaging 54:5,17 method 54:24 62:17,19 73:20 methodology 17:3 methods 46:7 50:19 51:11 60:18,22,24 61:2,23 104:3 middle 111:15 migrated 50:6,21 54:11 million 12:11 mind 65:19 mine 6:2 minutes 117:16 misheard 73:9 misquoting 7:3 missed 74:5 missing 59:3 misspoke 68:21 mixed 64:8 mobile 28:3 41:10 67:7,11,14,15,18 67:20,21 68:9,23 69:22,24 70:5,9 70:19 71:5,7,8,14 71:25 72:2,6,9,16 72:18 73:6,8,14 73:23 75:15 81:18 81:23 83:17,22 84:19 86:2,4 89:10,12 111:14 111:16 mode 50:16 51:3 56:22 57:4,7,9,13 57:14 58:23 59:1 59:24 60:1,4 91:19,20 93:1,2,6 93:9 108:15 modules 36:6 moment 6:3 43:1 60:6 63:3 64:11 money 8:20 19:22 27:1 42:4 107:24
---	--	---	---	---

108:18 monitor 5:25 month 19:21 20:8 21:14 morning 4:9 motivate 106:17 motivation 64:25 65:10 moving 34:14 MSD 50:16 multiple 18:8 22:21 23:9 26:6 27:11 64:22 110:12 113:24 mutually 72:17	49:21 50:6 51:13 54:7,9 never 39:14,15 new 2:14,14 73:22 83:17 nexus 65:1 NFC 71:6 nodding 5:8 nomenclature 102:11 non-obviousness 16:24 non-permanent 75:14 81:16 nonvolatile 25:13 normal 78:16 normally 32:17 57:2 89:18 notarial 119:15 Notary 119:4 120:25 note 60:22 62:17 66:20 notes 6:15 notification 72:14 Now's 42:5 number 7:2 9:16 11:12 15:9,10 19:12,13 20:23 21:6,8,25 22:14 22:20,25 23:2,9 23:14,24 26:17 29:9 36:8 38:9 39:12 40:11 41:7 42:18,24 43:4,8 43:10,13,15,18,19 43:20,21,25 44:1 44:2,4,9,15,17,18 44:21,24,25 45:3 45:4,5,9,11,16,18 45:22,23,25 46:4 46:4,5 51:10 53:7 54:22 55:23 73:5 75:18,22,23,23 76:4,8,9,11,18,22 76:25 77:2,6,6,7,8 78:3,14,15 82:4	98:19,21,24 100:8 100:9,11,14,16,20 101:2,16,19,22,24 102:19 103:2,11 105:25 107:20 108:20 111:2,3 113:10 numbered 68:19 numbers 15:7 29:10 43:5,6 46:8 NW 2:5 NX 62:18	obvious 63:10,13 63:16,20 64:2,7 64:13,19 65:24 88:23 90:13,13 96:10,20 104:8,21 obviousness 16:13 16:17 17:2,7 64:21 offer 11:16 offered 63:5,8 93:22 OFFICE 1:1 officer 119:4 offline 106:24 107:25 109:2,16 112:6 oh 14:7 92:20 okay 5:10 6:7,21 7:4,7 15:12 21:3 41:18 42:5,14 46:12,22 48:2 52:5 56:16,21 59:18 62:10 63:4 64:10 66:15 67:2 68:21 74:8 77:18 77:21 87:14 88:1 91:2,22 92:3,11 93:3,19 97:21 99:19 100:17 101:23 103:10 106:6,15 114:16 once 4:14 11:18 80:5 one-to-many 22:25 one-to-one 87:5 one-way 31:11 ones 30:12 54:23 online 107:2,5,9,17 107:23 108:9,16 109:10,13 112:13 112:15 open 108:7 operate 33:4 58:22 78:5 115:14 operated 117:11 operates 28:6 operating 21:10	73:7 78:2 92:25 93:2 operation 102:8 104:20 operations 104:10 104:17 operator's 108:21 opining 96:19 opinion 16:3 17:7,7 18:13 63:8,17,19 63:21 70:14,25 71:24 76:6 80:14 80:20 97:14,22 110:2 opinions 15:25 17:1 63:5 opportunity 96:12 opposed 26:11 option 112:16 options 110:18 111:10 114:12 116:4 orange 67:12 order 12:11 19:4 79:5 98:16 ordinary 16:21 29:12 31:15 32:19 33:12 35:2 65:3 organizations 11:14 origin 29:2 44:8 original 6:25 31:22 75:2 outcome 119:13 output 25:14 31:11 32:7 33:5,6,8 34:1 outputs 33:17 outside 11:20,23 21:21 37:20 38:1 50:20 outstanding 21:15 OV 1:9 13:15,23 120:2 overall 25:22 override 27:9 owned 53:12 Owner 1:10 2:10
N		O		
N 2:1 4:2 name 4:9 11:4 21:4 21:17 named 51:5 nature 7:23 11:1 near 15:13 near-field 69:14 necessarily 15:20 necessary 50:24 need 7:18 9:10 10:12,17,21 12:16 19:2 26:17 44:23 44:25 57:16 60:7 63:23 71:8 83:18 84:6 88:10 98:17 99:8,17 107:22 116:2 needed 79:5,6 needing 109:9,13 needs 58:19 neither 119:11 network 25:21,25 28:3 41:6,10,10 41:11 50:8 54:6 55:18 57:4 68:25 69:5 70:4,4,5 71:9 72:23 81:23 104:1 108:20 networking 107:12 networks 41:12		O 4:2 Object 9:15 objection 8:4 12:8 13:5 14:14 16:6 17:10,23 18:2,17 18:25 19:25 20:15 21:21 22:6,10,18 23:16 24:16,25 25:9,17 26:3,12 27:17 29:4 30:8 31:7,17 32:21 33:23 34:24 35:8 35:15,20 36:2,10 36:19,24 37:3,7 38:3,19 40:7,22 41:2,15 42:20 43:16 44:10 45:1 45:12 46:1,25 49:15 50:3 51:8 51:23 52:23 56:4 57:15 63:14 65:12 66:2 67:19 68:13 69:2 72:4 73:2 74:18 75:19 76:10 79:4,17 81:1,12 82:17,23 84:1,24 85:20 86:23 95:11 96:23 99:15,24 100:10 102:23 103:15 104:24 105:9 110:23 113:9,16 116:5,22 objective 16:23		

P	84:12,15 88:11,16	13:16 17:2,13	18:3,4,21 19:16	94:25 96:7 104:7
p 2:1,1 4:2 15:3	89:3,19,25 90:1,3	22:3 24:22 28:9	20:6 26:14 29:15	104:19 105:15
36:23	90:7,11,25 91:4	31:13 32:8,12,16	30:13,18 32:4	116:18 117:9
P.C 2:11	91:25 92:10,14,17	33:2,10,13 46:16	34:3 50:15 97:9	personalization
p.m 117:23	92:20 93:17,21	63:9 66:14,25	PayPass 50:17	39:9,9
pad 102:1	94:15,17,18 95:4	114:25 116:21	93:20,25 94:8	personalized 39:22
page 6:3 15:4,7,9	97:17,25 98:25	117:5	95:5,9,12,13,14	40:10
15:11,13 16:12	99:4,20,21,22	pause 4:21	95:14,14,15,19,22	persons 104:4
56:17,18 60:13,21	100:24,25 101:3,5	paused 6:25	95:23,25 96:9	pertinent 16:22
62:11 66:15,19	101:6,7,12,13,14	pay 8:25 12:3 18:6	97:2,6 111:11	petition 68:20
69:8,8 71:17 73:5	101:19 102:15	19:21,21 20:7,8	payroll 81:25	Petitioner 1:7 2:2
73:10,11,14 74:8	103:8,17,25 104:7	21:15 23:21	percent 10:1,4,7	Ph.D 1:13 4:3
75:4 76:2 87:14	110:1 111:14,16	payload 75:16	percentage 9:8	118:3 120:4,21
87:19,20 103:9,9	113:18 114:22,23	81:19,21 82:14,22	12:14	phone 41:10 69:11
106:23 113:18	115:12	payment 8:1 9:23	perform 44:7 61:6	70:15 89:10
114:24 117:3	paragraphs 96:6	14:20 18:4,5,7,8	94:13 102:7	phrase 18:12 45:4
PAGE/LINE 120:6	112:18	18:15,15,19,20	performed 98:12	68:17 76:3 86:14
pages 14:25 15:1	parameters 79:9	19:5,6,23 20:13	period 8:18 9:8,19	physical 20:12 57:2
16:13 103:8	105:11,14	20:18,19,20,22,24	9:20	89:7,14
paid 9:3	parentheses 70:8	21:14,24 23:6,9	permanent 38:18	picture 67:22
PAN 19:14,15	71:18	23:13,15,20 29:14	38:20 39:3,24	piece 18:23 39:21
22:14 23:25 25:3	part 14:2 24:17	34:17 38:23 39:1	40:5,18 100:12,20	55:12 60:6
40:16,17,20,21,24	40:16 59:5 66:3	39:2,4,6,7,10,11	101:10,16 102:6,9	PIN 39:19 48:14
40:25 78:2,3 81:7	66:13 71:19 75:16	39:18,22 40:1,6	102:11,20 109:4	49:5
82:4,4 84:6,7,8,10	79:13 81:18 82:2	40:10,11 41:25	113:4	place 78:18 99:22
84:13,18 93:16	82:13,21 83:22	42:1,22,23 46:24	person 4:15,16	109:5 114:20
98:19,19 100:8,8	84:6,17 85:2,16	47:2,5,11,13,21	17:16,20,25 18:13	115:5
100:11,11,19,19	86:18,25 108:1	48:5,16 49:14,16	18:24 19:9 20:11	places 72:18 111:5
101:2,2,15,15,18	110:5,8 111:5	49:18,20,21,22,24	22:2,8 24:21 25:4	plain 18:1 22:4
101:19,22,22,24	particular 14:15	50:2 51:6,6,10,11	25:7 26:1,9 27:14	24:23 25:8 27:20
101:24 102:19,19	18:22 19:7 22:17	51:11,12 52:20,25	27:19 28:8,13,16	28:11,17 31:16,18
111:2,6 113:8,10	23:6,8,13 24:3	53:24 55:7,18	29:12,20,24 30:2	32:13
114:3	28:5 37:24 43:8	56:2 57:3,12,24	30:6,14,20,24	please 4:19,25
paper 5:22 60:6	44:7 48:20 52:19	57:24 58:9 62:21	31:15 32:11,18	32:25 116:25
paragraph 15:15	65:23 83:23 91:23	67:7,20 68:1,4	33:12,21 34:21	PMAC 36:23
16:16 17:3 46:7	97:4 105:8	72:3 73:14 88:6	35:2,5,12,17,22	point 6:14 15:5
46:10 47:5,9,10	particularly 31:24	89:8,11,20,20,22	35:25 36:16,22	38:22,23 39:25
48:3,3 64:20	84:16 98:8	89:25 90:2,10	37:1,5,19,23	40:1 66:10 71:16
66:16 69:7,8 70:7	parties 119:12	92:1,21,24 94:3,4	38:17 41:5,8,13	75:10 76:1 78:19
70:12,24,25 71:17	partly 52:13	94:16,19,24 95:7	41:19 42:18,24	79:10 92:9 98:11
71:23 72:10,14	pass 117:13	96:9,13,21 97:8	43:2,11 44:5 45:8	100:6 101:21
73:11,19 74:9	passcode 48:14	97:10 98:2 104:1	45:24 46:3,9	109:24 111:21
75:10,11 76:1	49:5	104:11,18 105:8	49:13,23 51:19	point-of-sale 71:6
79:10,12,15,18,20	password 49:12	107:15 108:6,8,10	52:7 55:8 65:14	pointed 59:1,6 82:9
81:14,15 82:19,20	patent 1:1,2,6,10	109:6,8 116:2,19	76:6 80:14,17,23	82:13 112:4
82:24 83:8,9 84:9	2:10 5:19,19,20	117:2,8	81:2,6,9 88:7	pointing 75:7 93:14
	7:5,8 12:25 13:7,7	payments 11:6 12:1	90:17 93:5,8	95:5 100:18

points 27:24 popularity 31:25 portion 40:20,25 47:15 48:20 49:7 79:20 82:9 84:14 114:18 portions 47:17 111:21 POS 60:2 68:24 69:13,19,22 70:17 71:14 72:1,7 88:13 110:4 possibilities 24:6 possible 25:21 29:2 40:24 108:5 109:5 109:7 115:5 posted 21:13 potentially 24:3 26:22 27:8 55:13 pounds 12:11 precise 20:4 precisely 59:22 92:5 predict 75:25 77:10 77:12,15 predictable 104:12 predominant 20:23 50:18 predominantly 12:24 54:10 present 15:20 23:20 67:2 105:11 115:9,10 pretty 74:22 100:22 prevalent 107:11 previous 77:19 102:25 previously 7:20 primary 18:9 19:13 principles 105:16 printed 20:25 24:2 prior 8:20 9:4 10:24 13:13 15:16 15:19 16:4,19,20 64:22,24 65:1,9 probability 45:16 probably 10:8	41:23 74:9 89:13 89:17 procedural 4:18 process 33:10 39:8 48:25 49:5 77:24 96:21 98:17 99:6 99:25 101:23 109:2,14 116:20 117:2,8 processing 25:12 51:18 58:5 76:3 94:2,12 97:22 98:1,10 104:3 110:18 111:10 114:12 produce 33:5 products 11:13 51:11 programmer 14:5 programming 14:8 programs 14:6 projects 7:21,23,24 7:25 8:3 proof 41:23 proper 7:19 proportion 9:22 protocol 52:1,4,5 87:18 88:21 protocols 51:21,24 prove 39:20 109:1 provide 41:21 60:17 64:24 provided 58:9 60:22 61:2,24 62:18 provides 62:24 105:24 providing 57:21 61:16 proving 109:12 provision 81:22 provisional 5:20 66:8,12 78:23 79:7,14 82:10,13 82:16 83:3 84:16 92:13,14 95:6 98:6 99:11,13	100:23,25 101:11 101:14 102:15,19 103:6,7,13 105:4 105:5 provisioned 73:22 provisioning 67:11 67:14,16 69:24 71:3,10,12 72:9 72:15,19 85:24 proxy 59:19 Pub 36:1 Public 119:4 120:25 publications 59:9 publishes 59:8,10 purchase 19:18 purchases 18:6 purpose 29:17 47:12 66:6,10 97:7 put 39:13 63:2 89:3 90:17 102:8	quoted 36:8 quotes 89:4,12 QVSDC 51:2	Recess 42:7 62:4 83:6 106:8 117:19 recipient 41:21 recited 68:19 73:4 recites 87:16 91:4 96:1 110:4 recognize 117:10 recognized 97:5 recommendation 34:18 record 6:8,11,13 42:6,8 62:3,5 83:5 83:7 86:16 106:7 106:10 108:5 110:3,7,10,12,20 111:4,8 114:3 117:15,18,20 119:7 recorded 5:5 records 7:18 9:11 10:12,18,21 23:13 23:14 recover 40:24 48:16 recross 117:13 red 66:22 67:4 68:24 redirect 117:21 reduced 119:9 refer 6:22 7:7,10 26:7,10 42:14 46:18,21 79:6 88:1 89:11 95:19 113:19 reference 15:16,19 42:11 47:1 63:2 68:16 70:22 94:19 94:23 95:17 96:8 106:20 117:3 referenced 5:23 52:17 57:22 references 13:9 64:23,24 65:2,9 65:13,19 93:4 referred 3:1 16:23 68:22 89:9 referring 15:7
---	---	---	--	---

37:15 56:23 68:3 79:21 87:9 89:24 93:6,8 95:21 114:21,23 115:1 refers 18:14 73:6 94:16 106:24 regarding 7:15 8:13 16:13 17:8 70:8,13 82:13 Registered 119:3 rejected 44:4 relate 71:24 94:1 related 87:2 119:11 relationship 23:1 relative 12:5 relatively 109:14 relevance 12:9 relevant 70:13 104:5 relied 17:14 relying 73:1 remaining 12:23 47:11,13 remember 7:16 10:17 43:1 66:24 remote 70:9,14 72:14,25 73:3,21 74:7,16 84:20,20 116:19 117:2,8 remote-SE 73:16 74:2,3,13,15 remote/cloud 69:10 remotely 1:14 rendered 15:25 17:1 63:10 renders 15:17 repeat 55:6 98:11 98:13,16 105:13 106:1 116:25 Reported 1:23 reporter 5:5 119:1 119:4 represent 53:13,17 representing 19:3,4 request 67:15 72:18 83:11,16,18 83:20 85:16 86:19	87:1,6 112:1,13 requested 83:22 119:10 requesting 83:19 112:16 requests 112:7 required 48:11,13 requires 30:10 respect 96:16 respond 88:13 110:10 112:21 response 6:18 39:23 83:11,16 86:25 87:17,18 88:14 91:4,5,7,8,9 91:12,13,19 93:13 94:14 96:4 104:1 110:15,20,21,21 110:22 111:4,7,17 111:23 112:2,22 113:24 114:1,1,2 114:3,4,7,12 115:9,11 response- 88:20 responses 88:3,19 94:5,11 rest 50:20 116:17 result 28:18 30:9 33:11,14,20 34:5 34:19 36:12 40:19 43:13 46:4 75:22 77:7 78:13 98:14 101:25 109:21 resultant 34:7 resulting 43:21 results 34:16 104:12 retained 13:1,4,13 retrieve 85:24 retrieves 97:23 retrieving 98:3 return 73:20 107:7 111:16 returned 111:3,5,8 111:9,12,23 112:2 112:23 114:11 returning 94:14	review 12:25 13:3 106:22 reviewed 48:21 49:2 reviewing 13:6 47:16 ride 108:12 riding 108:16 right 4:17,22 5:4 6:17 7:5,12 15:11 15:15 17:12 21:20 23:6,15 26:2 31:6 41:22 42:3,4,15 46:19 49:8 52:10 56:12,20 58:23 59:5 60:4 61:8 63:10 64:6 66:20 66:22 68:21 69:20 73:12,17 74:17 75:8,16 79:3 82:10 85:19 86:12 86:14 88:21 89:1 89:2 90:2,4,5,15 90:21 92:12,20 93:9 96:14,15 100:9 102:22 103:14 106:16 111:6 112:9 114:20 115:12 right-hand 102:8 rightmost 102:3 room 55:3,15,17 roughly 9:13 round 112:21 run 14:21,21 61:9 61:11 116:10 running 20:16 46:4 70:3 75:23 77:7 106:23 runs 61:12 113:3	115:7 satisfies 110:3 satisfy 93:15 satisfying 110:5,7 savings 23:22 saw 49:4 saying 44:5 48:3 64:13 69:17 83:21 87:3 93:4 95:18 97:2 98:1 102:14 115:2,4,20 says 15:2,13 49:11 60:17,22 61:1 62:17 70:19 76:3 79:25 80:5,8 82:24 89:21,25 90:1 91:7 92:21 112:5 scenario 23:4 scheme 54:25,25 116:16 schemes 11:10 49:20 52:1,12 53:10,13,16 54:3 55:22,25 56:1,5 58:10 59:14,15 105:14 school 14:8 scope 16:19 19:1 21:22 22:19 23:17 25:10,17 26:4,13 29:5 31:8 34:25 35:9 36:3 38:4 40:8 41:3 43:17 44:11 45:2,13 46:2 50:4 51:9 52:24 65:12 69:3 75:20 84:2,25 85:21 105:10 screen 5:25 6:16,17 seal 119:15 search 88:10 second 6:9 22:24 69:8,11 72:2,8,11 72:22 87:6 108:3 second-to-last 73:13	secondary 16:22 17:9 secondly 40:12 section 16:11 56:22 60:12,17,17 61:24 62:13,16,24 secure 31:23 32:1 39:14,15,15,18 70:2 97:9 104:10 104:18 secured 70:1 security 21:8 36:6 60:11 62:8 70:3 see 6:15,17 9:18 15:22 16:14,24 20:17 21:1,8 23:13 47:9,15 57:2 60:16,22 62:13,16 65:4 69:15 70:2,10 71:20 73:13 74:5 74:6,11 75:6 76:2 78:25 79:12 81:19 83:12 87:15,23,25 88:14 91:3 94:21 94:22 96:18 99:4 99:6,18,19,20,23 101:1,3,4 103:16 104:5,20 111:25 112:20 115:12 117:4,16 seeing 6:19 99:2 114:18 sell 11:14 send 72:16 94:11 105:25 sending 27:23 71:4 sense 65:3 107:15 sent 42:22 52:21 60:1,3 85:15 86:18 107:5 108:20 109:23 110:14 113:25 114:1,3,4 sentence 60:16,21 70:6,18 74:19 79:24 97:25
---	---	---	---	---

103:17 112:5 sentences 106:23 separate 26:11 65:8 72:7 separately 47:17 92:8 sequence 45:21 78:3 82:4 98:19 100:8,11,19 101:2 101:15,19,22,24 102:19 serpent 34:22 35:1 35:4 serve 12:7 server 97:23 98:1 98:10 99:6 service 21:25 27:7 serving 8:9 session 46:24 47:7 47:8,11,14,22 48:5,9,11,19 62:14,17,23 75:21 76:4,7,11,16,18 76:21,23 77:1,13 78:7,11,15,16,20 80:6,18 81:4 85:2 85:9,23,24,25 86:5,9 87:13 98:20,21 100:9,15 103:2,12 105:21 109:3 112:25 113:4,8,11,15 set 28:22 48:9,11 85:23 96:2 119:14 Seth 2:12 4:9 38:12 41:16 55:6 sets 59:20 setting 12:1 SHA 33:15 SHA-1 31:24 33:18 SHA-2 31:25 SHA256 31:25 sheet 118:8 120:1 shopping 68:6 short 83:4 106:5 shorthand 6:22 show 82:20 94:18	97:4 showing 6:3 shown 69:9,14 shows 71:11 78:19 100:19 101:15 111:22 side 52:16 sign 117:21 signature 109:7,9 118:12 signatures 109:22 signed 118:8 significance 67:4 signing 119:10 similar 90:1 similarly 58:14 simple 65:3 simplest 19:11 simply 42:14 96:19 single 26:8,10 92:1 110:14 114:7 single- 81:3 single-use 73:22 79:18,25 80:9,12 80:15,23,25 sitting 9:12 situation 23:18 52:13 skill 16:21 17:16,20 17:25 18:13,24 19:9 20:11 22:2,8 24:21 25:4,7 26:1 26:9 27:14,19 28:8,13,16 29:12 29:20,24 30:3,6 30:14,20,24 31:15 32:11,18 33:12,21 34:21 35:2,5,12 35:17,22,25 36:16 36:22 37:1,5,19 37:23 38:17 41:5 41:8,13,19 42:18 42:24 43:3,11 44:5 45:9,24 46:3 46:9 49:13,23 51:19 52:7 55:8 65:3,14 76:6	80:15,17,23 81:2 81:6,9 88:7 90:17 93:5,8 94:25 96:7 104:5,8,19 105:15 116:18 117:9 skills 11:15 slightly 43:7 92:4 slindner@bclgpc... 2:16 slot 57:24 small 107:20 smaller 31:20,22 55:23 smart 14:21,22 smartphone 67:22 socket 70:2 solution 25:22 34:19 solutions 11:16,17 11:18 somebody 117:9 someone's 55:3 soon 41:16 sorry 9:5 10:5 23:3 46:10,12 55:3,6 59:3 63:6 73:9,11 84:11 92:13,15,18 95:1 98:21 101:7 104:25 107:12 113:14 116:10 117:3 sort 4:17,21 68:5 75:7 sound 4:23 5:8 17:18 Sounds 117:17 source 115:13 space 50:12 54:17 54:20 55:24 speak 13:12 spec 58:17 specific 21:4,6 45:5 49:10 84:5 86:19 specifically 68:8 101:8 104:18 specification 54:24 54:25 56:5 58:17	58:22 60:23 61:2 62:24 90:9 93:20 93:22,25 94:7,8 95:5 96:2,3,5,19 97:3 111:9 specifications 13:10 30:1,4 33:19 36:5,7 40:13 51:15,20 52:8,17,18,20 53:1,8 54:4 55:1 57:17,21,22 58:8 58:9,12,15,24 59:10,20,23 61:5 61:23 62:23 65:8 65:13,16 66:1 94:1,2 96:11,22 97:6,15 104:20 111:3 115:17,21 116:1 specified 96:3 specify 79:8 88:3 specifying 11:16 20:3 specs 59:7 63:3 80:18 spend 42:4 spent 9:19,23 10:1 10:9,15 SSL 70:2 SSL/TLS 69:12,17 standard 1:16 16:13 33:25 34:4 36:1 57:13 90:23 104:19 standardized 104:10,17 standards 30:1,19 stands 65:19 start 77:25 97:24 99:8 101:23 started 14:8 89:7 starting 98:17 113:2 starts 56:18 101:12 101:19 state 73:10	stated 113:20 114:20 115:3 statement 46:13 States 1:1 53:24 statistical 43:20 44:16 stenographically 119:8 step 34:10 57:16 73:21 112:8 steps 26:17 96:18 sterling 12:11 storage 25:12,13 stored 47:11 storing 48:4 story 79:13,13 stream 44:19,19,22 45:10 Street 2:5 stretch 12:4 106:12 stripe 50:24 56:24 56:25 95:16 Stuart 1:13 4:3 118:3 120:4,21 subject 117:13 submitted 5:11 7:12 59:20 submitting 104:1 Subscribed 120:22 subscript 75:13 subsequent 43:22 subway 108:7,12 108:16 successfully 48:15 sufficiently 43:21 suggestion 64:25 suggests 81:3 suitable 35:6 104:3 suite 31:24 supervision 119:10 supplementary 18:10 supported 59:24 70:25 supports 58:22 sure 4:24 6:10 14:10 19:11 25:18
---	--	--	--	---

45:7 46:20 67:1 71:2 73:25 77:3 83:5 86:15 100:17 100:22 114:19 suspect 94:22 switches 116:16 sworn 4:4 120:22 symbols 69:15 synched 86:25 91:14 system 25:5,8,12,15 26:2,5,8,11 27:4,7 27:13 49:14,16 51:6,13 53:24 55:12 67:11,14,16 69:10,24 70:10,15 71:3,10,12 72:3,9 72:15,19,25 73:4 73:8,16,22 74:2,3 74:6,7,8,13,15,16 81:23 84:20,21 85:24 96:10 97:10 105:8 108:16 109:24 117:11 systems 11:3 25:20 26:11 27:12,25 46:7 49:22,24 51:6,12 55:7 56:2 61:13 90:10 96:9 104:3 105:12	74:20 79:24 109:4 talks 49:10 90:9 104:6 tasks 25:24 TC 112:17 technical 8:12,13 8:16 11:6,25 technique 104:12 technologies 41:8 41:11 technology 11:12 69:23,25 107:12 tell 9:24 42:18 43:2 80:3 105:12 106:1 106:24 temporary 113:6 ten 12:22,23 term 17:21 18:1 22:3,9 24:22 25:5 27:15 28:9,14 32:12 35:23 36:14 36:23 37:2,6,20 38:18 39:24 41:6 41:14 42:17,19 43:9 47:2 49:14 49:16 69:5 71:15 72:13 76:11,12 88:9 93:7 94:23 95:12,19,22 110:6 116:19 117:1 termed 109:21 terminal 23:21 42:22 43:4 50:7 51:17,21,25 52:10 52:16 54:5,14,15 54:17,21 55:16,17 56:19 57:19,24 58:3,13,18 60:2 61:18 71:7 88:13 88:19 91:15 94:3 94:4,5,10,12 107:7,20 108:2 112:5,11,14 116:11,15 terminals 50:23 54:3 57:1,22 88:6 107:15 108:21	109:8 terms 14:24 17:13 17:15,17 19:24 20:1 42:10 45:3 46:23 53:5 89:20 90:10 99:1 117:4 testified 4:6 testify 4:4 testifying 13:22 testimony 86:17 118:5,6 119:7,8 testing 11:17 tests 43:20,23,24 44:7,16 thank 48:1 59:18 87:21 thanks 4:12 theories 64:15 thing 5:8 27:12 53:18 59:17 76:20 things 4:18 13:10 51:14,14 52:2 59:15 95:9 think 7:18 12:10 14:7 16:10 17:11 20:1,25 23:19 25:1 34:13,17 45:14 48:2 57:16 59:19 63:15,19,23 64:16 71:11 73:6 74:4,11,25 77:1 77:19 79:7,13 80:19 81:4 85:1 86:11 106:3 113:23 thinking 85:22 third 102:4 thorough 114:17 thought 23:18 77:18 92:18 thousand 24:6 three 97:19 112:11 three- 22:23 three-digit 21:8 24:1,5,8,9,14,17 throwing 34:20 time 1:16 8:16,18	9:8,18,22 10:1,4,7 15:8 19:12 20:17 20:21 23:5 31:24 42:5 47:23 50:14 53:24 54:8,10 55:15 59:22 86:9 108:8 time-to-live 86:3 times 65:1 timestamp 84:21 84:22 85:1,3,7,10 86:1,7 87:3,7,8 titled 56:22 TLS 70:3 today 4:11 5:4 6:22 7:7 9:12 14:2 15:6 42:15 46:19 today's 6:15 token 73:15 74:21 tonight 106:15 top 12:20,22,23 68:6 75:1 113:19 114:24 Track 50:10,10,11 111:5 114:11 trade 11:4 TRADEMARK 1:1 traditionally 110:17 transaction 23:24 24:19 26:15,19,20 26:20 27:1,2,5,9 27:10 39:12,18 42:23 48:17,19 50:7,19 55:20 57:5,20 76:20,24 78:6,12 80:1,10 80:11 82:25 92:2 93:7,9 94:24 98:3 100:13 103:1,11 104:16 107:5,19 107:21,22,25 110:12 112:6,15 112:16 113:7,13 115:23 116:3,17 transactions 21:12 27:4,7 48:10 50:2	52:14 57:25 58:1 58:22 59:24 94:17 94:20 95:7 104:4 104:11,18 107:16 114:10,15 115:14 transcript 119:6 transcription 118:6 transfer 57:5 transferring 50:9 50:22 72:12 transformation 54:24 transformed 54:16 54:20,23 55:22 transient 25:13 transit 11:7,11 12:24 108:3,6,19 108:21,25 109:8 transmit 57:1 73:15 transmits 84:21 transmitted 75:15 81:18 86:10 transmitting 74:20 transport 50:7 70:2 traveling 108:24 TRIAL 1:2 triple 33:1 34:6,14 37:12,12,16 102:7 113:11 true 104:13 118:5 119:6 truncate 34:20 truncates 31:20 truth 4:5,5,5 try 46:21 96:25 97:1 106:12 trying 4:21 43:1 70:24 77:19 92:6 106:11 114:16 turn 21:7 46:14 63:24 90:25 106:19 two 21:10 24:7 25:19,19 27:23,24 40:9 47:17 64:14 64:14 65:1,18
---	---	--	---	--

T

72:12,21 91:23 92:7 95:9,13 97:19 103:8,18 105:20 108:23 111:5 113:23 115:5 type 20:3 56:9 types 14:15 91:23 92:7 112:1,11 typewriting 119:9 Typically 110:11 typo 74:4,23 94:22	14:24 15:13,24 48:21 49:6 66:12 74:1 77:23 93:3 100:17 understands 18:4 understood 17:17 18:1 22:3,9,11 24:22 25:2,8,11 27:20,22 28:9,17 31:18,23 32:5,12 32:15,19 33:21,24 34:9,21 35:13,23 36:4,5 37:6,8,11 37:20 38:18,21 41:6,13,20 42:19 43:11,12 49:14 95:19,21 undertake 25:24 undertaken 26:17 unfamiliar 35:1,3 35:10 36:8,20 Union 12:3 unique 21:9,18 22:1 23:14 24:2 85:3 uniquely 22:16 unit 25:12 87:18 United 1:1 53:24 units 88:21 unpatentability 64:15 unpredictable 42:17,23 43:4,5,6 43:8,10,15,18 44:9,15,17,18,20 45:3,5,19,20 46:8 75:18,22 76:4,8,9 76:11,18,21,25 77:2,5,6 78:15 98:20,23 100:9,14 100:16 103:2,11 UNREADER 98:2 98:23 unrelated 24:4 unsolicited 72:16 upwards 53:14 use 8:1 15:9 30:19	31:3 32:4,17 37:21 53:10 55:2 55:9 57:8,10 78:13,22 81:4 84:18 86:6 98:9 105:14 108:3,23 109:2,17,19 useful 43:22 44:16 85:4,11,12,13,13 85:17 86:19 108:1 usefulness 30:18 user 48:7 49:11 uses 22:3 24:22 28:9 32:12 34:4 42:17 43:5 74:19 83:11 88:9 90:22 92:8 93:7 101:22 109:20 usually 89:9 109:21 utility 97:16 utilized 90:19 utilizes 57:13	verify 109:8 verifying 103:18 version 59:8 75:3 105:25 video 4:15 5:5 view 18:12 40:19 60:7 Visa 9:21 12:2,18 13:6 21:18 49:18 50:16 51:1 52:25 58:14,14 114:9 115:10,14,22 116:3,6,10,14	38:13 71:1 93:12 107:1 109:4 weaknesses 32:3 welcome 87:22 went 78:23 96:24 108:4 weren't 29:10 WHEREOF 119:14 whichever 114:13 115:4 wifi 28:2 41:9 70:4 WILLIAMS 2:4 6:10 8:4 9:15 12:8 13:5 14:14 16:6 17:10,23 18:2,17,25 19:25 20:15 21:21 22:6 22:10,18 23:16 24:16,25 25:9,17 26:3,12 27:17 29:4 30:8 31:7,17 32:21,23 33:23 34:24 35:8,15,20 36:2,10,19,24 37:3,7 38:3,12,19 40:7,22 41:2,15 41:18 42:6,20 43:16 44:10 45:1 45:12 46:1,25 49:15 50:3 51:8 51:23 52:23 55:4 56:4 57:15 63:14 65:12 66:2 67:19 68:13 69:2 72:4 73:2 74:18 75:19 76:10 79:4,17 81:1,12 82:17,23 83:5 84:1,24 85:20 86:23 95:11 96:23 99:15,24 100:10 102:23 103:15 104:24 105:9 110:23 113:9,16 116:5,22 117:15,18,20 win 12:2
U			W	
U-M-A-C 37:2 U.S 1:6 7:4 12:24 20:19,22 50:5,14 50:19,20 54:8,10 55:15 57:8 UK 11:5 39:19 UMAC 37:2 UN 75:13 unannotated 75:3 unclear 23:19 47:12 65:17 71:15 UNCLOUD 66:5,7 66:10 76:22,25 78:13,22 97:23 98:2,4,9,22 understand 4:25 5:2 6:23 7:11 15:16 16:17 18:11 18:14 19:3,4,10 20:12 25:18 29:13 29:14 30:15,17,20 31:16 33:13 35:18 44:6 45:24 46:3 47:21 48:2 64:21 64:23 65:14,15 66:4,11 67:18 70:24 76:8 78:17 79:2,6 80:15,23 81:3 88:8 92:6 93:6,8 96:8 105:15 114:16 116:19 understanding		v 1:8 13:23 120:2 valid 92:1 113:7 validated 107:4 validates 98:2 validating 100:1 103:21 validation 92:23 105:16 value 9:2 29:6,16 29:18 33:8 37:9 38:25 42:25 43:1 48:6 55:19,20 77:15,16 81:7,11 105:3 values 98:4 103:19 variants 50:14,24 varied 56:9 various 12:6 16:18 49:24 verbal 5:7 verification 48:10 48:12,13 49:5 verified 107:4	wait 4:19 want 23:21 55:4 106:4 wanted 18:22 62:6 71:16 73:25 114:19 wants 83:17 Washington 2:6 wasn't 8:5 32:4 66:5 102:24 wave 58:2 108:5 116:7,11 way 7:25 13:19 28:10 29:12 31:21 32:7,17 37:15 38:7 44:21 54:16 56:3 61:4 62:23 63:25 65:22 76:15 88:24 90:13,17,20 97:12 104:15,22 105:6,19 110:7 113:23 114:6,13 ways 29:23 30:5 40:9 52:12 55:25 72:21 105:14 113:23 we'll 15:5 38:16 we're 11:5,25 14:2 37:11,15 41:24 49:17 59:4 64:8 71:4 87:12 103:7 we've 22:5 24:23	

wireless 41:6,7,9,10 41:12 68:25 69:5 81:23	68:7 73:24 83:14 97:20	1023 52:18 58:1	111:5 114:11	4-byte 45:15
wish 11:13 61:13	yield 104:12	1023-1029 3:7	115:17 116:12,13	4-byte-long 45:10
witness 8:9 104:25	York 2:14,14	1026 56:13 115:18	2.1 59:8	4.2 57:13,22 58:22
106:6 117:14,21	Z	1027 115:18	20 9:6,14 10:9,15	58:24 59:5,19
119:14 120:4	zero 44:1,1	1029 52:19 58:1	33:20 64:20	60:9
wondering 92:8	Zip 50:18	1037 90:6,9	120:23	4:14 117:23
word 26:5 27:25	Zoom 1:14	104 73:23	200 2:13	40 112:17
32:16,17 33:14	0	105 90:25 91:4	20001 2:6	41 112:17
52:5 68:2,4 69:4	0 45:17	106 73:15 88:11	2003 7:25	42 3:4 73:10
77:20 86:13 89:3	0's 44:19,20,22	11:00 106:15	2012 17:17,20	43 49:10 69:8 70:7
89:16 92:4	45:19 102:1	110 73:22 74:3,7,10	20:11 22:9 25:4	70:13,18 71:17
wording 91:23 92:8	1	74:13,15,22 75:6	27:14 28:13 29:13	44 94:17,18,21,22
words 4:22 5:6	1 10:7 16:18 50:10	117 93:17,21 95:4	29:20,25 30:3,7	45 103:25
64:8	59:9 73:1	96:6	30:25 31:16 32:20	46 3:5
work 7:18 8:6,20	1's 44:19,20,22	118 73:22 96:7	34:13,23 35:3,7	48 49:11
9:1,4,11,13 10:2	1,000 24:7	13 14:25 15:1,3,15	35:14,19 37:6	49 113:3
10:12,18,21,24	1.5.4 56:19	132 97:17,20,25	41:6,14,19 42:19	5
11:19,23 12:2	1.5.6 57:9	99:1,4,21 100:24	49:14,23 50:1,5	5 10:4
85:4,11,17 86:19	1.5.7 56:22	103:17	55:2,9 56:2	5.4 12:11
87:9 93:24 116:15	1.A-2 68:19,22	133 104:7	202.639.7700 2:7	50 47:4 79:12,15,18
worked 7:20 8:19	1.A-3 73:4	14 1:15 4:1 14:25	2024 1:15 4:1	79:20
9:20	1.A.1 73:6,6	15:1 16:12 116:20	119:16 120:3	500 73:20
working 9:9,19	1.E 88:12	117:1,6,7 120:3	2027 119:17	51 73:11,14 74:8
10:10,16	1.E-1 88:12	142 62:11	208 80:1	510 73:21
world 50:21 57:20	1.E-3 87:15 93:12	15 47:3,16 49:7,9	21 76:2	52 3:7
wouldn't 10:11	113:20,22 114:14	15th 119:15	212.951.1000 2:15	53 47:18 66:15,19
38:10 45:20 71:8	114:21 115:3,6	16 34:4,5 101:25	22 103:9	87:14,20
86:19	10 10:1 106:14	102:2,3	24 86:5	54 47:18
writing 5:6 14:6,10	10,032,171 1:7 7:5	16-byte 34:19	24th 2:13	55 47:4 112:22
written 75:12	100 73:16 74:2,6,8	160 33:20	25 119:17	56 112:20,22
wrong 65:20	74:12,19	17 94:15	28 56:17 103:9	57 112:20,22
X	10016 2:14	171 7:8 12:25 17:2	3	58 71:17,23 72:10
x 1:3,11	1009 3:3 79:7 95:7	17:13 22:3 24:22	3 16:21 59:9 90:8	59 72:14
Y	99:11 101:1,11,15	28:9 31:13 32:8	115:17 116:11,13	6
Yeager 5:19	1011 3:4 42:11,12	32:12,16 33:2,10	304 112:8	6 44:22 74:11
Yeah 79:12 101:18	78:19 79:1,8	33:13 63:9 114:24	306 67:25	60 3:6
117:6	92:16 95:8	116:20,23 117:5	308 97:23 98:1	60s 14:9
year 10:9,11,19	1012 3:5 46:14	18 16:16 17:3	31 116:20 117:1	61 100:25 101:4,5
12:10	106:20,21	182 110:1 111:14	35 111:25 112:4	62 87:19
years 9:6,14,25	102 92:10	114:22	37 90:1	63 113:3
10:8,14 13:11	1020 3:6 60:8,13	183 113:18 115:12	38 89:19,25 112:13	64 44:22 92:11,14
14:16	62:7	198-1 36:1	4	64-bit 29:9,10 33:8
Yep 62:20 66:18	1021 90:7,8	2	4 15:4 16:22 45:17	65 106:22
		2 16:19 50:10,11	45:21 59:9 96:1	68 101:3,6
		58:17,19 59:7,9	96:17 116:14	69 101:12,19,23
		60:9 62:8 106:21		

7 7 66:20 67:17,24 68:11 69:9 72:24 74:5,12 75:2,3,8 91:25 111:24 112:4,20 70 101:25 700 2:5 702 74:22 70s 14:9 71 101:7,13,14,20 102:2,15 103:8 77 92:17,20 7816 88:7 90:23 79 3:3				
8 8 34:7,12 60:12 61:24 75:4 113:2 8-byte 29:8,10 33:8 81 74:9 83 46:7,10 82:19,20 82:24 87 69:7 73:11,19 99:20,22,25 88 66:16				
9 9 76:1 9:58 1:16 4:1 93 114:24 9347 1:25 120:5 94 79:10 83:8 84:9 84:12,15 113:19 95 88:16 89:3 90:3 90:7,11 96 75:10,11 81:15 82:7 99 60:13,21 9F01 53:12 9F37 43:2 9F50 53:14,17,18 9F7F 53:12				

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.

28-6-29.

(Date)

Stuart Fiske

(Signature)

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

MASTERCARD INCORPORATED AND MASTERCARD INTERNATIONAL
INCORPORATED,

Petitioner,

v.

OV LOOP, INC.,

Patent Owner.

Case No. IPR2023-01289
Patent 10,032,171

**ERRATA SHEET FOR THE JUNE 14, 2024
DEPOSITION TRANSCRIPT OF STUART FISKE, PH.D.**

I, Stuart Fiske, do hereby make the following corrections to my June 14, 2024 deposition transcript:

PAGE	LINE	CHANGE/CORRECTION	REASON
51	1	"MasterCard" should be "Paypass"	Misspeak
53	12	"9F7F" should be "9F4F"	Misspeak
59	8	"contactless" should be "contact"	Misspeak
81	22	"provision" should be "provisioning"	Misspeak
95	15	"Magstripe" should be "M/Chip"	Misspeak
114	1	"response" should be "cryptogram"	Misspeak

I state under the penalty of perjury that, except for any corrections noted above, the transcript is an accurate record of the statements made by me.

Date: 28-6-28

/s/ Stuart Fiske

Stuart Fiske