IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
FORT WORTH DIVISION

THOMAS E. PEREZ [now R. ALEXANDER ACOSTA], Secretary of Labor,

Plaintiff,

v.

ASSOCIATION OF PROFESSIONAL FLIGHT ATTENDANTS,

Defendant.

Civil Action No. 4:16-cv-1057-A

APPENDIX OF EVIDENTIARY MATERIALS IN SUPPORT OF APFA'S MOTION FOR SUMMARY JUDGMENT

ANDREW D. ROTH
D.C. Bar No. 414038
ADAM BELLOTTI
D.C. Bar No. 1020169
ROBERT ALEXANDER
D.C. Bar No. 465673
Bredhoff & Kaiser, P.L.L.C.
805 Fifteenth St. N.W., Tenth Floor
Washington, D.C. 20005
Tel: (202) 842-2600
Fax: (202) 842-1888
Email: aroth@bredhoff.com
Email: abellotti@bredhoff.com
Email: ralexander@bredhoff.com

SANFORD R. DENISON
Texas Bar No. 05655560
Baab & Denison, LLP
6301 Gaston Avenue, Suite 550
Dallas, TX 75214
Tel: (214) 637-0750
Fax: (214) 637-0730
Email: denison@baabdenison.com

Attorneys for Defendant Association
of Professional Flight Attendants

TABLE OF CONTENTS

Respectfully submitted,

ANDREW D. ROTH*
D.C. Bar No. 414038
ROBERT ALEXANDER*
D.C. BAR No. 465673
ADAM BELLOTTI*
D.C. Bar No. 1020169
Bredhoff & Kaiser, P.L.L.C.
805 Fifteenth St. N.W., Tenth Floor
Washington, D.C. 20005
Tel: (202) 842-2600
Fax: (202) 842-1888
Email: aroth@bredhoff.com
Email: ralexander@bredhoff.com
Email: abellotti@bredhoff.com

Sanford R Denison
SANFORD R. DENISON
Texas Bar No. 05655560
Baab & Denison, LLP
6301 Gaston Avenue, Suite 550
Dallas, TX 75214
Tel: (214) 637-0750
Fax: (214) 637-0730
Email: denison@baabdenison.com

Attorneys for Defendant Association
of Professional Flight Attendants

* Admitted Pro Hac Vice

Dated: August 25, 2017

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on the 25th day of August, 2017, the above and foregoing Appendix of Evidentiary Materials in Support of Motion for Summary Judgment was served on the following Plaintiff's counsel of record electronically by email transmission and by overnight mail, as authorized by Federal Rule of Civil Procedure 5(b):

Brian W. Stoltz
Assistant United States Attorney
1100 Commerce Street, Third Floor
Dallas, Texas 75242-1699
Telephone: 214-659-8626
Facsimile: 214-659-8807
brian.stoltz@usdoj.gov

Sanford R Denison
SANFORD R. DENISON

Alderson®

COURT REPORTING

Transcript of **Stephen J. Willertz**

June 13, 2017

Perez v. Association of Professional Flight Attendants

Alderson Reporting
1-800-367-3376
info@aldersonreporting.com
http://www.aldersonreporting.com

Alderson Reference Number: 70651

Page 1

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
FORTH WORTH DIVISION

- - - - - - - - - - - - - - - - - - X
THOMAS E. PEREZ, Secretary of :
Labor, [now EDWARD HUGLER, :
Acting Secretary of Labor], : Civil Action No.
Plaintiff, : 4:16-cv-1057-A
v. :
ASSOCIATION OF PROFESSIONAL :
FLIGHT ATTENDANTS, :
Defendant. :
- - - - - - - - - - - - - - - - - - X

Washington, D.C.
Tuesday, June 13, 2017

Deposition of STEPHEN J. WILLERTZ, a witness herein, called for examination by counsel for Defendant in the above-entitled matter, pursuant to notice, the witness being duly sworn by MARY GRACE CASTLEBERRY, a Notary Public in and for the District of Columbia, taken at the offices of Bredhoff & Kaiser, 805 15th Street, N.W., Washington, D.C., at

Page 2

9:53 a.m., Tuesday, June 13, 2017, and the proceedings being taken down by Stenotype by MARY GRACE CASTLEBERRY, RPR, and transcribed under her direction.

Page 3

APPEARANCES:

On behalf of the Plaintiff:

BRIAN W. STOLTZ, ESQ.
Assistant United States Attorney
1100 Commerce Street, Third Floor
Dallas, Texas 75242-1699
(214) 659-8626

and

TAMBRA LEONARD, ESQ.
JENNIFER FREY, ESQ.
CLINTON WOLCOTT, ESQ.
U.S. Department of Labor
200 Constitution Avenue, N.W.
Room N-2474
Washington, D.C. 20210
(202) 693-5744

Page 4

On behalf of Defendant:

ANDREW D. ROTH, ESQ.
ADAM M. BELLOTTI, ESQ.
Bredhoff & Kaiser
805 15th Street, N.W.
Washington, D.C. 20005
(202) 842-2600

ALSO PRESENT:

KATHERINE ANDREWS, Summer Associate

Page 13

A. I apologize, but I don't specifically recall. I believe that I have, but I can't recall specific cases. What stands out in my mind more are the cases that I testified in the grand jury and in criminal trials.

Q. Were those election cases?

A. Those were criminal cases.

Q. Criminal cases. So there were no criminal penalties for election violations?

A. That's right. Those were all criminal cases.

Q. Any civil depositions or case testimony you can recall under Title IV of the LMDR?

A. I believe that I have been deposed in election cases, but I can't recall a specific one.

Q. Any cases involving electronic balloting?

A. No.

Q. How about mail balloting?

A. Not that I recall.

Q. So in 2012, I think, you've testified you became the head of the office, you came to headquarters in your office of field -- director of

Page 14

the office of field operations.

What are your primary responsibilities in that position?

A. Yes. I oversee and direct OLMS enforcement programs throughout our field offices around the country.

Q. So that would include a number of different programs, including the enforcement of Title IV regarding union elections?

A. Yes.

Q. And you have a staff at headquarters that works under you?

A. Yes. I don't have any direct reports at headquarters. The four regional directors that are located around the country report to me, the computer cadre enforcement coordinator, Bill Mitchell, reports to me, and I have a special assistant that reports to me.

Q. Who is that?

A. Her name is Antoinette Dempsey. She's located in Atlanta.

Q. So you have regional directors underneath

Page 15

you. You also have district directors of the various field offices around the country; is that correct?

A. Yes. The district directors report to the regional directors.

Q. They report to the regional directors?

A. Yes.

Q. When a complaint is filed by a union member concerning alleged problems or irregularities with an election, those are typically -- or they're required to be filed with the district director or the district office where the union election took place or is headquartered or how does that work?

A. They can be -- election complaints can be filed with any representative or employee of the Department of Labor.

Q. I see.

A. They could be filed with somebody from OSHA or MSHA. And we hope, in those instances, they make their way to OLMS fairly quickly.

Q. Right.

A. So they don't necessarily have to be filed with a district director. They could be filed with

Page 16

any of us.

Q. But, typically, they are filed with district directors?

A. Often they are.

Q. Sometimes they're filed with the national office directly?

A. Yes, sometimes they are filed with us in the national office.

Q. When they're filed somewhere else, are they always referred to the district?

A. Yes. The district office where the labor organization is physically located has jurisdiction to investigate that election complaint. So we would get that complaint to the district director in the particular field office as quickly as we could, so that the district director can open a case, assign it, and start investigating.

Q. Now, are there some cases, election challenges to union elections that are handled exclusively at the local level, at the district level, or do you get involved in every single election complaint?

Page 17

A. I don't necessarily get involved in every election complaint. The majority of election investigative work is done in the field. I may be contacted if there is a question or a problem or a scope issue or a jurisdictional issue or some novel question that needs to be answered.

Q. So in routine cases, are district directors at liberty to dispose of the complaint on their own, or do they need sign-off from headquarters in every case?

A. Let me explain how this works.

Q. Please.

A. So the field office opens an investigation. They conduct the investigation and write a report of investigation that is sent to the division of enforcement in OLMS headquarters. Sharon Hanley, the chief of the division of enforcement, she's in the office right next door to me. Then the case is assigned to one of the investigators in the division of enforcement, and that division of enforcement investigator reviews the report of investigation.

Page 18

The case is also assigned to an attorney in our solicitor's office who reviews the report of investigation, and then a case meeting is scheduled. And I attend those case meetings, as well as Sharon Hanley and whoever the DOE -- that's the Division of Enforcement -- investigator is and the attorneys from SOL. And we discuss the case and make a case determination.

Q. Now, was this case handled differently in that you sort of took more of a -- I mean, you were ultimately in charge of the investigation of this case; is that fair to say?

A. I wouldn't say I was in charge. I think, technically, the district director was still in charge of the investigation. But, yes, I took more of a hands-on approach to this investigation.

Q. And why was that?

A. Because it was an Internet voting system election case, and we were working on guidelines at the national office for electronic voting systems. And I decided to get involved and sort of monitor the results of the investigation as they came in.

Page 40

A. -- do we need to investigate this or not? I would say yes.

Q. If he's raised it, it's fairly encompassed within the scope of the investigation?

A. Yes.

Q. Let me go back to -- I know you said you didn't read it, but I still have one question about Exhibit 4.

On page 5 of the questionnaire, Bates stamp number 143 --

A. Yes.

Q. -- if you go down to the second to last paragraph of this questionnaire, it says at this page, "Morales stated that he couldn't single out any particular evidence to support his statement that he felt that APFA violated" -- and then skip integrity -- "the ballot secrecy of section 401(e)."

Does that surprise you?

A. The sentence goes on to say, I should say, "Other than his visibility to observe the ballot process."

Q. Right. Is there something about observing

Page 41

the ballot process that would lead a member to think there is a secrecy issue?

A. I don't know, and I can't speculate what's going on in his mind.

Q. I don't want you to speculate.

A. But, again, from an investigative policy standpoint, if a member raises an issue, maybe the member can't see any particular evidence. And the fact that the member can't see it causes them to suspect that it's not secret, that wouldn't be unusual.

Q. My question really is not so much of, you know, whether sort of it's a fair game for investigation at that juncture. My question is really different, is does it surprise you that this complainant couldn't provide any basis or evidence for his concern that ballot secrecy had been violated? Does that surprise you?

A. No.

Q. Why does it not surprise you?

A. Because the investigation noted that there was no tangible record or way for any candidates in

Page 42

this particular election, to observe the votes as they were recorded by the electronic system, or the way that they were tallied, and verify the accuracy or look inside the system in any way, shape, or form to make any sort of assessment as to whether or not votes and voters could be connected. There is just no way. So it wouldn't surprise me that a member might allege or suspect that this system wasn't specific in filing in a complaint.

Q. Okay. Before I leave the subject of the interview with Morales, do you know whether any other rank and file union member was interviewed in connection with your investigation of this complaint? I say "rank and file" because I know you interviewed union officials --

A. Yes.

Q. -- who were involved in the election. But any members who weren't part of the election, you know, part of the administration of the election. Did you interview anybody similarly situated to Morales regarding their concerns about observability or secret ballot violations?

Page 45

allegations. Read that. I'm going to have a series of questions --

A. Yes.

Q. -- about how you got to this result later on in the deposition. But for right now, my question to you is, are you aware of the complainant in this case, Mr. Morales, or any other rank and file union member ever expressing a concern or a believe that, to quote paragraph 21, that "The system stores and maintains member-identifying information and voting records on two servers in a way that could allow individuals with access to both of the servers to identify how a member voted"?

A. I didn't understand the question. Did --

Q. Did Mr. Morales, or any other rank and file union member ever express that concern to you, to your knowledge? To you or to a member of your investigatory team in this case? Did Mr. Morales ever say, Here's why I feel that ballot secrecy is a problem, because I have a sense that the system stores member information in a way that could allow individuals with access to both of the servers to

Page 46

identify how a member voted?

A. Okay. I'm not aware that Mr. Morales would ever have said that. I do know that he alleged a lack of voter secrecy.

Q. Correct. But he never raised this particular concern as the basis for why he was concerned about ballot secrecy?

A. I don't believe that he ever articulated anything about two servers.

Q. And correct me if I'm wrong, but, I think, you said you would find it highly unlikely that he would have enough knowledge about how the system worked that he would form such a belief?

A. Yeah, I don't know. I don't know to what degree he may have read up on BallotPoint's system. I do know that they have a website and there are some description of their system, but I don't know that.

Q. But you have no information to support --

A. No.

Q. And certainly those -- to your knowledge, that concern was ever expressed by him or any other rank and file member to you or any of your

Page 47

investigators?

A. I don't have any information on that, no.

Q. All right. As I think we have just reviewed, there was what, I think, it's fair to characterize as a fairly conclusory allegation in the complaints here, that ballot secrecy was a problem.

So were you -- at what junction did you get involved in investigating that and other allegations of the complaint?

MR. STOLTZ: Object to the extent that that characterization may be argument.

But go ahead.

THE WITNESS: Yes, I reviewed the documents that BallotPoint and APFA initially provided.

BY MR. ROTH:

Q. You're getting ahead of me. So let me do it this way, actually. And that was a very inartful way for me, but your answer to my inartful question has led me to ask you to mark this as Exhibit 6 --

(Willertz Exhibit No. 6 as marked for identification.)

Page 70

obtain the data in the voter database.

Q. You mean the member database?

A. The member database. I sometimes refer to it as voter database because it's --

Q. Oh, voter rather than the vote.

A. Yes.

Q. I got it. What BallotPoint calls the MRNS?

A. Yes.

Q. All right. And what exactly transpired at the demonstration that heightened your interest in obtaining that?

A. It was clear that information, you know, was passed from one server to the other, and then to the member and to the election administrator, Cindy Horan, that appeared to us -- or at least made us suspect even more that there was a link between the voter and the vote contained in the data that was in this database.

Q. You mean there was data that if -- in the two servers --

A. Exactly.

Page 71

Q. -- that could be combined?

A. Exactly. That if we -- if BallotPoint provided the member table or the voter table, that there was going to be information in there that would allow us to link the voter and the vote by comparing it against the vote table.

Q. When you say "provide the table," in other words --

A. The data in the table.

Q. -- create a table that would show the data that was in the member database?

A. I --

Q. I mean, I think you agreed before, and let me just clarify for the record, you're not maintaining that BallotPoint had already generated and had in their warehouse somewhere a table that had all that data in it. You were looking for them to generate that table?

A. Again, I don't know. And I'm not a technical expert, so I don't know whether it needed to be generated. What I suspected was the data was there. In what format it existed and whether it

Page 72

needed to be reformatted or a new database needed to be created to release it, again, that's over my head in terms of technical expertise. But it appeared that the database contained IP addresses from which the members voted, and it appeared to contain at least an eight-hour window on a particular date as to when the member voted.

At that point, we didn't know for sure whether or not there might even be a more detailed time/date stamp in the database, but we knew, based on the demonstration, there was at least an eight-hour date/time stamp window.

Q. So you wanted to see that data because --

A. We wanted to see that data.

Q. If that data were provided to you through software changes, or whatever had to be done, then you didn't particularly care. You just wanted the data?

A. Exactly.

Q. You didn't focus on what needed to be done?

A. Yes.

Page 73

Q. You didn't question or not question their claims of what was involved. You just wanted the data?

A. Yes.

Q. And you were hell bent on getting that data?

A. Yes. We served the subpoena and --

Q. Right.

A. After that.

Q. Before we get to the subpoena, let me mark 9.

(Willertz Exhibit No. 9 was
marked for identification.)

BY MR. ROTH:

Q. Can you identify this document?

A. Yes. This is written follow-up request that was made after the demonstration. And, as is indicated in the first sentence, I made the request verbally during the meeting that was the demonstration.

Q. And the request being, "I want the table entitled 'officer election members' and all data it

Page 74

contains (regardless of election) during the balloting period."

Okay. And correct me if I'm wrong, but ultimately, BallotPoint howled and you backed off the request for all elections. You just wanted the data for that particular election?

A. Yes. And if it helps to explain --

Q. Please.

A. The reason we asked regardless of the election, we had, in the previous year, conducted another election investigation involving an electronic voting system that didn't involve this union, and it didn't involve BallotPoint, but the investigation disclosed that the data was sequenced chronologically in order of receipt of votes across all the elections that the company was administering or conducting at the same time.

Q. Okay.

A. And we didn't know if that, perhaps, was similar in any way to BallotPoint. But just to preserve the possibility that there may be some chronological sequencing of rows of data, that's why

Page 75

we initially requested it that way.

Q. Now, this, like all these correspondence back and forth, are coming from or to Michelle Hussar. But you were involved in the framing of this request, correct?

A. Yes.

Q. And it says you want the information, "even if an override of the system is necessary."

Were those your words?

A. I don't know who drafted those words. It might have been. Again, I apologize for any technical shortcomings. I don't know necessarily what an override of this system is.

Q. You can't testify in terms of what your thinking was in saying that?

A. No. In re-reviewing this letter now, I think it was a poor choice of a word in the request, "override of the system." I don't even know what that would mean.

Q. Well, I think you testified previously that the source code that -- software source code that's used in an election is part of the system,

Page 76

right? I mean, the system doesn't stand apart from the application software code that's -- I mean, is your technical understanding at least that great, that you would know that's part of the system?

A. I think what I understand is that there is a whole lot of detailed software code that tells the system what to do.

Q. Right. When you say, "tells the system what to do," I mean, it is part of the system, right?

A. It runs the system.

Q. It runs the system?

A. Yes.

Q. Okay.

A. And, again, my not technical knowledge is that the software code can be changed. You could change a line of code that would alter the way a system runs. There may be a line of software code that says when a voter pushes number 1, record a vote for the candidate identified as the number 1 candidate, for example. And there would be a way to change that line of software code to make it number 2, and so that would alter the way the system runs.

Page 77

Q. So would it be fair to say, then, if you change the code, you're changing the system?

A. It's possible, yes.

Q. I mean, the system, presumably, is written in a way -- the code is written in a way that if somebody votes, presumably, for candidate 1, that's how it's recorded?

A. Yes.

Q. But you're saying it's your understanding that, you know -- you don't know exactly from a technical standpoint how, but it's your understanding that somebody could rewrite that code --

A. Yes, I understand.

Q. -- to say, all right, every time somebody votes for one, count it as two?

A. Yes.

Q. And that would be a change to the system?

A. Yes.

Q. And so is it possible that when you said "override of the system," you meant, I don't care if you need to change the software code that was run, that was in place at the time, I don't care. I just

Page 78

want the data?

A. That was our understanding.

Q. Because I know you can do that.

A. If you have to write a new line of code to --

Q. So be it?

A. -- provide the table, do so. Yes.

Q. But you didn't have an understanding, one way or the other, whether that was, in fact, required?

A. Yes, I didn't.

Q. So, again, I want to be sure the record is clear. Let me go back just to summarize.

So you didn't investigate, and you don't know, one way or the other, whether an override of the system was, in fact, required to generate that data?

A. I believe that Gerry Feldkamp said in the BallotPoint demonstration, that they would have to make some modification of the software.

Q. And you accepted that?

A. Yes.

Page 79

Q. You didn't look behind that?

A. I didn't question that.

Q. And you have no evidence to question that --

A. No.

Q. -- that you accumulated in the course of your investigation?

A. That's right.

Q. So I think you may have said this already, but just to confirm, BallotPoint resisted providing that data, and you ended up having to subpoena them for it, correct?

A. Yes, that's correct.

Q. And whose decision was it to issue the subpoena? Was that a product of your group deliberations?

A. Yes. I know I probably made the ultimate call to say, Let's subpoena those records.

Q. Okay. Do you recall when exactly that subpoena issued? I think it was early August or late July.

Does that sound right to you?

Page 86

get -- I'm not going to stop and talk about that now.

But, ultimately, you concluded, based on the work that the three of you did, and as described in the interrogatories, that your suspicion here, your tentative conclusion that the system appears to have allowed for was, in fact, the case?

A. Yes.

Q. Can you give him back D-5, which is the complaint?

I asked you some questions about this before, but let me turn to Factual Allegation No. 21.

A. Yes.

Q. And that's sort of another way of framing that point that was in one of the investigatory findings, correct, that the system --

A. Yes.

Q. There is data in it that can be matched up, if you have access to both of the servers?

A. Yes.

Q. That could be done?

A. Yes.

Q. In the course of your investigation, by

Page 87

the way, did you uncover any evidence that BallotPoint had, in fact, matched up that data -- had pulled and matched up that data?

A. No.

Q. Let me just sort of -- I want to parse this factual allegation with you a little bit. It says, the first sentence, "This Internet-based electronic voting system permitted the names of voters to be linked with their voting choices."

A. Yes.

Q. Now, you previously testified -- and correct me if I'm wrong, if I'm mischaracterizing -- that part of the system is the software code applications. So you have no evidence, as you've testified, that the system, including the source code that was in place at the time of the election, permitted the names of voters to be linked with their voting choices, correct?

A. I don't know what that characterization means.

Q. What do you --

A. I --

Page 117

logical matter, it seems logical to me, but you would conclude that if it cost them $1 million, it would be pretty unlikely that they would invest that kind of money or 100 hours, invest that kind of time in doing that. Is that fair?

A. I don't know about -- perhaps. I don't know how many hours.

Q. It would have been --

A. I don't remember how many hours. 100 hours. I don't know.

Q. That was one of the reasons you were asking for this information?

A. Yes.

Q. So, generically, then, things like cost of doing something to connect the voter with the vote and time, those are all relevant considerations in assessing whether there has been a ballot secrecy -- there's a ballot secrecy issue, in your mind?

MR. STOLTZ: Objection, calls for a legal conclusion.

THE WITNESS: I think -- we know there is a ballot secrecy issue because we connected the voter

Page 118

and the vote. So we know the law was violated. Again, the LMRDA has a strict secrecy requirement. We connected the voter and the vote. So that's a violation.

As far as I'm concerned, you know, regardless of how long it would have taken BallotPoint to reconfigure or make changes to the system to access the data, if they, indeed, even -- I should add, if they, indeed, needed to make a software code change to view the data. I don't know that.

Again, I would defer to technical experts.

BY MR. ROTH:

Q. Okay. I mean, obviously, you need -- as an investigator, you need to understand Department policy in order to know what to investigate, what questions to ask and stuff like that. So, I think, I sort of heard two conflicting -- on the one hand, you said that kind of information is relevant to your -- under DOL policy, in terms of what might be a violation.

And, on the other hand, I heard you say it

Page 119

wouldn't have mattered, even if you found out it cost them 10 million -- it would be cost prohibitive and time prohibitive, so it wouldn't -- you could almost rule out the prospect that they did it, that wouldn't matter?

A. Yes. The fact that we were able to connect the voter and the vote and to say positively, affirmatively, over 4,000 members, this is how they voted in this election, is a violation.

Q. No matter how remote the prospect that they would, in fact -- that BallotPoint, in fact, would have done something like this?

A. Right.

Q. In the absence of a complaint and investigation? That's totally irrelevant, in your view?

A. I'm not saying it's irrelevant. I'm saying it's a violation.

Q. It's a violation that --

A. The fact that we could connect the voter and the vote is a violation.

Q. So it's possible?

Page 120

A. No, the fact that we did.

Q. The fact that it can be done, it's possible. You did it?

A. We did it, exactly.

Q. Which is proof that it's possible?

A. Exactly.

Q. So as long as you prove that it's possible, under your understanding of the policy that -- you're investigating under a policy, correct? These questions really didn't -- weren't ultimately relevant to your determination that there was a violation, whatever the answer was -- to this would be?

A. It was already a violation, yes.

Q. Was already a violation, in your view?

A. Yes.

Q. I take it that your answer would be the same with respect to any assessment of BallotPoint's sort of bona fides, in terms of whether they were known to be a reputable organization or known to be unscrupulous in some way, that would be irrelevant to you. Because you're not in the business of assessing

Page 143

prompted their development of one-vote, no void, what you would say is, That's all well and good, but it didn't go far enough, basically?

A. That's exactly what I would say. I think they picked up on some of the principles that we discussed in the stipulated settlement, and they employed parts of that, but I don't believe they went far enough.

Q. In your view, did it represent an improvement over the prior system?

A. I don't know that it did. I mean, the fact that we were able to connect the voter and the vote, I mean, it's still a fatal flaw. If they would have gone the whole way so that no member voter information ever enters the system, then the secrecy problem is cured.

Q. Are you aware that they've made further refinements to their system so that they no longer -- that the software no longer collects IP address information and time stamp information? Are you aware of that?

MR. STOLTZ: Objection, ambiguous.

Page 160

know?

A. As far as I know, no.

Q. Just one final question on this.

I know you said there was some member communication about confirmation numbers, but are you aware of any communication with a rank and file member, either with personal or with one of your investigators, where they expressed concern that the fact that they got a confirmation e-mail was suggestive of a secret ballot problem?

A. No, I don't have any information in regards to that.

Q. All right. I'm sure this will be a relief to you, but I'm going to switch gears now to observer issues, reserving the right to come back with a question or two that crosses the divide.

Just as sort of a generic question about observers, my understanding of the function of an observer -- and I want to get, sort of, your understanding of the function of observer and see if it jives with mine.

My understanding is that's a human being

Page 161

with eyes. And the statute says you have to have one at the polls and at the counting of the ballots. And so you have -- the point of that is that you have somebody who can see if there is either some hanky-panky or fraud or tampering or something illicit, they can see with their own eyes that that's happening.

Or something sort of illicit, you know. Just mistakes, ballots are being miscounted, you know, innocently. There's some -- anything, whether it's illicit or nonillicit, that would affect the accuracy of the tally. They can -- an observer is there and functions as somebody who can tell and then spill the beans on something like that.

Is that fair?

A. Yes, I think that's fair. That's what the statute says at the polls and at the counting of the ballot.

Q. And the statute says that.

And that's sort of your understanding of the point behind having an observer, right?

A. Yes.

Page 166

have -- we just talked about what an observer is. An observer is somebody who visualizes.

A. Exactly.

Q. Is it possible to have an observer at the polls in a remote electronic voting system election? An election held by remote electronic voting of a client at ballot, is it possible to have an observer at the polls? There are no polls, correct?

A. Correct.

Q. I mean, people vote. That's what an electronic vote is. People vote, either from their personal computers or from their phones.

A. Exactly.

Q. There is no polling place. Similar to a mail ballot election, correct?

A. Similar. And that's why we've -- the department in OLMS has put out guidelines and guidance for observer rights in the context of a mail ballot election, realizing that there aren't actual polls.

Q. Right. You can't --

A. There's other observer rights that -- you

Page 167

know, that are built in, like the mailing of the ballots to the members.

Q. Right. But the statute requirement of having an observer at the polls is impossible in both the mail ballot and the electronic ballot context, correct?

MR. STOLTZ: Objection, calls for a legal conclusion.

BY MR. ROTH:

Q. I'm not asking for your legal conclusion. I'm asking for a physical possibility.

Is it physically possible to have a human observer visualizing the balloting at the polls in an election that doesn't have polls?

MR. STOLTZ: Same objection.

THE WITNESS: Yeah. There's --

BY MR. ROTH:

Q. You can answer.

A. There is no way that an observer could observe somebody filling out their ballot in their living room in a mail ballot election. And there is no way that an observer can observe -- you can set up

Page 168

a system where an observer can observe somebody voting from their personal computer in their living room.

Q. Or their telephone when they're running through an airport --

A. Yes.

Q. -- to get on a plane?

A. Which makes it incumbent upon a system to provide --

Q. Alternatives?

A. -- some alternative mechanisms for candidates to have observer rights so that observers can see some sort of -- visualize and see some sort of tangible record that could help them verify that the system is accurately recording votes, and that the system is accurately tallying the votes.

Q. But the alternatives don't necessarily have to be observers. They could be other technological safeguards, correct? Like client-side encryption is not an observer, right?

A. I don't think the client-side encryption is an observer right. I think your analogy is

Page 171

are counted?

A. Yes.

Q. Aren't the votes counted through a software application that is a counting -- is like a computer? Doesn't the counting take place inside the gears of a computer?

A. That's right. So there is no way --

Q. That is right.

A. That's right. I don't believe that there is a way for an observer to observe the counting of the ballots electronically.

Q. Right.

A. But I do believe that it's possible to build in a paper backup that will allow an observer to observe the tallying of the ballots.

Q. That wasn't my -- I understand that, and I'll come back to that. The more you want to say about that, I'm more than happy to let you say.

But just for the present time, you would acknowledge, at least, that -- forget checking the count, but the actual count itself that's performed inside the gears of a computer, the observer, Morales

Page 172

was not able to see that?

A. No.

Q. And it was not possible for him to see that?

A. That's right. I agree.

(Willertz Exhibit No. 13 was marked for identification.)

BY MR. ROTH:

Q. Can you identify this document?

A. Yes. This is the OLMS compliance tip for electing union officers using remote electronic voting systems. We published this on our website. I think it was in October 2016.

Q. Is it still up on the website?

A. It is still up on the website, yes.

Q. And this is a true and accurate copy, as far as you can tell?

A. Yes, as far as I can tell.

Q. Copy of what's been taken off the website?

A. Uh-huh.

Q. Just -- if you turn to page -- it's not paginated, but one, two -- nor is it Bates stamped.

Page 173

The third page, the first carryover paragraph, last sentence, where it says, "In the context of electronic voting systems" -- and here you're talking about Mode electronic voting systems -- "in which the polls and tally are not visible, assuring the integrity of such systems presents."

And that's what we were just talking about. You can't have an observer visualizing those things, so you've got to come up with some other mechanism.

Then you start talking about mail ballot. So let me ask you about mail ballot. And you've already acknowledged that there were no polls in the mail ballot. So you can't have an observer at the polls, so you come up with a substitute set of safeguards.

I take it -- and these are embodied in the regulations cited, correct?

A. Yes.

Q. And, I take it, that these safeguards are -- I mean, every case may vary and they may not

Page 174

be followed accurately, but if these safeguards are followed, you believe that that -- OLMS believes that those serve as adequate safeguards in the mail ballot election context?

A. Yes.

Q. Adequate safeguard for what? To prevent against what? For what -- or what are they safeguards against, these alternatives?

A. Adequate safeguards for the handling of the ballots. I mean, it gives candidates the right to have an observer observe the process and understand the process and have some sort of independent verification that the ballots were mailed to all members. That members had an opportunity to vote. That there was a mechanism for receipt of those ballots.

That they can observe the pickup of the ballots at the appointed time and see the return ballots and inspect them and to also see them brought back to a tallying site and observe the separation of the inner secret ballot envelope from the outer envelope with identifying information. And then

Page 175

observe the separation of those two different types of envelopes. And then observe, at that point, the opening of the secret ballot envelope, the removal of the actual ballots.

And then the counting of the ballots so that they can see, with their own eyes, that the ballots are being counted correctly, according to the voter's intent. They can see markings, a checkmark for Candidate A, and they can see that the counters are accurately counting those votes and registering the votes for their proper candidate.

Q. Okay.

A. Yeah.

Q. Those are the sort of substitutes for the inability to have all of the observer requirements that the statute provides for?

A. Well, it's just, basically, the first, because the tallying of the ballots is --

Q. The counting.

A. The counting of the ballots --

Q. That's incorporated?

A. -- is incorporated here.

Page 176

Q. That's not an alternative.

A. Yes.

Q. That's incorporated within the regulations?

A. Yes.

Q. Okay. I got that. I want to take each one of those, sort of, three things individually and ask you about them.

The right to have an observer at the preparation and mailing of the ballots. Now, I'm just trying to sort of get a sense of the practicality of that. Let's take a union like APFA. They've got 20,000 members or so. They're spread out all across the country. Just like in the electronic ballot here, where you had a third party in Michigan prepare the ballots, you're going to have to pick somewhere.

I think APFA has traditionally picked their home area of Dallas/Fort Worth to have -- hire a company to do the preparation of the ballots, but it's not going to -- correct me if I'm wrong, but in practical terms, it's not really going to be feasible

Page 192

adequate safeguards in a mail ballot election?

A. Yes.

Q. On the regulations.

Switching gears now to remote electronic. Correct me if I'm wrong, but I read this guidance as saying that notwithstanding the fact that the polls and the tally are not visible, so the traditional observer rights don't apply, it, at least in theory, is possible to handle electronic balloting in the same way as mail balloting. In other words, we will come up with a set of alternatives --

A. Yes.

Q. -- that we regard as adequate, okay?

A. (Witness nodding.)

Q. And there are some here that you say are just absolutely required as alternatives, and others you say you give a range of things that might be acceptable and things like that. But at bottom -- and I don't want to get into the detail of all of these, because these weren't even in place at the time of the BallotPoint election that were at issue, correct?

Page 193

A. Correct.

Q. That this reflects a view of OLMS that it is, at least theoretically, possible that you could come up with a set of substitutes for the traditional observer rights, such as this technology, paper, paper balloting, client-side encryption, auditing, various auditing rights are noted. You could come up with a series of safeguards that would serve the same function in a remote electronic balloting context as these alternative safeguards in the mail ballot context.

That would give us -- or at least theoretically possible that we would regard an electronic election conducted with these group of safeguards as meeting the general mandate in the statute that the adequate safeguards are in place.

Is that fair?

A. Yes. Yes. Although, I don't know that I would put client-side encryption in that category.

Q. Yeah. So I'm looking at D here. It says, "The use" -- this is under "must include."

A. Okay, this is must include.

Page 195

did, I apologize. And, I guess, the record will reflect it. But I don't think I asked you to what extent you participated in this, in the drafting of these guidelines.

A. I worked on this quite a bit, yes.

Q. Quite a bit. Based on the experience you have with these systems from your various investigations?

A. Yes.

Q. So at least you're familiar --

A. Yes.

Q. You're intimately familiar with these various concepts, at least?

A. Yes.

Q. Whether you necessarily agree with each and every one of them is neither here nor there.

But you're familiar with them?

A. Yes.

Q. So let me ask you this: In your investigation of the BallotPoint election, the national office areas election in January 2016, did you specifically investigate the issue of whether

Page 196

these kind of other types of safeguards were put in place or are contained with the BallotPoint system? Was that sort of an investigatory topic of yours?

Does that question make sense?

A. Yes.

Q. Was that an area of inquiry in your investigation?

A. Yes. I think we definitely gathered as much information as possible to determine what could be observed, in terms of by a candidate observer in the observer process, yes.

Q. No. But I thought you've already said that it was -- I want to be clear, because it's not just semantics. You can't -- I thought you've already testified it's impossible to observe the polling place because there is no polling place.

A. Right.

Q. And it's impossible to observe the actual count. So, I guess, what you're saying is you looked at whether there were other technologies -- whether there were or were not other technologies, such as paper ballot records.

Page 199

Q. I understand.

A. As you've said earlier.

Q. But it's not an observer right, is it?

A. It is an observer right to observe the tallying of the ballots. That's what the statute calls for.

Q. I don't want to be argumentative.

A. Okay.

Q. So you did look -- you did consider these issues?

A. Yes.

Q. What other safeguards were in place at BallotPoint? Did you reach a conclusion in your investigation as to -- well, let me back up a second.

Are you aware that the statute -- not the statute -- the Department of Labor regulations state that the statute has a separate requirement from observer rights, and the requirement is a general mandate that adequate safeguards be provided in an election? Are you aware of that?

A. Yes.

Q. Did you make a finding, in the course of

Page 200

your investigation, as to whether the union, through the hiring of BallotPoint, provided adequate safeguards to ensure a fair election, and, therefore, satisfied that general mandate? Did you make an investigatory finding on that point?

A. Yeah. We didn't find that there was a violation of general fairness adequate safeguards. The finding was that there was not observer rights.

Q. Observer rights, okay.

A. Yes.

Q. And in the same vein -- do you have the complaint in front of you still?

A. Yes.

Q. Is there any factual allegation in this case that BallotPoint -- that the union did not comply with the general mandate in the statute to provide adequate safeguards to ensure a fair election?

A. No, I don't see that here.

Did I miss it?

Q. All right. Where are we here?

MR. ROTH: Can we just take a short break?

Page 217

one theory.

A. Yes.

Q. All right. Let me go back to the interrogatories.

Do you still have those in front of you?

A. Yes.

Q. So you do but I don't. Let's see. All right. Moving on to -- we're still at page 8. A little further down the paragraph -- the two paragraphs starting "moreover" on page 8.

A. Yes.

Q. I have a few questions. If you want to take a second to read those two paragraphs, the "moreover" and the "further."

Just let me know when you've had a chance to review that.

A. Yes, I've read that paragraph.

Q. Can you read both of them, the "moreover" and the "further"?

A. Okay, further. Okay.

Q. Now, what I read you to be saying in the "moreover" paragraph is, that you were able to link a

Page 218

voter with a vote in 4,081 cases, through the methodology that you've described here in the interrogatories?

A. Yes.

Q. And that if you assume that all or a substantial part of those 4,000, by virtue of the secret ballot violation, because you call them affected voters, the ones who were affected by the secret ballot violation, if they had changed their votes, or if they had cast their votes for the losing candidate, that could have affected the outcome of the election.

Now, my question to you is, doesn't that presuppose that these 4,081 people knew about the secret ballot violation, and, therefore, changed their votes out of some type of fear that, you know, if they voted for one candidate as opposed to another, i.e., the favorite candidate, that their vote could be revealed, and, therefore, they could be retaliated against?

So, to prevent that, they would vote for somebody else? Doesn't that presuppose some type of

Page 219

knowledge on the part --

A. No.

Q. Does not?

A. No. We don't look at it that way. When we look at a fact with respect to nonsecret votes, we would count up the number of nonsecret votes and compare them to the margins. And if the number of nonsecret votes exceeds the margins, we may -- it may have affected, because it mathematically may have affected.

Q. Well, it can only mathematically have affected the outcome if it changed people's votes, right? And it wouldn't change people's votes unless they had some knowledge of the violation, correct?

A. Well, when we look at secrecy violations, we don't know what's going on in the voter's head. We don't know what they know or what they don't know or whether there is subtle coercion or how the violation may have affected. So we look at the maximum number, the number of nonsecret votes compared against the margins, and then we say, It may have affected.

Page 220

Q. Okay. When you say "we," is that sort of --

A. Department of Labor, OLMS.

Q. Is that --

A. That's our policy.

Q. That's your policy?

A. The way we look at secrecy violations, yes.

Q. So, in your view -- under that policy, in your view, it's totally irrelevant whether the member would have known about the secret ballot violation or not?

A. Well, we don't -- no, it's not irrelevant. But we don't know. And we don't know -- we can't get inside of the heads of the voters at the time that they were voting. We don't know. And so we presume effect, and we count up the nonsecret votes.

As an example, in a manual election, if voters are marking their ballots in an open cafeteria and members are milling around and there is no partitions and other members could look over the person's shoulder to see how they're voting, we would

Page 221

determine how many people -- how many voters voted in that manner.

We would see those are nonsecret votes and we would compare that number against the margins and we would say that any of those races that had margins less than the number of nonsecret votes, may have affected the outcome, even though we may not know how that affected how those voters marked their ballots.

Q. In the manual vote example, though, correct me if I'm wrong, but if people are looking over people's shoulders and stuff, that could give rise to a legitimate fear on the part of the member, because he sees people looking over his shoulder, that people actually can see how they voted. And the union hasn't taken adequate steps with partitions or whatever to prevent that.

So that strikes me as a situation where the presumption that it did affect their vote has some validity to it.

You testified earlier -- and I'm going to get to another one of your interrogatory responses -- that there is no way a member would know that the

Page 222

system stores information in a way that somebody who had access to two servers could connect -- I mean, they don't have -- you testified earlier they don't have access to the BallotPoint system. And, I think, your exact words were, "and they don't have the technological know how."

There is no way you said that they would know and, therefore, be put into a reasonable fear that their vote was being surveyed or monitored or was not totally secret?

MR. STOLTZ: Objection, misstates the prior testimony.

BY MR. ROTH:

Q. Okay. You can answer my question.

So my question to you is, in that far different context, wouldn't you agree that it's totally counterintuitive, at best, to presume that a voter would know about the secret ballot violation?

A. I don't know that it would be counterintuitive. I don't know that they would know. What we say is that the system has to be secret, and if it's not secret, we don't know how that may affect

Page 223

how people vote. I point to the example of the member -- the voter who asked that question to Cindy Horan --

Q. Right.

A. -- Hey, I wrote down my confirmation number --

Q. Right.

A. -- is there any way that anybody can use that confirmation number to determine how I voted, as an example of a member or voter wondering, you know, is it secret? Can someone tell how I voted? They just sent me an e-mail. They sent me a confirmation number. Is there a link?

We don't know what may be going through these members' heads when they're voting, whether they suspect that there is a secrecy problem or not.

Q. I understand that. I understand that. But you're not saying that the use of confirmation numbers was a violation of the statute, are you?

A. No. The ability for us to link the voter and the vote was this secrecy violation.

Q. Through this methodology?

Page 224

A. We weren't able to do it with the confirmation numbers because they didn't keep the confirmation numbers. They overrode the confirmation numbers.

Q. You were able to do it, as you set forth in the interrogatories, because there was this data on the two servers that, when you connected it up through this very painstaking process that you described, you were able to link them up, and that you say shows that there was a secret ballot violation.

And my question to you is, if no member would have been aware of that capability of the system to be linked up, how would that influence their vote? They didn't even know about it.

A. I don't know.

Q. Can you explain?

You say you don't know. Can you explain to me how -- through what mechanism a person's vote would be affected if they had no knowledge of that capability of the system? How would that affect their vote if they didn't know about it?

Page 225

A. There is no way for them to know exactly what was behind the scenes or in the black box. But either the fact that it was not secret and that there could have been questions, concerns, suspicions on the part of the members, means it may have affected the outcome.

Q. But other than that one inquiry about confirmation numbers, you're not aware -- I think you testified earlier -- of any inquiry or stated concern from a member about this capability of matching up the data to learn people's identity in terms of how they voted?

A. No. Other than the complaint itself. But --

Q. The complaint?

A. The complaint by Mr. Morales.

Q. But Mr. Morales didn't --

A. He didn't discuss--

Q. He just said, There is a secret ballot violation, correct? He didn't specify?

A. He wasn't as specific as the other member who questioned the confirmation number.

Page 226

Q. He wasn't specific at all, was he? He just said, I fear -- or I believe there has been a secret ballot violation?

A. Yeah, he raised the issue.

Q. In the same vein, let me turn to page 9, No. 3, 6. So paragraph 3, subparagraph 6, where you say, "BallotPoint's election system is not accessible for inspection by members or their agents; moreover, it's complicated, highly-technical design makes it highly unlikely that a union member could discern whether it was functioning to only count votes from eligible voters, and to accurately count those votes."

Isn't it also true that given that BallotPoint's election system is not accessible for inspection by members or their agents, and is moreover a complicated, highly-technical design, doesn't that make it highly unlikely, if not impossible, that a member could discern that there is data in the two servers that could be connected up to link a voter with the vote?

A. Right.

Page 227

Q. Correct?

A. That's correct. I think the fact that there is a secrecy violation, and that the voter and the vote can be connected for over 4,000 voters, means that there is a secrecy violation. How it affected how they voted, we don't know. But we know that --

Q. But you're still saying it may have affected the outcome of the election?

A. Yes.

Q. Because you just say so?

A. And I've seen --

Q. That's your policy?

MR. STOLTZ: Objection, argument.

Go ahead.

THE WITNESS: Yes. In a nonsecret election, if the election is nonsecret, the number of nonsecret votes determines the effect on outcome.

BY MR. ROTH:

Q. And that's the OLMS view of the statute?

A. Uh-huh.

Q. And, I guess, your answer would then be

Page 228

the same on the "further" paragraph, where it says -- or maybe not. You tell me. It says, "9,355 members voted. Over 11,000 members did not vote. If the election had been conducted with a secret ballot, it is possible that these 11,000 nonvoting members would have voted, and that the votes would have changed the election outcome."

Now, my question to you, again, is, it's only possible, correct, for the 11,000 members not to vote out of fear of a secret ballot that their ballot could be revealed, if they have some inkling that their ballot might be revealed, correct?

A. That's right.

Q. And the violation here is that it could be revealed by matching up data with data from the two servers.

A. That's right.

Q. But you have no evidence that any member knew that was possible?

A. That's right.

Q. Okay. Let's turn to page 9. "The following facts" -- I'm going to read this sentence

Page 268

Notice Date: 06/23/2017

Deposition Date: 06/13/2017

Deponent: Stephen J. Willertz

Case Name: Perez v. Association of Professional Flight Attendants

Page: Line Now Reads Should Read

Page 42, line 9, "specific" should read "secret"

Page 111, line 19, "district" should be "strict"

Page 191, line 1, "avoided" should be "voided"

Page 212, line 21, "a fact" should be "affect"

Page 247, line 11, "contacted" should be "contracted"

Page 254, line 11, "a fact" should be "affect"

Page 269

CERTIFICATE OF DEPONENT

I hereby certify that I have read and examined the foregoing transcript, and the same is a true and accurate record of the testimony given by me.

Any additions or corrections that I feel are necessary, I will attach on a separate sheet of paper to the original transcript.

I swear under penalty of perjury that the foregoing is true and correct.

Stephen J. Willertz
____
Signature of Deponent

Dated: _

~~I hereby certify that the individual representing himself/herself to be the above-named individual, appeared before me this _____ day of ____________, 2017, and executed the above certificate in my presence.~~

~~NOTARY PUBLIC IN AND FOR~~

~~_______________________~~

~~County Name~~

~~MY COMMISSION EXPIRES:~~

Page 270

CERTIFICATE OF REPORTER

UNITED STATES OF AMERICA) ss:
DISTRICT OF COLUMBIA)

I, MARY GRACE CASTLEBERRY, RPR, the officer before whom the foregoing proceedings were taken, do hereby certify that the foregoing transcript is a true and correct record of the proceedings; that said proceedings were taken by me stenographically to the best of my ability and thereafter reduced to typewriting under my supervision; and that I am neither counsel for, related to, nor employed by any parties to this case and have no interest, financial or otherwise, in its outcome.

Mary Grace Castleberry

Notary Public in and for
The District of Columbia

My commission expires: 7/14/2021

Willertz Deposition
Exhibit 13

OLMS COMPLIANCE TIP

Electing Union Officers Using Remote Electronic Voting Systems

The Labor-Management Reporting and Disclosure Act (LMRDA) establishes democratic standards for conducting regular elections of union officers and elections of delegates who elect officers. The Office of Labor-Management Standards (OLMS), an agency within the Department of Labor, is responsible for enforcing the LMRDA. The LMRDA requires every local labor organization to elect its officers by secret ballot, and every national, international and intermediate labor organization to elect officers by secret ballot among the members in good standing or by representatives chosen by secret ballot. *See* 29 U.S.C. 481(a), (b), (d). The LMRDA further requires that adequate safeguards to insure a fair election shall be provided, including the right of any candidate to have an observer at the polls and at the counting of the ballots, 29 U.S.C. 481(c), and that the ballots and all other records pertaining to the election shall be preserved for one year following the election, 29 U.S.C. 481(e). The LMRDA also gives union members who believe that a violation of the election provisions of the LMRDA has occurred the right to file a complaint with the Secretary of Labor.

Purpose of this compliance tip:

This guidance has been developed by OLMS to explain how the LMRDA's requirements apply when implementing remote electronic voting systems in union officer elections. The challenges presented in assuring the secrecy and security of remote electronic voting systems have been well-documented in the context of public elections, which Congress used as the model for union elections under the LMRDA.[i] While remote electronic voting has not been widely adopted for public elections, technology to address these challenges has been a matter of extensive study and discussion. Two significant challenges are the tension between maintaining the secrecy of the ballot while ensuring that each eligible member's vote is accurately cast, and ensuring observability for a voting technology that does not necessarily generate "ballots" that can be observed at the "polls" and at their "counting," as the LMRDA provides. Because the technology in this field is evolving, it is difficult to identify definitive solutions that are most likely to permit voting that is in conformance with the LMRDA. Further, new technology is likely to provide additional methods of conducting remote electronic voting consistent with the LMRDA.[ii]

The specific guidance presented here is based on current technology and the characteristics and design elements of remote electronic voting systems that OLMS has reviewed to date. While all remote electronic voting systems must comply with the LMRDA's requirements, it is possible that solutions other than those identified here would also satisfy these requirements. Thus, OLMS will evaluate each electronic voting system that is the subject of a complaint under title IV of the LMRDA on a case-by-case basis to determine whether it meets the requirements of the statute. If you have questions about remote electronic voting systems, OLMS welcomes you to contact us at olms-public@dol.gov Moreover, OLMS recognizes that innovative voting technology may be developed that enhances compliance with the requirements of the LMRDA, and OLMS invites such innovative developments to be shared with us, also at olms-public@dol.gov

Remote electronic voting systems:

The LMRDA does not require a particular method or system of voting. Labor organizations may establish their own methods or systems of voting for officer elections as long as they are consistent with the LMRDA. Some labor organizations, in recent years, have chosen to conduct officer elections using remote electronic voting systems or have expressed interest in using a remote electronic voting system to elect their officers. The term "remote electronic voting systems" is meant to include: (1) electronic voting from remote site personal computers via the Internet; and (2) electronic voting from remote site telephones. It is not meant to include electronic voting machines used for casting votes at polling sites or electronic tabulation systems where votes are cast non-electronically but counted electronically (such as punch card voting or optical scanning systems). As with other voting procedures, remote electronic voting systems may be permissible under the statute so long as they satisfy the LMRDA's standards.

1. __Guidance for preserving ballot secrecy__:

LMRDA Section 3(k) defines a secret ballot as: "the expression by ballot, voting machine, or otherwise, but in no event by proxy, of a choice with respect to any election or vote taken upon any matter, which is cast in such a manner that the person expressing such choice cannot be identified with the choice expressed." 29 U.S.C. 402(k). Several court cases make it clear that the requirement of a secret ballot in union officer elections is to be interpreted strictly. Ballot secrecy requires that no person, including an independent third party, have access to information allowing such person to learn how a particular member cast his or her vote at any time. Moreover, a member's vote must remain secret after the ballot is cast.

One way to help to insure that ballot secrecy is maintained in an electronic voting system is to avoid creating a connection between a voter's identity and the vote cast, *i.e.*, voters' names would never be entered into the system as part of the voting credentials (the term "credentials" in this guidance includes the multiple codes used for various purposes in electronic voting systems, including access codes, log-in codes, confirmation codes, etc.). In this way a voter's identity could never be linked to his or her vote using information in the system. This can be accomplished by determining voter eligibility prior to mailing the voting credentials and by randomly assigning the credentials to each eligible voter. Once this initial eligibility determination is made and the credentials mailed, there can be no mechanism to void or prevent the casting of ballots by any members who were determined to be eligible. Such a system, however, can present logistical challenges. For example, a union may need to provide replacement credentials to members who have not received or have lost their voting credentials or issue such credentials to newly eligible members. If duplicate credentials or other processes are used to resolve these logistical challenges, all material must be secured when not in use and observers must be given the opportunity to observe the processes employed when using the materials.

Systems should employ proper safeguards to prevent a voter from being able to provide visual proof of the content of his/her vote in order to prevent secrecy violations in the form of coercion or vote buying/selling. For example, the system must not display the voter credential and the content of the vote in such a way that it permits the voter to capture and share the image, nor should lists matching voter credentials and the content of the vote be publicly available.

To the extent that technology is developed for public elections that allows for the inclusion of voter-identifying information in a manner that protects vote secrecy, that technology may also be appropriate for use in union elections.

2. __Guidance for preserving observer rights__:

Section 401(c) of the LMRDA requires that "adequate safeguards to insure a fair election shall be provided, including the right of any candidate to have an observer at the polls and at the counting of the ballots." 29 U.S.C. 481(c). This requirement provides for the essential monitoring that votes were cast by eligible union members and that those votes were accurately tallied. In the context of electronic voting systems, in which the "polls" and "tally" are not visible, assuring the integrity of such systems presents challenges.

The Department's regulations have permitted the conduct of election by mail ballot, as long as safeguards are followed to protect secrecy and to allow observation of specific stages of the election process, namely, the preparation and mailing of the ballots, their receipt by the counting agency, and the opening and counting of the ballots. 29 CFR 452.97, 107(c). Similar procedures in the context of electronic voting, which permit observation and protect the security of the vote from its casting to its counting, must include:

a) The opportunity to view the list of members and make eligibility challenges prior to the distribution of voter credentials.

b) The opportunity to observe the preparation and distribution of voting credentials to be used by members. Observers must be allowed to view the process, but must not be allowed to see the specific voting credentials that are sent to individual members, which must be kept secret.

c) The opportunity to observe any later distribution of credentials to members who did not receive or who lost credentials. Again, observers must be allowed to view the process, but must not be allowed to see what specific voting credentials are sent to individual members, which must be kept secret.

d) The use of technology that protects the integrity of the vote from the point when it is cast by the voter through the voting process, such as client-side encryption technology, that runs on the voter's computer or in conjunction with any computer-telephone integration, rather than on the election server.

e) The opportunity to observe any steps necessary for the counting of the votes, and any other steps necessary to audit that process.

f) The use of technology that provides a secure method of independent vote verification that allows the voter or an observer to confirm that the vote was recorded and counted accurately. Safeguards should be employed, however, to prevent such features from presenting secrecy lapses and opportunities for voter coercion. Safeguards that could preserve this aspect of observability without compromising vote secrecy may include:
    i. Allowing each member to view a printed ballot version of his or her electronic vote, which contains a credential known only to the voter and which is stored in a supervised, secure, observable location. These printed ballots could also be tallied in a supervised, secure, observable location to verify the accuracy of the electronic vote count.
    ii. Allowing each member to confirm the accuracy or integrity of his or her vote by inspecting a non-public list of the electronic votes alongside the credential known only to the voter, stored in a supervised, secure, observable location.
    iii. Allowing each member to confirm the accuracy or integrity of his or her vote by inspecting a posted list that pairs representations of votes (e.g., as hashes or codes that would allow a voter to know that the vote has not been changed but would not reveal the vote choice itself) alongside voter credentials, or representations of voter credentials.

The electronic voting system should contain mechanisms by which observers can verify, prior to an election, that the system is working properly.

The electronic voting system should include hash chains on the activity logs and the ballot box.

The electronic voting system should be audited by an authorized independent party periodically.

For any electronic voting system, there should be a document or documents that specify the security policy for all systems that will come into contact with the voter or vote information. Further, every role and its corresponding access should be clearly specified, using mathematical descriptions where applicable. The security policy should also include a risk assessment, threat analysis, and modifications made to mitigate such risks/threats.

3. ***Guidance for preserving records:***

The electronic votes and any paper versions of the electronic votes, and all other paper and electronic records pertaining to the election, including eligibility lists, the voting credentials, the log files, the time stamped software code used to run the electronic voting system, and the ballot tally results, must be preserved for one year.

4. ***Guidance for preserving right to vote:***

An alternative voting method must be provided, upon request, to any member who does not have access to the electronic voting system.

Remote voting must be implemented in a manner that does not create barriers for individuals with accessibility needs.

Office of Labor-Management Standards Field Offices

Atlanta, GA
Birmingham, AL
Boston, MA
Buffalo, NY
Chicago, IL
Cincinnati, OH
Cleveland, OH
Dallas, TX
Denver, CO
Detroit, MI
Ft. Lauderdale, FL
Honolulu, HI
Kansas City, MO
Los Angeles, CA
Milwaukee, WI
Minneapolis, MN
Nashville, TN
New Orleans, LA
New York, NY
Philadelphia, PA
Phoenix, AZ
Pittsburgh, PA
St. Louis, MO
San Francisco, CA
Seattle, WA
Tampa, FL
Washington, DC

For the address and telephone number of our field offices, please call 1-866-4-USA-DOL (1-866-487-2365) , or view our online organizational listing at **http://www.dol.gov/olms/contacts/lmskeyp.htm.**

OLMS

Office of Labor-Management Standards
U.S. Department of Labor
October 2016

Visit us at **www.olms.dol.gov**
E-mail us at **olms-public@dol.gov**
Call the DOL National Call Center at **1.866.487.2365**

REFERENCES

[i] Nelson Hastings, et al.: Security Considerations for Remote Electronic UOCAVA Voting. National Institute of Standards and Technology, NISTIR 7770 (February 2011). *Available at*: http://www.nist.gov/itl/vote/upload/NISTIR-7770-feb2011-2.pdf.

[ii] U.S. Vote Foundation: The Future of Voting: End-to-End Verifiable Internet Voting Specification and Feasibility Assessment Study (July 2015). *Available at:* https://www.usvotefoundation.org/E2E-VIV.

ADDITIONAL RESOURCES

iVote Advisory Committee Final Report, Aug. 21, 2015, Utah Lt. Governor Spencer J. Cox

Peter Haynes, "Online voting, rewards and risks," Atlantic Council, (2014). *Available* at: http://www.atlanticcouncil.org/publications/reports/online-voting-rewards-and-risks

Barbara Simons and Douglas W. Jones, "Internet Voting in the U.S." (2012), 55 *Communications of the ACM* 68, http://cacm.acm.org/magazines/2012/10/155536-internet-voting-in-the-us/fulltext.

U.S. Election Assistance Commission (EAC), "A Survey of Internet Voting" (September 2011), http://www.eac.gov/assets/1/Documents/SIV-FINAL.pdf.

David Jefferson, "If I Can Shop and Bank Online, Why Can't I Vote Online?" https://www.verifiedvoting.org/resources/internet-voting/vote-online/

Association for Computing Machinery (ACM) U.S. Public Policy Council, "Issue Brief: Internet Voting and Uniformed and Overseas Citizens absentee Voters," http://usacm.acm.org/images/documents/IB_Internet_Voting_UOCAVA.pdf.

Drew Springal, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Maggie MacAlpine, J. Alex Haldermann, "Security Analysis of the Estonian Internet Voting System," *Proceedings of the 21st ACM Conference on Computer and Communications Security* (CCS '14) (November 2014), https://estoniaevoting.org/findings/paper/.

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
FORT WORTH DIVISION

THOMAS E. PEREZ [now R. ALEXANDER ACOSTA], Secretary of Labor, Plaintiff,	
v.	Civil Action No. 4:16-CV-1057-A
ASSOCIATION OF PROFESSIONAL FLIGHT ATTENDANTS, Defendant.	

STIPULATION

Plaintiff, the Secretary of Labor, stipulates as follows for all purposes in this action:

In giving deposition testimony in this case on June 13, 2017 with respect to various Department of Labor ("DOL") policies and practices deemed relevant by Defendant, Stephen J. Willertz was authorized to testify and did testify on the DOL's behalf within the meaning of Fed. R. Civ. P. 30(b)(6).

Respectfully submitted,

JOHN R. PARKER
UNITED STATES ATTORNEY

Brian W. Stoltz

Brian W. Stoltz
Assistant United States Attorney
Texas Bar No. 24060668
1100 Commerce Street, Third Floor
Dallas, Texas 75242-1699
Telephone: 214-659-8626
Facsimile: 214-659-8807
brian.stoltz@usdoj.gov

Attorneys for Plaintiff

Dated: June 30, 2017

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
FORT WORTH DIVISION

THOMAS E. PEREZ [now R. ALEXANDER ACOSTA], Secretary of Labor,	
Plaintiff,	Civil Action No. 4:16-CV-1057-A
v.	
ASSOCIATION OF PROFESSIONAL FLIGHT ATTENDANTS,	
Defendant.	

PLAINTIFF'S RESPONSES TO DEFENDANT'S FIRST SET OF INTERROGATORIES

Plaintiff, the Secretary of Labor, provides the following responses to the first set of interrogatories served by defendant, the Association of Professional Flight Attendants:

1. Describe in detail the method used or steps taken to "match the names of 4,082 voters out of 9,355 votes cast to their choice of candidates," as alleged in Paragraph 23 of the Complaint.

Response:

1. During its investigation, the Department of Labor Office of Labor-Management Standards (OLMS) received data contained in the EID15-VotesTable (Votes Table), which was maintained on the Election Server. This Votes Table data was received in the form of an Excel spreadsheet. OLMS also received data from the EID15-OEM-data-20160909-104048 table ("OfficersElectionMembers" table), which was maintained on the

Member Registration and Notification Server (MRNS), and which was provided by BallotPoint on September 12, 2016. This MRNS data was received in the form of a text file, which was converted to an Excel spreadsheet for readability. Each set of data contained information regarding votes cast over the Internet and by telephone.

2. The Votes Table consisted of a line of data for each vote cast. Each row contained a number of fields showing attributes of the voter, including the IP address or area code from which the vote was cast, the exact time the vote was cast, the "vote string" showing the voting choices, and the voter's domicile.

3. The MRNS data consisted of a line of data for each member who logged in to vote. Each row contained a number of fields showing attributes of the member, including the IP address from which the member voted, the date and eight-hour window during which the member voted, the member's name, and the member's domicile.

4. OLMS was able to match the names of voters to the particular vote that they cast by comparing the data from the Votes Table to the MRNS data.

5. OLMS used a different method to match the APFA member to his or her vote depending on if the vote was cast by Internet (including web-browsing capability of cell phones) or by telephone (call-in). In analyzing votes cast by Internet and telephone (call-in), OLMS began by reviewing the data line-by-line and cross-referencing individual lines of the MRNS data with those from the Votes Table. OLMS initially connected voters to votes via this "line-by-line data analysis method." Given the large amount of data, OLMS subsequently used automated processes in Excel and Access to more quickly make voter-to-vote connections, a process referred to as the "automated data analysis method."

Voter-to-Vote Matches Made for Votes Cast by Internet

Line-by-line data analysis method: Votes cast by Internet

6. Stephen Willertz and Tracy Shanker began by cross-referencing individual lines of the MRNS data with individual lines of data from the Votes Table, analyzing three fields across both the MRNS data and the Votes Table: (1) IP address; (2) date/time information; and (3) voter's domicile, following the steps below.

7. They identified a unique IP address in the MRNS data.

8. They searched for that same unique IP address in the Votes Table.

9. When the search revealed only one result, they determined that they had likely matched voter with vote. To ensure that they had established a match, they verified that two additional fields (*i.e.*, domicile and date/time information) also matched.

10. Once the unique IP address, domicile, and date/time information were matched, then the voter's name from the MRNS data could be linked to the voter's vote string, establishing that the voter's choices for each race could be linked.

11. When IP addresses from the MRNS table search revealed more than one matching IP address in the Votes Table, they analyzed the date/time ("oem_access_when") field.

12. The "oem_access_when" field in the MRNS table contains the voting date and the time of voting, recorded in eight-hour windows. Specifically, when the time of voting was between 12:00 a.m. midnight and 7:59 a.m., the time was listed as "0000." When the time of voting was between 8:00 a.m. and 3:59 p.m., the time was listed as "0800." When the time of voting was between 4:00 p.m. and 11:59 p.m., the time was listed as "1600." As an example, if a member voted on January 6, 2016, at 9:34 p.m., the "oem_access_when" field in the MRNS table would read "20160106-1600."

13. As stated above, the Votes Table lists the exact time of voting in the "timestamp" field; time is listed in military time format (hour/minutes/second). Utilizing the example above, if a member voted on January 6, 2016, at 9:34 p.m., the "timestamp" field would read "2016-01-06 21:34:22.000."

14. When Willertz and Shanker compared the date/time information in the MRNS table and Votes Table, and obtained more than one unique IP address to establish the match, then they analyzed the domicile ("oem_attr1") field to eliminate non-matches. To illustrate, the Votes Table sometimes contained more than one row with a date/time [hour/minute/second] that fell within the MRNS table's "date and eight-hour window" field associated with the IP address in question. In these cases, analyzing the domicile field usually enabled Willertz and Shanker to eliminate non-matches to find the one matching set of data.

15. In some instances, the data analysis steps outlined above did not reveal a one-to-one match because two different members voted from the same IP address, during the same eight-hour window, and were based in the same

domicile. (For example, this appeared to occur when two flight attendants resided at the same physical address.) Willertz and Shanker were still able to connect voter with vote in this situation when the two voters' respective vote strings were identical.

Automated data analysis method: Votes cast by Internet

16. William Mitchell used Excel and Access to analyze the MRNS data and data from the Votes Table. This method included the following steps.
17. He used Excel to sort the Votes Table data and the MRNS data to identify all votes cast via Internet.
18. Utilizing one working spreadsheet, he copied data for all Internet voters into separate worksheets, and then sorted/filtered the data to isolate unique IP addresses.
19. Using Excel's conditional formatting function, he identified and highlighted all of the duplicate IP addresses. He filtered the data to select all highlighted cells (*i.e.*, cells indicating duplicate IP addresses), and then applied a filter to select all of the *non*-highlighted cells (*i.e.*, cells indicating *unique* IP addresses). He then copied the unique IP addresses from the Votes Table and the MRNS data into separate worksheets within the same working spreadsheet, and did the same with the duplicate IP addresses.
20. He imported the unique IP addresses data (from the Votes Table and MRNS data) into Access, and created an Access query that matched all of the unique IP addresses from the Votes Table with those from the MRNS data. This query established a connection between voter and vote for approximately 3,421 members.
21. The 3,421 figure includes ten votes for which the IP addresses from the Votes Table data and MRNS data did not completely match for unknown reasons. However, because both the domiciles and the timestamps/eight-hour voting windows match up in each instance, OLMS determined that these ten rows of data were highly likely to reflect voter-to-vote connections.
22. To establish a connection between voter and vote for the duplicate IP addresses, he copied and pasted the duplicate IP addresses from Votes Table and MRNS data side-by-side in a separate worksheet within his working spreadsheet. He needed to revert to the line-by-line data analysis method to attempt to make voter-to-vote matches for duplicate IP addresses. These data fit into these four general categories:

a. Votes from duplicate IP addresses where the votes were cast in different eight-hour windows (*match between voter and vote could be made when the votes were cast during different eight-hour windows*).

b. Votes from duplicate IP addresses where votes were cast in the same eight-hour time window, but the domiciles were different (*match between voter and vote could be made when the domiciles were different*).

c. Votes from duplicate IP addresses where the votes were cast in the same eight-hour window, and the domiciles were the same, but the vote string was identical (*indicating that a match between voter and vote was made*).

d. Votes from duplicate IP addresses where the votes were cast in the same eight-hour time window, and where the domiciles were the same, but the vote strings were different (*no match between voter and vote could be made*).

A total of 433 voter-to-vote matches were made by using this "line-by-line" method to analyze duplicate IP addresses.

23. The "automated" and "line-by-line" data analysis methods resulted in approximately 3,854 matches of voter and vote. These 3,854 matches comprise 41.2% of the total number of ballots cast (9,355) in APFA's January 9, 2016 election.

<u>Voter-to-Vote Matches Made for Votes Cast by Telephone</u>

24. With respect to the votes cast by telephone (call-in), OLMS was again able to match the names of voters to their vote using two methods; first, by reviewing the data line-by-line and cross-referencing the MRNS data and the Votes Table data; and second, by using automated processes in Excel and Access to analyze the large volume of data more quickly.

Line-by-line data analysis method: Votes cast by telephone

25. Willertz initially compared the MRNS data showing members who had voted by telephone to the Votes Table data showing the votes of the members who had voted by telephone.

26. He examined the MRNS data for all telephone voters within a particular eight-hour voting window.

27. Within one particular eight-hour voting window, he identified rows of data in which there was only one *voter* from one particular domicile who voted within that eight-hour period.

28. He searched the Votes Table for all telephone votes within that same eight-hour window, and identified any rows of data in which only *one* telephone vote was received from a voter in the domicile that was just identified in the MRNS table. When he identified only one telephone voter from a particular domicile (in one eight-hour window) and only one vote string from a telephone voter from that same domicile (in the same eight-hour window), he was able to successfully connect the voter with voter with his or her vote.

Automated data analysis method: Votes cast by telephone

29. Mitchell filtered the Votes Table and the MRNS data table to identify only the votes cast by telephone. He copied and pasted this data (side-by-side) on a separate worksheet within his working spreadsheet.

30. He sorted the data from the Votes Table by "timestamp" (*i.e.*, time of voting, down to the second) and then by "attr1" (*i.e.*, domicile).

31. He sorted the MRNS data by "oem_access_when" (*i.e.*, time of voting, in eight-hour window format), and then by "oem_attr1" (*i.e.*, domicile).

32. Using Excel's subtotal command, he identified how many telephone votes were cast on each date and during each eight-hour window.

33. He then used Excel's conditional formatting feature to highlight all the *duplicate values* based on "attr1" (*i.e.*, domicile) in each subtotal grouping – for both the Votes Table data and for the MRNS data. The unique "attr1" (*i.e.*, domicile) rows in the Votes Table and the MRNS data were now easily identified – since they were all the rows that were *not* highlighted.

34. He used Excel to filter the *non*-highlighted "attr1" (*i.e.*, domicile) rows, and subsequently copied and pasted that data from the Votes Table and the MRNS data side-by-side in a separate worksheet within his working spreadsheet.

35. The result of Mitchell's analysis is an additional 227 voter-to-vote matches.

To conclude, the data analysis of the votes cast by Internet (including the web-browsing capability of cell phones) undertaken by Willertz, Mitchell, and Shanker resulted in 3,854 matches of voter and vote. Adding these 227 voter-to-vote matches for votes cast by telephone (call-in) resulted in matching a total of 4,081 voters to the voters' choice of candidates. These 4,081 matches comprise 43.6% of the total number of ballots cast (9,355) in APFA's January 9, 2016 election. Note that this figure is one match fewer than the 4,082 reported in the complaint. That figure included an extra header row in Excel which did not actually include a matched vote and should have been disregarded. Thus the total number of matched votes was actually 4,081 rather than 4,082.

* * * * * * *

2. Describe in detail the complete factual basis for your contention in Paragraph 27 of the Complaint that the violation of 29 U.S.C. § 481(a) alleged by You in the Complaint may have affected the outcome of the APFA's election for the offices of National President, National Vice President, National Secretary, and National Treasurer.

Response:

The ES records indicate that 9,355 of 20,656 eligible APFA members voted in at least one of the four national officer races during the January 9, 2016 national officer election using BallotPoint's electronic voting system, specifically its "One-Vote-No-Void" or "OVNV" method.

This voting system stored and maintained member-identifying information and voting records on two servers in a way that could allow individuals with access to both servers to identify how a member voted. Member records, including voter email addresses are stored on the MRNS while members' votes are stored on the ES. A link between these two servers, and thus between the voters and their votes, is evident because the system is capable of sending a confirmation email message to the voter after the voter has voted successfully or after a voter has voted, but the system has malfunctioned, so that the voter is notified that he or she must vote again. In addition, when election administrators submitted support requests, the information generated by the system viewable to BallotPoint Engineers could be combined with member information known by the election administrators to link the particular member who requested support to his or her vote. Accordingly, the fact that the voters voted using a balloting method that permitted their identities to be identified with their choices tainted all votes cast and the integrity of the election, and the national officers who were subsequently installed in their posts after the election also were not elected by "secret ballot" as required by 29 U.S.C. § 481.

Moreover, when OLMS analyzed the data maintained in the system, as described in the response above, it was able to match over 40% of the individual members to their voting choices. Even assuming that the only effect on the election is the percentage of votes for which OLMS could make a connection, these 4,081 votes far exceeded every margin in the national officer election. In addition, the "winning" vote margins of the candidates who advanced to a run-off and/or won their races were such that if it is assumed that all of the affected voters had cast their votes for the losing candidates, different outcomes would have occurred.

Further, while 9,355 members voted in at least one of the national officer races, over 11,000 members did not vote in any race, and if the election had been conducted with a secret ballot it is possible that these non-voting members would have voted and that their votes would have changed the election outcome.

Finally, under LMRDA case law, proof that a ballot-secrecy violation occurred creates a presumption that the outcome of the election may have been affected, and the

APFA bears the burden of providing genuine, tangible, and probative evidence that there was no effect on the outcome of the election.

* * * * * * *

3. Describe in detail the complete factual basis for your contention in Paragraph 27 of the Complaint that the violation of 29 U.S.C. § 481(c) alleged by You in the Complaint may have affected the outcome of the APFA's election for the offices of National President, National Vice President, National Secretary, and National Treasurer.

Response:

The following facts highlight the defects of the electronic voting system which do not permit a candidate's observer to verify that a vote was recorded and tallied accurately:

1. No tangible permanent record of the votes cast, paper or otherwise, independent of the computer system was maintained which would have allowed a manual recount to verify the electronic count.
2. No tangible permanent record, paper or otherwise, independent of the computer system was maintained which would have demonstrated that votes were received from each voter.
3. The APFA Board of Directors voted against providing observers with observer access to the BallotPoint system, which would have allowed candidates or their observers to log onto the BallotPoint website to access the Vote Digests.
4. Two BallotPoint system generated reports, the "Who Voted" and the "Who Did Not Vote" reports, were not made available to observers.
5. Candidates and their observers were only permitted to see the results of the election on a screen at the APFA headquarters; they could not observe the ballot-tallying process nor could they confirm that the tally presented was the authenticate tally sent from BallotPoint .
6. BallotPoint's election system is not accessible for inspection by members or their agents; moreover, its complicated highly-technical design makes it

highly unlikely that a union member could discern whether it was functioning to only count votes from eligible voters and to accurately count those votes.

7. The lack of tangible records or any method of inspecting the accuracy of the system in assigning and counting votes makes effective auditing of the system impossible.
8. BallotPoint did not maintain its system at the time of the election so that election records could be accessed by observers; in fact, by design, its system did not retain a record of the confirmation emails sent to members and its system automatically deleted support request records after sixty days.
9. BallotPoint/CCComplete is located in Portland, Oregon, while the APFA headquarters is located in Euless, Texas.
10. The two servers and the logs showing software modifications for the BallotPoint election system are located in a separate facility, LightPoint, in Portland, Oregon, to which APFA members do not have access.
11. The election vendor, Allied Media, located in Fenton, Michigan, used a program to erase its records so that they could not be used to check which members received ballots and their access codes.
12. There were irregularities; 19 extra votes were present on the MRNS. OLMS has not yet been able to confirm the reason for this irregularity or if related irregularities exist, and this information was not presented to voters and/or observers.
13. Ten voters who were on the Who voted list were also on the Ineligible voter list. OLMS has not yet been able to confirm the reason for this irregularity or if related irregularities exist, and this information was not presented to voters and/or observers.
14. In analyzing the data maintained by the MRNS and the ES servers, it appears that the system may have improperly recorded some votes as having come from multiple IP addresses. OLMS has not yet been able to confirm the reason for this irregularity or if related irregularities exist.
15. The BallotPoint electronic voting system did not utilize client-side encryption, necessary to protect the security of the votes cast by members' computers or telephones.

Once it is established that a candidate was denied the opportunity to have an observer at the polls and the counting of the ballots, there is a presumption that the violation "may have affected the outcome of the election." Defendant bears the burden of providing genuine, tangible, and probative evidence that the failure to provide candidate's the right to have an observer at the polls did not affect the outcome of the election. Because the system provides no method of proving that the votes were properly transmitted from the voters or counted as cast, it is not possible to provide such proof.

Respectfully submitted,

JOHN R. PARKER
UNITED STATES ATTORNEY

Brian W. Stoltz

Brian W. Stoltz
Assistant United States Attorney
Texas Bar No. 24060668
1100 Commerce Street, Third Floor
Dallas, Texas 75242-1699
Telephone: 214-659-8626
Facsimile: 214-659-8807
brian.stoltz@usdoj.gov

Attorneys for Plaintiff

<u>Certificate of Service</u>

On May 25, 2017, I served the foregoing document on defendant, the Association of Professional Flight Attendants, by mailing it by prepaid first-class mail (CMRRR 7016 2070 0001 0698 1138) to defendant's counsel of record, addressed as follows:

Andrew D. Roth
Bredhoff & Kaiser, P.L.L.C.
805 Fifteenth St., N.W., Tenth Floor
Washington, D.C. 20005

Brian W. Stoltz
Brian W. Stoltz
Assistant United States Attorney

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
FORT WORTH DIVISION

THOMAS E. PEREZ [now
R. ALEXANDER ACOSTA],
Secretary of Labor,

Plaintiff,

v.

ASSOCIATION OF PROFESSIONAL
FLIGHT ATTENDANTS,

Defendant.

Civil Action No. 4:16-CV-1057-A

DECLARATION OF STEPHEN J. WILLERTZ

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury under the laws of the United States that the responses to the interrogatories contained in Plaintiff's Responses to Defendant's First Set of Interrogatories in this action are true and correct to the best of my knowledge.

Executed on this 25th day of May, 2017, at Washington, D.C.

Stephen J. Willertz

Stephen J. Willertz
Director of the Office of Field Operations
Office of Labor-Managements Standards
U.S. Department of Labor

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
FORT WORTH DIVISION

R. ALEXANDER ACOSTA, Secretary of Labor, Plaintiff, v. ASSOCIATION OF PROFESSIONAL FLIGHT ATTENDANTS, Defendant.	Civil Action No. 4:16-cv-1057-A

DEFENDANT APFA'S ANSWERS TO PLAINTIFF DOL'S FIRST SET OF INTERROGATORIES

Defendant, the Association of Professional Flight Attendants ("APFA"), hereby answers the first set of interrogatories propounded on it by the Plaintiff, R. Alexander Acosta, acting in his official capacity as the Secretary of Labor.

APFA has not completed its investigation of all the facts relating to this litigation. All of the objections and answers contained herein are based only on the information, documents, and sources that are presently available and known to APFA, based on a reasonable and ongoing investigation of available sources. APFA expressly reserves its right to supplement, clarify, revise, or correct any or all of the objections and answers, and to supplement its objections, and answers, as well as its assertions of privileges, as appropriate.

APFA objects generally to Plaintiff's interrogatories to the extent they call for information protected by the attorney-client privilege or the attorney work-product doctrine.

Each of Plaintiff's interrogatories is set forth in bold preceding APFA's answer and/or objections to that interrogatory.

INTERROGATORY NO. 1: Describe in detail the complete factual basis for the APFA's denial of the contention in paragraph 27 of Plaintiff's original complaint that the violation of 29 U.S.C. § 481(a) alleged by Plaintiff in the original complaint may have affected the outcome of the APFA's election for the offices of National President, National Vice President, National Secretary, and National Treasurer at issue in this action.

At this point in time, the facts known to APFA which support this denial are as follows:

1. In his internal union complaint, *see* DOL 0087, Samuel Morales stated no basis for his "feel[ing]" that APFA violated the ballot secrecy provision of the LMRDA. Nor did he assert (much less point to any evidence) that the secrecy of any union member's vote had actually been compromised, or that any member had claimed that a concern about ballot secrecy impacted how, or if, that member voted.

2. In his subsequent complaint to the DOL, *see* DOL 0001, Mr. Morales likewise stated no basis for his "belie[f]" that APFA violated the ballot secrecy provision of the LMRDA. Nor did he assert (much less point to any evidence) that the secrecy of any union member's vote had actually been compromised, or that any member had claimed that a concern about ballot secrecy impacted how, or if, that member voted.

3. The Complaint Interview Questionnaire prepared by DOL investigator Keith King, *see* DOL 0139, states that Mr. Morales was interviewed by the DOL on March 8 and 17, 2016, and that in his interview Mr. Morales stated "that he couldn't single out any particular evidence to support his statement that he felt that APFA violated . . . the ballot secrecy provision of [the LMRDA]."

4. In his deposition, Stephen J. Willertz testified that, to his knowledge, during the course of the DOL's investigation, neither Mr. Morales nor any other union member expressed a

concern that—to quote paragraph 21 of the DOL's Complaint in this matter—"[t]he [BallotPoint] system stores and maintains member identifying information and voting records on two servers in a way that could allow individuals with access to both of the servers to identify how a member voted." *See* Willertz Dep. at 45-47.

5. In his deposition, Mr. Willertz further testified that based on the evidence "noted" in the DOL's investigation, "[t]here is just no way" that voters in the challenged APFA election could have made "any sort of assessment as to whether or not votes and voters could be connected." *See* Willertz Dep. at 41-42.

6. Along the same lines, an Interrogatory Response signed by Mr. Willertz states that "BallotPoint's election system is not accessible for inspection by members or their agents; moreover, its complicated highly-technical design makes it highly unlikely that a union member could discern whether it was functioning to only count votes from eligible voters and to accurately count those votes," *see* Responses at pp. 9-10, and Mr. Willertz admitted in his deposition testimony that the same considerations make it "highly unlikely, if not impossible, that a member could discern that there is data on the two servers that could be connected up to link a voter with the vote," *see* Willertz Dep. at 226-27.

7. A Statement of Reasons disposing of a prior election challenge brought by Mr. Morales, *see* Willertz Dep., Exh. 18, coupled with the two election complaints filed by Mr. Morales in this matter, *see* subparagraphs 1-2 above, show that Mr. Morales challenged the national officers' election at issue here on secret ballot grounds because the DOL had planted a seed in Mr. Morales' head that the BallotPoint system did not adequately ensure ballot secrecy, and not because Mr. Morales had an independent feeling or belief that such was the case.

Discovery in this action is ongoing, and APFA anticipates that it will be able to develop additional facts in support of its denial in the course of that discovery.

INTERROGATORY NO. 2: Describe in detail the complete factual basis for the APFA's denial of the contention in paragraph 27 of Plaintiff s original complaint that the violation of 29 U.S.C. § 481(c) alleged by Plaintiff in the original complaint may have affected the outcome of the APFA's election for the offices of National President, National Vice President, National Secretary, and National Treasurer at issue in this action.

At this point in time, the facts known to APFA which support this denial are as follows:

1. The facts and opinions set out in Part III.B of Curt Stapleton's expert report, which APFA provided to the Secretary on June 30, 2017, and which Mr. Stapleton likely will be called upon to elaborate on in his forthcoming deposition.

2. The facts and opinions summarized in Part (ii)(6) of the Rule 26(a)(2)(C) Disclosure pertaining to Gerry Feldkamp's anticipated expert testimony, which APFA provided to the Secretary on June 30, 2017, and which Mr. Feldkamp likely will be called upon to elaborate on in his forthcoming deposition.

3. Mr. Feldkamp, Mike Baum, and Bob Thompson, the three BallotPoint engineers with privileged access to the BallotPoint system, are anticipated to confirm that they did not engage in any form of misconduct or tampering with the software application related to the recordation and counting of votes in the challenged APFA election. And BallotPoint's business reputation and track record, among other factors, stand as independent confirmation of this fact.

4. In his deposition, Mr. Willertz testified that "I don't have any evidence that the results [of the election] are inaccurate or wrong." *See* Willertz Dep. at 249.

5. In his deposition, Mr. Willertz further testified that a "spot check" of the underlying vote data in the election disclosed nothing irregular. *See* Willertz Dep. at 265-66.

6. There are no facts, and the DOL has cited none, that raise a reasonable possibility that the alleged violation of 29 U.S.C. § 481(c) may have affected the outcome of the challenged APFA National Officer Elections.

Discovery in this action is ongoing, and APFA anticipates that it will be able to develop additional facts in support of its denial in the course of that discovery.

INTERROGATORY NO. 3: Describe in detail all ways in which candidates' observers were permitted to observe any aspect of the APFA's election for the offices of National President, National Vice President, National Secretary, and National Treasurer at issue in this action, including how and when the candidates and/or their observers were notified of any observer opportunities.

1. Candidates were permitted to inspect (but not copy) the membership list once within the thirty (30) days prior to the mailing of the ballots. Candidates are permitted to inspect (but not copy) the membership list and a list of the voting members from the previous National Officer elections once within forty-five (45) days prior to the mailing or electronic availability of the ballots. Candidates were informed of these opportunities through the form candidate letter sent by Cindy Horan to all candidates. *See* DOL0397-DOL0401. In addition, the complainant in this matter, Samuel Morales, was advised, in a December 24, 2015 email from National Ballot Committee Chairperson Cindy Horan, that he could review a list of eligible voters and a list of ineligible members at the ballot count. *See* APFA-00000252, APFA-00000262.

2. Observers were permitted to observe the preparation and mailing of the ballots (that is, the voting credentials prepared and mailed by Allied Media). Candidates were informed of this opportunity through the form candidate letter sent by Cindy Horan to all candidates. *See* DOL0397-DOL0401.

3. Observers were provided by the APFA National Ballot Committee with a daily list of the APFA members who became eligible to vote after the ballots (that is, the voting

credentials prepared and mailed by Allied Media) had been mailed. Observers had 48 hours to challenge the eligibility of any newly eligible member. Candidates were informed of this opportunity through a candidate letter sent by Cindy Horan to all candidates on December 10, 2015. *See* APFA-00000290-APFA-00000291. Candidates were also informed of this opportunity in the APFA Policy Manual, § 14.O. *See* APFA-00000216.

4. Observers were permitted to attend the APFA ballot count at APFA Headquarters. Candidates were informed of this opportunity through the form candidate letter sent by Cindy Horan to all candidates. *See* DOL0397-DOL0401. Candidates were also informed of this opportunity in the APFA Policy Manual, § 14.Q. *See* APFA-00000218- APFA-00000219. In addition, any member in good standing was permitted to observe the ballot count from gallery space. Members were informed of this opportunity in the APFA Policy Manual, § 14.Q. *See* APFA-00000219.

5. Candidates were permitted to request to view the Who Voted and Who Did Not Vote Reports after the ballot count. Information regarding a candidate's right to view these reports was not communicated to candidates in a formal communication, but would be shared with candidates in response to candidate inquires regarding which members voted. In addition, the complainant in this matter, Samuel Morales, was advised, in a December 24, 2015 email from National Ballot Committee Chairperson Cindy Horan, that he could review a list of the members who voted at the ballot count. *See* APFA-00000252, APFA-00000262.

Respectfully submitted,

Andrew D. Roth

ANDREW D. ROTH*
D.C. Bar No. 414038
ROBERT ALEXANDER*
D.C. BAR No. 465673
ADAM BELLOTTI*
D.C. Bar No. 1020169
Bredhoff & Kaiser, P.L.L.C.
805 Fifteenth St. N.W., Tenth Floor
Washington, D.C. 20005
Tel: (202) 842-2600
Fax: (202) 842-1888
Email: aroth@bredhoff.com
Email: ralexander@bredhoff.com
Email: abellotti@bredhoff.com

SANFORD R. DENISON
Texas Bar No. 05655560
Baab & Denison, LLP
6301 Gaston Avenue, Suite 550
Dallas, TX 75214
Tel: (214) 637-0750
Fax: (214) 637-0730
Email: denison@baabdenison.com

Attorneys for Defendant Association
of Professional Flight Attendants

* Admitted Pro Hac Vice

Dated: July 12, 2017

Verification

I, Cindy Horan, do verify under penalty of perjury that I have read Defendant's Answer to Plaintiff's Interrogatory No. 3 and know its contents. I am informed and believe that the factual matters set out in the above response are true and accurate to the best of my knowledge, information, and/or belief.*

Cindy Horan

Cindy Horan
APFA National Ballot Committee Chairperson

* The APFA's Answers to Interrogatories 1 and 2, which are in the nature of contention interrogatories, have been prepared by undersigned counsel on the preceding page.

DATED: July 10, 2017

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on the 12th day of July, 2017, the above and foregoing document was served on Plaintiff's counsel of record electronically by email transmission and by USPS, First Class mail, postage prepaid, as authorized by Federal Rule of Civil Procedure 5(b), addressed to the following:

Brian W. Stoltz
Assistant United States Attorney
1100 Commerce Street, Third Floor
Dallas, Texas 75242-1699
Telephone: 214-659-8626
Facsimile: 214-659-8807
brian.stoltz@usdoj.gov

ADAM BELLOTTI

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF TEXAS

FORT WORTH DIVISION

THOMAS E. PEREZ, [now)
R. ALEXANDER ACOSTA],)
Secretary of Labor,)
Plaintiff,)
)
VS.)NO. 4:16-CV-1057-A
)
ASSOCIATION OF PROFESSIONAL)
FLIGHT ATTENDANTS,)
Defendant.)

DEPOSITION OF GERRY FELDKAMP

TAKEN ON BEHALF OF PLAINTIFF

* * *

BE IT REMEMBERED THAT, pursuant to the Federal Rules of Civil Procedure, the deposition of GERRY FELDKAMP was taken before Paula D. Tieger, a Registered Professional Reporter and Notary Public for the State of Oregon, on July 14, 2017, commencing at the hour of 9:29 a.m., in the office of McKanna, Bishop, Joffe, 1635 NW Johnson Street, Portland, Oregon.

* * *

APPEARANCES:

U.S. Department of Justice
United States Attorney's Office
By: Brian W. Stoltz
Assistant United States Attorney
1100 Commerce Street, Suite 300
Dallas, Texas 75242
214-659-8626
brian.stoltz@usdoj.gov
Counsel for the Plaintiff

McKanna Bishop Joffe
By: Noah Scott Warman
Attorney at Law
1635 NW Johnson Street
Portland, Oregon 97209
503-821-0959
nwarman@mbjlaw.com
Counsel for CCComplete Election Services

Bredhoff & Kaiser
By: Robert Alexander
Attorney at Law
805 Fifteenth Street, NW
Washington, DC 20005
202-842-2600
ralexander@bredhoff.com
Counsel for Association of Professional Flight Attendants

Also Present: Joe Kiniry, Tambra Leonard,
Dan Hilderbrand

* * *

A Yes.

Q And you understand that this lawsuit concerns specifically the APFA's national officer election that occurred around balloting, for the first round at least, 09:48:14 concluded in 2016?

A Correct. Yeah.

Q Okay. And are you aware that the Secretary of Labor has sued the APFA under a theory that the election did not protect ballot secrecy, and that observers in the 09:48:32 election were not allowed to tally and -- or to verify or observe that the ballots were tallied and recorded accurately?

A I am aware of that.

(Exhibit No. 1 was marked)

09:49:08 Q BY MR. STOLTZ: I've handed you, Mr. Feldkamp, a document that's marked as Exhibit 1. And I'll tell you that this document was provided to me by the lawyers for the APFA and is signed by, I believe, Adam Bellotti, who is one of the lawyers.

09:49:26 Do you recognize Exhibit 1?

(The witness reviews the document)

THE WITNESS: Yes, I do.

Q BY MR. STOLTZ: And what is Exhibit 1?

A Defendant APFA's Rule 26(a)(2)(C) disclosure of Gerry 09:50:01 Feldkamp.

Q It's fair to say, in this document, the APFA has informed us that it may present testimony from you about various subjects; is that what you understand this to mean?

09:50:12 A Correct.

Q And did you work with or talk with the APFA's lawyers about the preparation of this document, Exhibit 1?

A Yes.

Q And did you actually review this document as it exists in its present form before it was sent to me? 09:50:28

A Yes.

Q Now, there is -- the document is divided into a summary of opinions and a summary of factual explanations.

09:50:52 For example, on page 2, do you see where it says Opinion and Factual Explanations?

A I do.

Q Is it fair to say that the explanation of the opinions in this document which are said to be your opinions, is it true that those are, in fact, your opinions? 09:51:07

A These are my opinions.

Q Okay. And the same question for the factual explanation.

09:51:15 Is it true that the explanation of factual explanations here is your explanation?

A Yes.

Q So, you adopt this document, essentially, as if it were your own testimony?

09:51:27 A Correct.

Q Can you provide a brief -- and we will get back to that document later.

Can you provide us a brief overview of how the BallotPoint system works for the type of election that is 09:51:53 at issue here -- well, specifically -- let me start over.

When we're talking about the BallotPoint system here, can we agree that we're talking about the BallotPoint system as it existed and was used at the time of the APFA national officer elections?

09:52:08 A Yes. Let's do.

Q Can you give us a brief overview in broad terms, how did that system function?

A Are you looking for an explanation beginning to end of an election, or...

09:52:25 Q Well, how about this. Physically, what is the system comprised of? Is it a single computer? Is it multiple computers? That sort of thing.

A Okay. We'll start there. The hardware consists of two -- and we'll call them virtual entities here. One's 09:52:43 called the MRNS for member registration and notification

vote, creating its message digest, comparing it against
what exists now at that moment on the MRNS, and say, oh,
it's already there.

Q So, am I understanding correctly that a singly
10:26:03 encrypted vote is briefly created on the MRNS in order to
then create a doubly encrypted vote that's sent to the
ES?

A No, that's not correct.

Q Okay. Then is there ever a singly encrypted vote in
10:26:21 existence anywhere?

A It begins as part of the encryption process on the
election server. That singly encrypted vote is passed to
the MRNS. So, the MRNS receives that. It uses that to
create the doubly encrypted vote from which the vote
10:26:40 digest is created, and it also uses that singly encrypted
vote and it creates a message digest of that for storage.

Q So, the MRNS receives the singly encrypted vote, uses
that singly encrypted vote to create a message digest and
a vote digest, and then discards or does not retain the
10:26:59 singly encrypted vote; is that correct?

A That is correct.

Q Thank you.

A Okay.

(Exhibit No. 3 was marked)

10:27:15 Q BY MR. STOLTZ: Okay. Mr. Feldkamp, you have a document now that's been marked as Exhibit 3.

Do you recognize what this document is?

(The witness reviews the document)

THE WITNESS: Yes, I do.

10:27:59 MR. STOLTZ: Okay.

Q BY MR. STOLTZ: And what is it?

A The official results -- the printed results from the national officer election of 2016.

Q Now, if we look on Exhibit 3, the first grouping is 10:28:17 the candidates for national president.

Do you see where it says that?

A Yes.

Q And I just want to make sure I understand the relationship between these totals on Exhibit 3 that are 10:28:26 given, which are the votes for each of the candidates. I want to make sure I understand the relationship between those totals and the votes table, which is on Exhibit 2. So, if you can please look at Exhibit 2, if you have it. Now, the first candidate who is listed here under 10:28:42 national president on Exhibit 3 is Lori Bassani.

Do you see that?

A Yes, I do.

Q Okay. And Exhibit 3 reflects that Lori Bassani received 599 votes; is that right?

10:28:55 A It says so. Yes.

THE WITNESS: Correct.

Q BY MR. STOLTZ: What is Exhibit 9?

A This is my description of the One-Vote, No-Void process.

11:53:27 Q And does Exhibit 9 accurately explain the election method that was used in the election at issue in this lawsuit?

(The witness reviews the document)

THE WITNESS: Yes.

11:54:10 Q BY MR. STOLTZ: Now, you mentioned the -- earlier, the -- we talked about the double encryption of votes that started on the ES, and they had transferred, and then they end up on the ES as a doubly encrypted vote.

Do you remember that?

11:54:24 A Yes.

Q At BallotPoint -- and you used the phrase, I think, a vote digest or a message digest.

That's what BallotPoint refers to that system of creating these doubly encrypted votes and hashes and 11:54:38 digests; correct?

A The vote digest is a quantity produced from that.

The vote digesting or double encryption method are two ways that we refer to that process.

Q And did -- is one purpose of the vote digesting 11:54:54 process to address the observeability requirement of the

Page 130

CERTIFICATE

I, Paula D. Tieger, a Registered Professional Reporter and Notary Public for the State of Oregon, hereby certify that said witness personally appeared before me at the time and place set forth in the caption hereof; that at said time and place I reported in stenotype all testimony adduced and other oral proceedings had in the foregoing matter; that thereafter my notes were transcribed through computer-aided transcription, under my direction; and that the foregoing pages constitute a full, true and accurate record of all such testimony adduced and oral proceedings had, and of the whole thereof.

Witness my hand at Portland, Oregon, this 27th day of July, 2017.

NDTCA · Signed Electronic Transcript

Paula D Tieger

Paula D. Tieger, RPR 49286
Expires 9/30/19
Notary Public 957195
Expires 12/8/20

Feldkamp Deposition
Exhibit 1

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
FORT WORTH DIVISION

R. ALEXANDER ACOSTA, Secretary of Labor, Plaintiff, v. ASSOCIATION OF PROFESSIONAL FLIGHT ATTENDANTS, Defendant.	Civil Action No. 4:16-cv-1057-A

Defendant APFA's Rule 26(a)(2)(C) Disclosure of Gerry Feldkamp

Defendant, the Association of Professional Flight Attendants ("APFA"), hereby makes the disclosure required by Fed. R. Civ. P. 26(a)(2)(C) with respect to the expected expert witness testimony of Gerry Feldkamp:

(i) the subject matter on which the witness is expected to present evidence under Federal Rule of Evidence 702, 703, or 705:

Mr. Feldkamp is expected to present evidence under Federal Rule of Evidence 702, 703, or 705 on the following subjects:

1. Whether the BallotPoint electronic voting systém as it stood at the time of the APFA's January 9, 2016 officers' election (hereinafter, the "1/9/16 system") was designed in a manner that permitted the names of voters to be linked with their voting choices;

2. Whether the software changes to the 1/9/16 system made by BallotPoint in response to the Department of Labor's ("DOL") investigatory subpoena, had they been made by

Feldkamp
Ex. 1

BallotPoint on its own initiative, would have left a forensic trail that would have been detectable by the DOL in its investigation;

3. The accuracy of the contention in this case that the ability of BallotPoint's 1/9/16 system to send confirmation emails messages to voters is evidence of a linkage between the voters and their votes;

4. Whether software changes to the 1/9/16 system made by BallotPoint on its own initiative as a result of the DOL's investigation have now made it impossible to match the names of voters with their voting choices in the manner accomplished by the DOL in the course of its investigation;

5. Whether, under an electronic voting system of the kind used by BallotPoint, it is physically possible for an individual to observe the recording and counting of the ballots with his or her own eyes;

6. The prospect that the vote count generated by BallotPoint at the conclusion of APFA's January 9, 2016 election was either tampered with or miscalculated.

(ii) a summary of the facts and opinions to which the witness is expected to testify:

Mr. Feldkamp is expected to offer the following opinions supported by the following factual explanations:

1. **Opinion: BallotPoint's 1/9/16 system was designed in a manner that did not permit the names of voters to be linked with their voting choices at any time during or after the election.**

Factual Explanation: In support of this Opinion, Mr. Feldkamp will explain that the BallotPoint electronic voting system stores data on two servers: the Election Server (ES) and the Member Registration and Notification Server (MRNS), which are physically housed separately in a Tier 4 co-location facility (http://lightpointnw.com) and communicate solely over the Internet. Member-identity information is stored only on the MRNS; cast votes are stored on the ES. The operations of those separate servers, in turn, are controlled by software applications running on both the ES and the MRNS. This software is the part of the system that, among other things, directs the servers as to what data to collect and log, where to store that data, which users are permitted access to that data, and the manner in which such users may access it.

To permit names of voters to be linked with their voting choices would require that either: (a) the MRNS transmitted certain member-data to the ES over the Internet; or (b) the ES transmitted cast certain vote-data to the MRNS. All such transmissions are controlled by software on the two servers. The software necessary to send and/or receive such data did not exist on either server at the time of the election or at any time thereafter, until DOL-OLMS forced by subpoena that such software be written. After such software was written, only DOL-OLMS ever possessed the two strong encryption keys necessary to decrypt the extracted data.

2. **Opinion: Had BallotPoint, on its own initiative, made the software changes to the 1/9/16 system that BallotPoint ultimately was forced to make in order to comply with the DOL's investigatory subpoena, BallotPoint's actions would have left a forensic trail that would have been detectable by the DOL in its investigation.**

Factual Explanation: In support of this Opinion, Mr. Feldkamp will explain that BallotPoint Election Services proactively and voluntarily set up a process in 2007 whereby any revisions to the MRNS software would be done by BallotPoint producing a compact disc containing the software to be installed by an independent third-party (http://lightpointnw.com) over the Internet; at no time during installation is the MRNS physically accessed. The software is encrypted with keys unknown to LightPoint, to prevent it from installing unauthorized software. LightPoint maintains an archive of every such installation disk. From this archive and the encryption keys for each individual software revision, one can reconstruct the software in operation on the MRNS at any point in time since 2007. In addition, BallotPoint maintains parallel CD and electronic archives which corroborate the software archived by LightPoint. For ease of review, BallotPoint made available to DOJ a complete, unencrypted version of the MRNS software during its visit to BallotPoint on May 31 and June 1, 2017.

Had BallotPoint written MRNS software that would permit the association of voters' names to votes, the installation disks archived by LightPoint would include that software, thus leaving a forensic trail held by LightPoint. Indeed, by force of the DOL-OLMS subpoena such software was written in September 2016, resulting in a forensic trail that identifies the software steps necessary to extract such data from the 1/9/16 election record. Examination of the software existing prior to the subpoena-forced development would show that no such steps had previously existed in the BallotPoint software.

3. **Opinion: The ability of the 1/9/16 system to send confirmation email messages to voters is not evidence of a linkage between the voters and their votes.**

Factual Explanation: In support of this Opinion, Mr. Feldkamp will explain that a voter logs in to the BallotPoint system by specifying a unique "access code" to the MRNS, which verifies in its "membership-table" that the access code was issued by the MRNS, and for which election. Once verified, the MRNS sends an electronic message to the ES telling it that a voter with certain attributes (for APFA, this is the airport "base" for the member) will soon be transferred to the ES to cast his/her vote. In response, the ES returns to the MRNS a "one-time password," which is a unique "session-level tag" that identifies this voting session; this value is not stored on disk or in a database on the MRNS, and is held on the MRNS only until the voting session terminates, either by casting a vote or the session timing out (a voter is given a maximum of 20 minutes to cast a vote once logged in).

The purpose of the one-time password is to prevent disenfranchisement of a voter whose voting session ends prematurely, perhaps due to the user closing the web browser or hanging up the phone before casting a vote.

When a voter casts a vote and the vote is encrypted and stored on the ES, the last step in the voting process is for the ES to officially notify the MRNS that the voting session has ended. This is done by the ES sending the one-time password to the MRNS. No vote-information is included in this operation. The MRNS marks in its membership-table that this individual has now voted, and so will not be permitted to later re-enter the system to vote again. If the member's record in the voting roster included an email address, then an email will be sent to that address indicating that a vote has been cast using this member's account. This operation does not and cannot associate a voter with a vote, because: (a) the MRNS does not receive vote-information; (b) the one-time password that was stored in the MRNS memory is deleted immediately; (c) the one-time password is never stored with voter-identity on the MRNS; and (d) the one-time password is never stored with cast votes on the ES.

4. **Opinion: The software changes to the BallotPoint system made by BallotPoint on its own initiative as a result of the DOL's investigation in this matter have made it impossible to match the names of voters with their voting choices in the manner accomplished by the DOL in the course of its investigation.**

Factual Explanation: In support of this Opinion, Mr. Feldkamp will explain that the data used by DOL-OLMS to violate the secrecy of the 1/9/16 election were two values stored for each member in the MRNS's membership-table. These values identified the IP (Internet) address from which the member voted, and an 8-hour-resolution timestamp of the time at which the member logged in to vote. These values were used by DOL-OLMS in conjunction with IP address and timestamp data associated with votes stored on the ES to violate secrecy in the

1/9/16 election. Without the IP address and timestamp values stored on the MRNS during the 1/9/16 election, DOL-OLMS could not have associated voters' names with votes. Further, without the software added only by force of the DOL-OLMS subpoena in 2016, DOL-OLMS (and BallotPoint) could not have accessed the MRNS IP address and timestamp data, enabling it to associate voters' names with votes.

As a result of the 1/9/16 election investigation, BallotPoint has stopped logging the IP address and timestamp quantities on the MRNS as well as the ES. Therefore, associations of voters with votes in the present BallotPoint system are no longer possible. Mr. Feldkamp will further explain that, because BallotPoint has stopped collecting and storing this information, certain features, such as the ability of BallotPoint system administrators to provide voter-specific information in response to user-initiated support requests, that had been part of the BallotPoint voting system in previous elections (including the 2016 APFA National Officer Election) are no longer possible.

5. **Opinion: Under an electronic voting system of the kind used by BallotPoint, it is physically impossible for an individual to observe the recording and counting of the ballots with his or her own eyes.**

Factual Explanation: In support of this Opinion, Mr. Feldkamp will explain that the recording of cast ballots (not to be confused with the casting of ballots) on BallotPoint's servers is done by a software application running on the ES. The counting of the ballots is likewise done by a software application running on the ES after an election closes (in the 1/9/16 election, the ES software actually tallied the ballots twice, once using the plain-text versions of the votes first recorded on the ES, and once using the doubly encrypted votes stored on the ES; *see* Answer 6, below). By the nature of digital electronic systems, it is impossible for humans to physically view the actual storage/retrieval of data or the computations performed by a computer. These operations occur at space and time scales far too small for direct human observation.

6. **Opinion: There is no reasonable possibility that the vote count generated by BallotPoint at the conclusion of the APFA's January 9, 2016 election was either tampered with or miscalculated.**

Factual Explanation: In support of this Opinion, Mr. Feldkamp will explain that there are many safeguards built into and around the BallotPoint system to prevent and/or detect tampering or software errors that may cause the election results to be incorrectly calculated.

To protect against unauthorized access from the outside-world, both the Election Server (ES) and the Member Registration and Notification Server (MRNS) are front-ended by dedicated firewalls. The software protocols permitted by the firewalls are limited to those needed to run those servers.

Previous "penetration-testing" system audits tested the many input boxes that the ES and the MRNS present to users, before or after logging in. Using web proxies, auditors bypassed input-validity checks performed in JavaScript, to see if "SQL injection" and "cross-site scripting" techniques could be used to compromise the system. These attempts were thwarted because the web server software running on the ES and the MRNS also validate the inputs. The manipulated inputs were recognized as hacking attempts, and those BallotPoint sessions were force-closed. Note that no web browser controls connect directly to any database: all input is programmatically validated before data is stored in a database table.

The normal way for a voter to enter the BallotPoint system is by supplying a login credential that was previously issued by the system. APFA voters' credentials are delivered by US Mail. Each member at each election is issued a unique, randomly-generated, 12-digit "access code." If an invalid access code is entered, the user is given a few chances to get it right before the session is force-closed. The IP address from which the invalid attempts were issued is noted by the MRNS and subsequent attempts to log in from the same IP address are automatically delayed, as a deterrent to automated attempts to "guess" a valid access code. The delays are relaxed and removed only after a period of time during which no invalid access codes are entered.

Once a voter or an administrator has successfully logged in to either the MRNS or the ES, each server enforces the user's browser following a required sequence of operations and verifies that any user-input has a format consistent with the type of input. Deviations from either a sequence or format will generally cause the server to force-close the user's session. If, for example, there are two possible selections for President but the user's browser has been manipulated to indicate a vote for a third, non-existent selection, the user's session will automatically be closed, with no vote being recorded. Similarly, if the election question permits selection of two of the five candidates and the browser has been manipulated to indicate votes for three candidates, the user's session is again force-closed. This verification means that invalid votes are prevented and never stored; only valid votes are accepted by the ES.

The ES application software in use during the 1/9/16 election first recorded cast ballots as "plaintext" vote strings (which are in a human-readable format) in the ES's vote-table. The application software in use accurately recorded each voter's vote string exactly as it arrived at the ES, ensuring that all votes cast for each candidate were recorded as votes for that candidate.

The plaintext vote was then passed through a process termed "double-encryption," which has been described in detail in various submissions to DOL-OLMS. Briefly, the double-encryption process consists of: (1) the ES encrypts each vote and several pieces of ancillary data with an election-specific encryption key, to produce a "singly-encrypted vote", or SEV; (2) the

ES sends the SEV to the MRNS without any voter-identifying information, which encrypts the SEV with a different (per-vote) encryption key, to produce a "doubly-encrypted vote", or DEV; (3) the "digital fingerprint" of the DEV is calculated by the MRNS, using a well-known, cryptographic algorithm, resulting in what is termed a "vote digest"; (4) the vote digest and the MRNS's per-vote encryption key are stored on the MRNS; (5) the DEV is returned to the ES; and (6) in the 1/9/16 election, the ES stored the DEV alongside the plaintext vote in its vote-table. (Votes are no longer stored in plaintext strings.)

The net effect of the double-encryption process is that a doubly-encrypted vote is stored on the ES, while its unique digital fingerprint—the vote digest—is stored on the MRNS. Due to the ancillary data used at Step 1 in the previous paragraph, the vote digest is uniquely related to a particular DEV, and it is impossible to determine what the original plaintext vote was from a vote digest. Therefore, even if the vote digests were accessible during the period of an election, it is not possible to "count" the election while it is taking place. The only information that can be gleaned by obtaining the set of vote digests during an election would be to know how many people have voted, which is permitted in all other forms of elections.

The BallotPoint system permits the union's election administrator or other persons designated by the election administrator to download the currently stored set of vote digests at any time during an election. In the 1/9/16 election, Cindy Horan of the APFA National Ballot Committee performed this task, downloading several sets of vote digests during and just after the election period.

When it was time to tally the 1/9/16 election, the BallotPoint system first tallied the election from the votes stored as plaintext on the ES. The software to perform the tally from plaintext has been in place for more than 15 years, and has been validated many times using other methods of counting, including counting by humans.

In addition to counting directly from the votes stored as plaintext, the doubly-encrypted votes (DEVs) that were stored on the ES at Step 6 of the double-encryption process were decrypted and tallied. The double-decryption process produced exactly the same set of votes as the plaintext votes, corroborating the votes stored as plaintext and the resulting tally.

The key observation here is that for the double-decryption process (which essentially reverses Steps 1 to 6 of the double-encryption process) to run successfully, the set of vote digests stored on the MRNS must contain a vote digest corresponding to every doubly-encrypted vote (DEV) stored on the ES. If there have been any software errors or tampering compromising either the DEVs stored on the ES or the vote digests stored on the MRNS, then there would exist some DEVs for which no corresponding vote digest exists. This prevents the decryption of any such votes, and this would be reported during the decryption process. No such errors occurred, meaning that all decrypted votes were valid.

Further, the vote digests downloaded by Horan during the election all appeared in the set of vote digests existing after the election closed; these vote digests were used during the double-decryption process. This evidences that no votes were dropped during the election.

All of the above leads me to conclude that there is no reasonable possibility that tampering or software errors occurred causing a miscalculation of the tally during the 1/9/16 election. The published results accurately reflect voters' votes.

Respectfully submitted,

ANDREW D. ROTH*
D.C. Bar No. 414038
ROBERT ALEXANDER*
D.C. BAR No. 465673
ADAM BELLOTTI*
D.C. Bar No. 1020169
Bredhoff & Kaiser, P.L.L.C.
805 Fifteenth St. N.W., Tenth Floor
Washington, D.C. 20005
Tel: (202) 842-2600
Fax: (202) 842-1888
Email: aroth@bredhoff.com
Email: ralexander@bredhoff.com
Email: abellotti@bredhoff.com

SANFORD R. DENISON
Texas Bar No. 05655560
Baab & Denison, LLP
6301 Gaston Avenue, Suite 550
Dallas, TX 75214
Tel: (214) 637-0750
Fax: (214) 637-0730
Email: denison@baabdenison.com

Attorneys for Defendant Association
of Professional Flight Attendants

* Admitted Pro Hac Vice

DATED: June 29, 2017

Feldkamp Deposition
Exhibit 3

APFA
ASSOCIATION OF PROFESSIONAL FLIGHT ATTENDANTS

National Officer Election

Official Results

Ballot ending: 01/09/2016 10:00:00 (Central)

The ballots were cast and tallied as follows.

TOTAL

Please select one of the following candidates for APFA National President:	Total	Percent
Lori Bassani	599	6.41
Steven Baumert	1168	12.50
Kimberly Goesling	449	4.80
Patrick Hancock	1750	18.72
Andrea S. Jones	53	0.57
Brian Morgan	1143	12.23
Bob Ross	3151	33.71
Rock Salomon	1034	11.06
Total	**9347**	

Please select one of the following candidates for APFA National Vice President:	Total	Percent
Marcus Gluth	2632	28.91
Nena Martin	4779	52.49
Samuel Morales	1693	18.60
Total	**9104**	

Please select one of the following candidates for APFA National Secretary:	Total	Percent
Nicole Darak	2572	28.16
Marcy Dunaway	3301	36.14
Jacob Fuller	1892	20.71
Donald LeBlanc	375	4.11
Jaana Lehtola	994	10.88
Total	**9134**	

Please select one of the following candidates for APFA National Treasurer:	Total	Percent
Craig Gunter	3344	36.52
Roee Rio Harrari	147	1.61
Stefany Jones	1582	17.28
Nestor Quecuty	935	10.21
Eugenio Vargas	3148	34.38
Total	**9156**	

BOS TOTAL

Please select one of the following candidates for APFA National President:	Total	Percent
Lori Bassani	7	3.37
Steven Baumert	60	28.85
Kimberly Goesling	1	0.48
Patrick Hancock	40	19.23
Andrea S. Jones	1	0.48
Brian Morgan	5	2.40
Bob Ross	63	30.29
Rock Salomon	31	14.90
Total	**208**	

Please select one of the following candidates for APFA National Vice President:	Total	Percent
Marcus Gluth	42	20.19
Nena Martin	129	62.02
Samuel Morales	37	17.79
Total	**208**	

Please select one of the following candidates for APFA National Secretary:	Total	Percent
Nicole Darak	45	21.63
Marcy Dunaway	56	26.92
Jacob Fuller	72	34.62
Donald LeBlanc	10	4.81
Jaana Lehtola	25	12.02
Total	**208**	

Please select one of the following candidates for APFA National Treasurer:	Total	Percent
Craig Gunter	55	26.44

Feld/Kamp
Ex 3

Roee Rio Harrari	0	0.00
Stefany Jones	9	4.33
Nestor Quecuty	12	5.77
Eugenio Vargas	132	63.46
Total	**208**	

CLT TOTAL

Please select one of the following candidates for APFA National President:	**Total**	**Percent**
Lori Bassani	98	15.88
Steven Baumert	3	0.49
Kimberly Goesling	52	8.43
Patrick Hancock	119	19.29
Andrea S. Jones	7	1.13
Brian Morgan	217	35.17
Bob Ross	47	7.62
Rock Salomon	74	11.99
Total	**617**	

Please select one of the following candidates for APFA National Vice President:	**Total**	**Percent**
Marcus Gluth	211	35.95
Nena Martin	235	40.03
Samuel Morales	141	24.02
Total	**587**	

Please select one of the following candidates for APFA National Secretary:	**Total**	**Percent**
Nicole Darak	480	79.47
Marcy Dunaway	32	5.30
Jacob Fuller	27	4.47
Donald LeBlanc	24	3.97
Jaana Lehtola	41	6.79
Total	**604**	

Please select one of the following candidates for APFA National Treasurer:	**Total**	**Percent**
Craig Gunter	434	72.33
Roee Rio Harrari	19	3.17
Stefany Jones	81	13.50
Nestor Quecuty	37	6.17
Eugenio Vargas	29	4.83
Total	**600**	

DCA TOTAL

Please select one of the following candidates for APFA National President:	**Total**	**Percent**
Lori Bassani	4	3.20
Steven Baumert	29	23.20
Kimberly Goesling	1	0.80
Patrick Hancock	33	26.40
Andrea S. Jones	2	1.60
Brian Morgan	4	3.20
Bob Ross	39	31.20
Rock Salomon	13	10.40
Total	**125**	

Please select one of the following candidates for APFA National Vice President:	**Total**	**Percent**
Marcus Gluth	40	32.52
Nena Martin	62	50.41
Samuel Morales	21	17.07
Total	**123**	

Please select one of the following candidates for APFA National Secretary:	**Total**	**Percent**
Nicole Darak	24	19.35
Marcy Dunaway	34	27.42
Jacob Fuller	44	35.48
Donald LeBlanc	6	4.84
Jaana Lehtola	16	12.90
Total	**124**	

Please select one of the following candidates for APFA National Treasurer:	**Total**	**Percent**
Craig Gunter	39	31.71
Roee Rio Harrari	1	0.81
Stefany Jones	23	18.70
Nestor Quecuty	11	8.94
Eugenio Vargas	49	39.84
Total	**123**	

DCU TOTAL

Please select one of the following candidates for APFA National President:	Total	Percent
Lori Bassani	10	9.43
Steven Baumert	0	0.00
Kimberly Goesling	28	26.42
Patrick Hancock	10	9.43
Andrea S. Jones	2	1.89
Brian Morgan	38	35.85
Bob Ross	8	7.55
Rock Salomon	10	9.43
Total	**106**	

Please select one of the following candidates for APFA National Vice President:	Total	Percent
Marcus Gluth	22	21.78
Nena Martin	50	49.50
Samuel Morales	29	28.71
Total	**101**	

Please select one of the following candidates for APFA National Secretary:	Total	Percent
Nicole Darak	74	71.15
Marcy Dunaway	10	9.62
Jacob Fuller	7	6.73
Donald LeBlanc	2	1.92
Jaana Lehtola	11	10.58
Total	**104**	

Please select one of the following candidates for APFA National Treasurer:	Total	Percent
Craig Gunter	72	68.57
Roee Rio Harrari	5	4.76
Stefany Jones	11	10.48
Nestor Quecuty	8	7.62
Eugenio Vargas	9	8.57
Total	**105**	

DFW TOTAL

Please select one of the following candidates for APFA National President:	Total	Percent
Lori Bassani	73	3.14
Steven Baumert	561	24.11
Kimberly Goesling	69	2.97
Patrick Hancock	548	23.55
Andrea S. Jones	8	0.34
Brian Morgan	71	3.05
Bob Ross	802	34.46
Rock Salomon	195	8.38
Total	**2327**	

Please select one of the following candidates for APFA National Vice President:	Total	Percent
Marcus Gluth	600	26.12
Nena Martin	1356	59.03
Samuel Morales	341	14.85
Total	**2297**	

Please select one of the following candidates for APFA National Secretary:	Total	Percent
Nicole Darak	426	18.52
Marcy Dunaway	1027	44.65
Jacob Fuller	595	25.87
Donald LeBlanc	72	3.13
Jaana Lehtola	180	7.83
Total	**2300**	

Please select one of the following candidates for APFA National Treasurer:	Total	Percent
Craig Gunter	659	28.66
Roee Rio Harrari	17	0.74
Stefany Jones	411	17.88
Nestor Quecuty	174	7.57
Eugenio Vargas	1038	45.15
Total	**2299**	

LAX TOTAL

Please select one of the following candidates for APFA National President:	Total	Percent
Lori Bassani	45	5.34
Steven Baumert	57	6.76
Kimberly Goesling	11	1.30
Patrick Hancock	133	15.78
Andrea S. Jones	2	0.24
Brian Morgan	32	3.80
Bob Ross	528	62.63
Rock Salomon	35	4.15

	Total	
Total	**843**	

Please select one of the following candidates for APFA National Vice President:	**Total**	**Percent**
Marcus Gluth	234	29.14
Nena Martin	468	58.28
Samuel Morales	101	12.58
Total	**803**	

Please select one of the following candidates for APFA National Secretary:	**Total**	**Percent**
Nicole Darak	141	17.58
Marcy Dunaway	463	57.73
Jacob Fuller	113	14.09
Donald LeBlanc	26	3.24
Jaana Lehtola	59	7.36
Total	**802**	

Please select one of the following candidates for APFA National Treasurer:	**Total**	**Percent**
Craig Gunter	222	27.85
Roee Rio Harrari	8	1.00
Stefany Jones	137	17.19
Nestor Quecuty	69	8.66
Eugenio Vargas	361	45.29
Total	**797**	

LGA TOTAL

Please select one of the following candidates for APFA National President:	**Total**	**Percent**
Lori Bassani	112	10.45
Steven Baumert	74	6.90
Kimberly Goesling	14	1.31
Patrick Hancock	187	17.44
Andrea S. Jones	14	1.31
Brian Morgan	96	8.96
Bob Ross	380	35.45
Rock Salomon	195	18.19
Total	**1072**	

Please select one of the following candidates for APFA National Vice President:	**Total**	**Percent**
Marcus Gluth	270	25.54
Nena Martin	550	52.03
Samuel Morales	237	22.42
Total	**1057**	

Please select one of the following candidates for APFA National Secretary:	**Total**	**Percent**
Nicole Darak	166	15.66
Marcy Dunaway	424	40.00
Jacob Fuller	208	19.62
Donald LeBlanc	41	3.87
Jaana Lehtola	221	20.85
Total	**1060**	

Please select one of the following candidates for APFA National Treasurer:	**Total**	**Percent**
Craig Gunter	292	27.55
Roee Rio Harrari	9	0.85
Stefany Jones	188	17.74
Nestor Quecuty	174	16.42
Eugenio Vargas	397	37.45
Total	**1060**	

MIA TOTAL

Please select one of the following candidates for APFA National President:	**Total**	**Percent**
Lori Bassani	101	6.68
Steven Baumert	227	15.01
Kimberly Goesling	35	2.31
Patrick Hancock	230	15.21
Andrea S. Jones	8	0.53
Brian Morgan	65	4.30
Bob Ross	568	37.57
Rock Salomon	278	18.39
Total	**1512**	

Please select one of the following candidates for APFA National Vice President:	**Total**	**Percent**
Marcus Gluth	343	22.97
Nena Martin	806	53.99
Samuel Morales	344	23.04
Total	**1493**	

Please select one of the following candidates for APFA National Secretary:	**Total**	**Percent**
Nicole Darak	235	15.78

Marcy Dunaway	597	40.09
Jacob Fuller	336	22.57
Donald LeBlanc	83	5.57
Jaana Lehtola	238	15.98
Total	**1489**	

Please select one of the following candidates for APFA National Treasurer:	**Total**	**Percent**
Craig Gunter	348	23.32
Roee Rio Harrari	7	0.47
Stefany Jones	313	20.98
Nestor Quecuty	273	18.30
Eugenio Vargas	551	36.93
Total	**1492**	

ORD TOTAL

Please select one of the following candidates for APFA National President:	**Total**	**Percent**
Lori Bassani	69	7.09
Steven Baumert	58	5.96
Kimberly Goesling	10	1.03
Patrick Hancock	276	28.37
Andrea S. Jones	1	0.10
Brian Morgan	28	2.88
Bob Ross	428	43.99
Rock Salomon	103	10.59
Total	**973**	

Please select one of the following candidates for APFA National Vice President:	**Total**	**Percent**
Marcus Gluth	369	38.68
Nena Martin	415	43.50
Samuel Morales	170	17.82
Total	**954**	

Please select one of the following candidates for APFA National Secretary:	**Total**	**Percent**
Nicole Darak	273	28.50
Marcy Dunaway	338	35.28
Jacob Fuller	216	22.55
Donald LeBlanc	35	3.65
Jaana Lehtola	96	10.02
Total	**958**	

Please select one of the following candidates for APFA National Treasurer:	**Total**	**Percent**
Craig Gunter	380	39.83
Roee Rio Harrari	7	0.73
Stefany Jones	192	20.13
Nestor Quecuty	91	9.54
Eugenio Vargas	284	29.77
Total	**954**	

PHL TOTAL

Please select one of the following candidates for APFA National President:	**Total**	**Percent**
Lori Bassani	31	4.31
Steven Baumert	4	0.56
Kimberly Goesling	118	16.41
Patrick Hancock	84	11.68
Andrea S. Jones	1	0.14
Brian Morgan	365	50.76
Bob Ross	64	8.90
Rock Salomon	52	7.23
Total	**719**	

Please select one of the following candidates for APFA National Vice President:	**Total**	**Percent**
Marcus Gluth	313	47.21
Nena Martin	206	31.07
Samuel Morales	144	21.72
Total	**663**	

Please select one of the following candidates for APFA National Secretary:	**Total**	**Percent**
Nicole Darak	445	66.42
Marcy Dunaway	103	15.37
Jacob Fuller	38	5.67
Donald LeBlanc	34	5.07
Jaana Lehtola	50	7.46
Total	**670**	

Please select one of the following candidates for APFA National Treasurer:	**Total**	**Percent**
Craig Gunter	523	75.14
Roee Rio Harrari	49	7.04

Stefany Jones	66	9.48
Nestor Quecuty	35	5.03
Eugenio Vargas	23	3.30
Total	**696**	

PHX TOTAL

Please select one of the following candidates for APFA National President:	**Total**	**Percent**
Lori Bassani	24	5.44
Steven Baumert	7	1.59
Kimberly Goesling	91	20.63
Patrick Hancock	69	15.65
Andrea S. Jones	5	1.13
Brian Morgan	175	39.68
Bob Ross	32	7.26
Rock Salomon	38	8.62
Total	**441**	

Please select one of the following candidates for APFA National Vice President:	**Total**	**Percent**
Marcus Gluth	154	36.67
Nena Martin	160	38.10
Samuel Morales	106	25.24
Total	**420**	

Please select one of the following candidates for APFA National Secretary:	**Total**	**Percent**
Nicole Darak	244	57.68
Marcy Dunaway	53	12.53
Jacob Fuller	51	12.06
Donald LeBlanc	29	6.86
Jaana Lehtola	46	10.87
Total	**423**	

Please select one of the following candidates for APFA National Treasurer:	**Total**	**Percent**
Craig Gunter	274	64.32
Roee Rio Harrari	21	4.93
Stefany Jones	61	14.32
Nestor Quecuty	36	8.45
Eugenio Vargas	34	7.98
Total	**426**	

RDU TOTAL

Please select one of the following candidates for APFA National President:	**Total**	**Percent**
Lori Bassani	2	4.44
Steven Baumert	10	22.22
Kimberly Goesling	0	0.00
Patrick Hancock	7	15.56
Andrea S. Jones	0	0.00
Brian Morgan	0	0.00
Bob Ross	26	57.78
Rock Salomon	0	0.00
Total	**45**	

Please select one of the following candidates for APFA National Vice President:	**Total**	**Percent**
Marcus Gluth	12	27.27
Nena Martin	28	63.64
Samuel Morales	4	9.09
Total	**44**	

Please select one of the following candidates for APFA National Secretary:	**Total**	**Percent**
Nicole Darak	6	13.64
Marcy Dunaway	27	61.36
Jacob Fuller	8	18.18
Donald LeBlanc	2	4.55
Jaana Lehtola	1	2.27
Total	**44**	

Please select one of the following candidates for APFA National Treasurer:	**Total**	**Percent**
Craig Gunter	9	20.00
Roee Rio Harrari	0	0.00
Stefany Jones	23	51.11
Nestor Quecuty	1	2.22
Eugenio Vargas	12	26.67
Total	**45**	

SFO TOTAL

Please select one of the following candidates for APFA National President:	**Total**	**Percent**

Lori Bassani	20	9.39
Steven Baumert	7	3.29
Kimberly Goesling	3	1.41
Patrick Hancock	10	4.69
Andrea S. Jones	0	0.00
Brian Morgan	7	3.29
Bob Ross	160	75.12
Rock Salomon	6	2.82
Total	**213**	

Please select one of the following candidates for APFA National Vice President:	Total	Percent
Marcus Gluth	18	8.65
Nena Martin	174	83.65
Samuel Morales	16	7.69
Total	**208**	

Please select one of the following candidates for APFA National Secretary:	Total	Percent
Nicole Darak	11	5.45
Marcy Dunaway	131	64.85
Jacob Fuller	43	21.29
Donald LeBlanc	8	3.96
Jaana Lehtola	9	4.46
Total	**202**	

Please select one of the following candidates for APFA National Treasurer:	Total	Percent
Craig Gunter	29	14.08
Roee Rio Harrari	3	1.46
Stefany Jones	63	30.58
Nestor Quecuty	9	4.37
Eugenio Vargas	102	49.51
Total	**206**	

STL TOTAL

Please select one of the following candidates for APFA National President:	Total	Percent
Lori Bassani	3	2.05
Steven Baumert	71	48.63
Kimberly Goesling	16	10.96
Patrick Hancock	4	2.74
Andrea S. Jones	2	1.37
Brian Morgan	40	27.40
Bob Ross	6	4.11
Rock Salomon	4	2.74
Total	**146**	

Please select one of the following candidates for APFA National Vice President:	Total	Percent
Marcus Gluth	4	2.74
Nena Martin	140	95.89
Samuel Morales	2	1.37
Total	**146**	

Please select one of the following candidates for APFA National Secretary:	Total	Percent
Nicole Darak	2	1.37
Marcy Dunaway	6	4.11
Jacob Fuller	134	91.78
Donald LeBlanc	3	2.05
Jaana Lehtola	1	0.68
Total	**146**	

Please select one of the following candidates for APFA National Treasurer:	Total	Percent
Craig Gunter	8	5.52
Roee Rio Harrari	1	0.69
Stefany Jones	4	2.76
Nestor Quecuty	5	3.45
Eugenio Vargas	127	87.59
Total	**145**	

- There were 20656 eligible voters, of which 9355 cast a ballot, representing 45.3% of the eligible voters.
- Of the 9355 ballots cast, 5433 (58.1%) were by phone, and 3922 (41.9%) were by web.
- There were 0 ballots cast in which the voter did not make a selection.

These Official Results witnessed and certified by Nena Martin, Marcy Dunaway, Kimberly Goesling, Sam Morales, Michael Truan, Liz Geiss, Marie Plevritis, Lena Gale, Cindy Horan, Leatha Harding-Berry and Avis Rives.

Nena Martin
witness

signature / date

Marcy Dunaway
witness ______ signature / date

Kimberly Goesling
witness ______ signature / date

Sam Morales
witness ______ signature / date

Michael Truan
witness ______ signature / date

Liz Geiss
witness ______ signature / date

Marie Plevritis
witness ______ signature / date

Lena Gale
witness ______ signature / date

Cindy Horan
witness ______ signature / date

Leatha Harding-Berry
witness ______ signature / date

Avis Rives
witness ______ signature / date

Report generated: 01/09/2016 10:20:57 (Central)

Feldkamp Deposition
Exhibit 9

One-Vote, No-Voiding Election Method

The OVNV Process

The "one vote, no voiding" (OVNV) BallotPoint election method described below uses the two-server BallotPoint (BP) architecture (Election Server (ES) and MRNS), but in a very different way from the method used in elections prior to 2015. OVNV was developed by BallotPoint in response to a meeting at DOL in November 2014, wherein DOL representatives verbally asserted the categorical position that any electronic election which supports recasting votes and/or voiding ballots does not comply with the LMRDA. The OVNV method has been in production use by many BallotPoint clients since early 2015.

The central features of OVNV are:

- Voting by both telephone and Internet is supported.
- Members are not permitted to recast votes. Eligibility to vote for any given member must be determined prior to that member having the opportunity to cast a vote in that election.
- Cast ballots cannot be voided. Every vote that is cast is counted.
- Elections are authored and uploaded exactly as they were in past BallotPoint elections, starting from a Word document template provided by BallotPoint.
- Rosters are uploaded via the MRNS by the client's election administrator. A single line in a roster lists a member's ID, name, address, voting attributes (e.g., station or base), and voting eligibility status at the time the roster is submitted. After processing the roster, the MRNS passes, in effect, the number of eligible voters in each distinct combination of voting attributes. The sole purpose and use of this information in the ES is to generate election-participation and tally reports, with breakdown based on voting attributes ; specifically, this information is not used in any part of the actual voting process, including authorization of voters or storage of cast ballots.
- Each member is mailed *at each election* a unique (across all elections for that client), 12-random-digit BP *access code* in the Voting Notice document. An access code applies to only a single election; unlike in the traditional BP system, members are not provided "permanent" credentials that can be used across different elections.
- As in past elections, an Internet voter browses to the client-specific Election Server website. But instead of entering an activation code or VIN+PIN, the voter clicks on a *Click to Log In* button. This transfers the user to the MRNS, which prompts for the (election-specific) access code. The MRNS verifies that the access code is valid and has not been used to cast a vote. If successful, the voter is automatically transferred back to the ES and a ballot appropriate to his or her voting attributes is presented. No member-specific information is sent to the ES.
- As in past elections, a telephone voter calls the client-specific ES phone system. In the OVNV method, the voter is then immediately transferred to the MRNS phone system; the ES phone system remains connected to the call, but cannot hear the keypad tones entered by the voter into the MRNS phone system. Once connected, the MRNS phone system prompts the member to enter an access code. The MRNS checks the access code and, if the member is eligible to vote

in an election, sends the member's voting attributes to the ES. No information that could be used to uniquely identify the member is sent to the ES. The MRNS phone system then hangs up, which automatically returns the caller to the ES phone system. Finally, the ES phone system presents the appropriate ballot (according to the voting attributes) to the member.

- When the member casts a ballot, the ES and the MRNS go through a chain of mathematical operations that results in a twice-encrypted vote being stored on the ES, and a unique, indecipherable representation of the encrypted vote being stored on the MRNS. We call the latter quantity a *vote digest*. NOTE: It is a BallotPoint client's option whether to include the confirmation number with the vote-data during the double-encryption process. APFA opted to not include it.
- A unique confirmation number is spoken or displayed after the twice-encrypted vote is successfully stored on the ES and the vote digest is successfully stored on the MRNS.
- Because votes are not stored with any information (e.g., VINs or activation codes, which were used in the traditional BP system) that could be used to isolate votes after the election, ballots cannot be voided in the OVNV method.
- Candidates' observers who have been authorized by the election committee to have login access to the MRNS may download at any time the latest set of vote digests for the election, regardless of where around the globe the observers may be located. This is an unprecedented capability for observers to verify that votes have not been dropped or altered (whether by software or storage errors or through malicious action) during the course of the election. The details of how this is accomplished are necessarily mathematical and will not be covered here. (Please refer to the files, *VoteDigestProcess-from-MRNS.pdf* and *OVD-OVNV-20160330-091139-97065879.txt*.)
- At tally time, *every* vote counted by the ES must correspond to a vote digest stored on the MRNS. The association of each now-decrypted vote will be shown—available as an Excel spreadsheet—to correspond to exactly one vote digest that was stored on the MRNS during the election. Each row of the spreadsheet corresponds to a cast ballot. If the BallotPoint client has opted to include confirmation numbers in the twice-encrypted vote-data, then each voter can locate his confirmation number and verify that the system recorded and counted the ballot as intended. As noted above, APFA chose to *not* include confirmation numbers.
- At tally time, a *Who-Voted Report* can be obtained by the election administrator when logged in to the MRNS. This report is compiled from the members who logged in through the MRNS.

Secrecy

The BallotPoint OVNV method addresses the secrecy requirement of the LMRDA by never providing member-specific information to the Election Server and by not tagging cast ballots with any member-specific information. When a vote is cast, it's effectively the same as dropping a paper ballot into a ballot box at an election conducted on-site: Once cast, it is indistinguishable from any other ballot.

The downside of this is that any challenges to eligibility must take place before a member appears in the voting roster as eligible to vote. For members who are not currently eligible but who may become eligible during the period of the election, they should initially be marked as ineligible in the roster; when a member subsequently becomes eligible, a new roster showing the now-eligible status can be submitted to the MRNS.

Observability

The OVNV system addresses the observability requirement of the LMRDA by providing access by candidates' observers to the vote digests being accumulated on the MRNS. These vote digests can be shown mathematically to correspond exactly to twice-encrypted votes stored on the ES. As described in *The OVNV Process*, above, candidates' observers can download all vote digests generated to date for the election in question. These can be compared to the vote digests shown in the spreadsheet produced at tally time to verify that votes were not lost or replaced during the election. Assuming the vote digests collected by observers match those shown in the spreadsheet (and this will be the case if observers don't alter the vote digests they collect), the decrypted votes shown in the spreadsheet can safely and reliably be used as the basis for an independent recount if necessary.

For individual members the Excel spreadsheet produced at tally time may list (per the BallotPoint client's option) the confirmation number and the corresponding unencrypted vote for every vote cast in the election. By retaining the confirmation number issued by the BallotPoint system when a ballot is cast, every voter can verify that his vote was recorded accurately.

Paper Trail

The Excel spreadsheet produced at tally time replaces any paper trail you might find referenced in the literature on electronic elections. It is a provably accurate basis for a manual recount.

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
FORT WORTH DIVISION

THOMAS E. PEREZ [now R. ALEXANDER ACOSTA], Secretary of Labor,

Plaintiff,

v.

Civil Action No. 4:16-cv-1057-A

ASSOCIATION OF PROFESSIONAL FLIGHT ATTENDANTS,

Defendant.

DECLARATION OF CURT STAPLETON IN SUPPORT OF APFA'S MOTION FOR SUMMARY JUDGMENT

I, Curt Stapleton, hereby declare as follows:

1. I am over the age of eighteen and am competent to testify as to all of the facts contained in this Declaration, of which I have first-hand, personal knowledge.

2. I have been retained by counsel for the Association of Professional Flight Attendants ("APFA") to render an opinion on certain aspects of BallotPoint Election Services' electronic voting system, which was used by APFA in the administration of APFA's 2016 National Officer Election.

3. My qualifications and work experience have been previously detailed in a written expert report that I prepared and signed on June 30, 2017. A true and correct copy of that report is attached to this Declaration as Exhibit A.

4. I hereby adopt the facts and opinions contained in Exhibit A, the content of which is incorporated herein by reference, as my testimony.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Executed in Frederick, MD this 17 day of August, 2017.

Curt Stapleton

Curt Stapleton

Stapleton Declaration
Exhibit A

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
FORT WORTH DIVISION

R. ALEXANDER ACOSTA, Secretary of Labor,

Plaintiff,

v.

Civil Action No. 4:16-cv-1057-A

ASSOCIATION OF PROFESSIONAL FLIGHT ATTENDANTS,

Defendant.

EXPERT REPORT OF CURT STAPLETON, CEO
ADEPT SECURITY CONSULTING

I. INTRODUCTION

A. Retention and Scope.

I have been retained by Bredhoff & Kaiser, P.L.L.C. to serve as an expert witness in the above-captioned case. My findings and opinions are set forth in this "Report."

B. Qualifications.

I am the founder and CEO of Adept Security Consulting, LLC ("AdeptSec"), a consultancy I founded in 2015 to provide network application penetration testing, systems security training, and security consulting.

Before founding AdeptSec, I served approximately eight years as a technical director for Aerstone, a cybersecurity consultancy providing security assessment and systems enhancement and sustainment. At Aerstone, I served as the service-area lead for penetration testing and security assessments, and I conducted security assessments for numerous clients including federal and state government agencies, financial institutions, and commercial companies.

Before joining Aerstone, I worked for almost 12 years at SAIC. There, I held positions ranging from security and software engineer to program manager to assistant vice president. I led a team of penetration testers who conducted security assessments of numerous federal agencies, including the Department of the Treasury and Department of Defense.

I have a Bachelor of Science in Computer Science from Mississippi State University and a Global Information Assurance Certification (GIAC) in Incident Handling, for which I authored a practical, *Employees are Crackers Too: Advanced Incident Handling and Hacker Exploits*.[1] In total, I have over 23 years of experience in the computer industry, including over twenty years of experience in system security engineering and risk assessments. As a result of my training and experience in the systems security field, I have extensive knowledge of, and practical expertise in, assessing information technology systems for their vulnerability to external and internal threats, and in designing systems to withstand attempts by attackers to gain unauthorized access or otherwise tamper with the data stored on that system.

I have not previously testified as an expert witness at trial or by deposition.

C. Fees.

AdeptSec is compensated for my time at the hourly rate of $250 per hour. In addition, AdeptSec was paid a flat fee of $11,500 plus expenses for making a site visit to the BallotPoint facility in Portland, Oregon, and preparing a preliminary analysis based on my visit. My compensation is not contingent in any way on the outcome of this case.

[1] Curt Stapleton, Employees are Crackers Too: Advanced Incident Handling and Hacker Exploits, SANS Institute (Oct. 7, 2001), *available at* https://pen-testing.sans.org/resources/papers/gcih/employees-crackers-102345.

D. Documents and Other Materials Considered.

- Complaint
- Materials reviewed in conjunction with site visit to BallotPoint
  - Application code modules containing references to “oem_access_” and “ipaddr” in use during the 2016 APFA NO election
  - MRNS baseline code (that is, MRNS application code at beginning of the 2016 APFA National Officer Election)
  - MRNS application code change logs for January 2016 and February 2016
  - Two application code changes made to MRNS application code during the course of the 2016 National Officer Election
  - MRNS application code currently used by BallotPoint in LMRDA-compliant elections
  - ES application code that performs the counting of the ballots
  - ES application code that generates a web page to display the results
  - ES application code that generates the CSV file containing the results
  - Text files of MRNS and ES application code change logs
  - Voter Participation Report from the 2016 APFA National Officer Election
  - Downloaded Vote Digests from the 2016 APFA National Officer Election
  - “TallyRecords-to-Consultants-TabDelimited.txt” - a spreadsheet containing DEV, downloaded vote digests, vote key, SEV, vote salt, and ballot selections for the January 2016 APFA NO election
  - “check-tally-records-eid15.cfm” code module (containing election key)
  - Printed copy of Post-Election Vote Digest
  - Printed copy of "ESTSAPFAEID15OEMRetrieval.cfm" code module (containing modification made in response to DOL subpoena)
- Interviews of the following BallotPoint personnel were conducted during the site visit:
  - Gerry Feldkamp
- I received additional oral information from the following BallotPoint personnel
  - Dan Hilderbrand
  - Mike Baum
  - Bob Thompson
- Election Official Interview Questionnaire of Cindy Horan, Chair of the APFA National Ballot Committee
- Plaintiff’s Answers to Defendant’s First Set of Interrogatories
- Defendant APFA’s Rule 26(a)(2)(C) Disclosure of Gerry Feldkamp
- Authoritative Literature (a complete list of the authoritative literature consulted in the drafting of this report is attached to the report as Exhibit C)

II. BACKGROUND

A. Security Assessments of Information Technology Systems

A security assessment of an information technology system is conducted to determine the risk of harm that may be done to owners and users of a system by threats to the system. For information-technology systems, common harms include: exposure of sensitive information to unauthorized parties, manipulation or degradation of information stored on the system, and unavailability to authorized parties of information stored on the system. The risk to the system, in turn, is a function of the degree and likelihood of harm—the greater the likelihood that a harm will occur, and the more severe the harm that will result if the threat is realized, the greater the risk to owners and users of the system.[2] Security assessors analyze the steps an organization has taken to identify threats, identify vulnerabilities, identify the adverse impact and likelihood of a vulnerability being exploited, and the steps taken to mitigate those threats and vulnerabilities. Based on this information, a security assessor ultimately makes a risk determination for the system.[3]

Threats to a system come in a variety of forms. Threat sources include natural disasters, technical failures, unintentional human errors, or intentional attacks by hostile actors.[4] Every system has a unique threat profile that is developed based on the purpose, architecture, and exposure (sometimes referred to as the attack surface) of the system. Understanding the credible

[2] U.S. Dep't of Commerce, National Institute of Standards and Technology ("NIST"), Special Publication 800-30, *Guide for Conducting Risk Assessments* (September 2012), at 12.

[3] *See* U.S. Dep't of Commerce, National Institute of Standards and Technology, Special Publication 800-30, *Guide for Conducting Risk Assessments* (September 2012), at Appendix I (template risk determinations).

[4] NIST's *Security Considerations for Remote Electronic UOCAVA Voting* explains that remote electronic voting systems face threats from internal sources including voters, election officials, and system administrators and external sources including hostile individuals or organizations not necessary to the election itself. U.S. Dep't of Commerce, National Institute of Standards and Technology Interagency Report 7770, *Security Considerations for Remote Electronic UOCAVA Voting* (Feb. 2011) (hereafter, "NIST IR 7770, *Security Considerations for Remote Electronic UOCAVA Voting*"), at 8-11.

threats and the sources behind those threats guides the security assessment of a system because the threats inform which system components, data, or processes may be vulnerable to attackers or susceptible to interference from unintentional human error.

For an information system to function optimally, its designers will consider and implement safeguards from threats that could affect the way in which the system is intended to operate, and threats to the information that is collected, processed, and stored by the system. Security assessors review threats to three core concepts of information protection: confidentiality, integrity, and availability.[5] In the information security industry, these concepts are understood as follows:

- Confidentiality refers to the possibility that information contained within the system will be disclosed to unauthorized persons or entities. In secret-ballot elections conducted via an electronic voting system, the core confidentiality concerns are (i) avoiding disclosure of confidential, personal voter information to unauthorized persons, and (ii) ensuring that the content of an individual voter's vote cannot be matched with the identity of the voter, that is "ballot secrecy."[6]

- Integrity refers to the maintenance by the system of complete and accurate information over its lifetime. In an electronic voting system, the core integrity concerns are ensuring that a vote was cast-as-intended, and ensuring that it was counted-as-cast.[7]

- Availability refers to the system's ability to collect and produce the information when it is needed and for as long as it is needed. In an electronic voting system, the core availability concerns include reducing the difficulty of casting a ballot in the first place—including the accessibility of the system to voters—and ensuring that the cast-ballot information is available to be counted at the moment of the tally.[8]

The degree to which each of these concepts is important varies based on the purpose of the system and the types of information processed. An information security assessment utilizes threat information, an understanding of the system, and its data protection requirements to

[5] U.S. Dep't of Commerce, National Institute of Standards and Technology, Special Publication 800-30, *Guide for Conducting Risk Assessments* (September 2012), at 6.

[6] NIST IR 7770, *Security Considerations for Remote Electronic UOCAVA Voting*, at 14.

[7] NIST IR 7770, *Security Considerations for Remote Electronic UOCAVA Voting*, at 23-24.

[8] NIST IR 7770, *Security Considerations for Remote Electronic UOCAVA Voting*, at 38-40.

determine if there are sufficient controls in place to protect the system and its users from harm. Depending on the purpose of the system, its exposure to threats, and the harm that will occur if one of the three core information protection concepts is compromised, a greater or lesser degree of control over the system's information might be appropriate.[9] Because each additional control implemented entails a cost (in terms of the cost in dollars, the complexity entailed in designing and maintaining the system, and in potentially reducing the system's functionality or robustness), the appropriate level of control is oftentimes not the *most* controlled system, but one maintaining reasonable controls given the purpose of the system and its individual risk profile.

In particular, introducing additional controls to protect one aspect of information security might increase the risk that another aspect of information security will be compromised. For example, in electronic voting systems, additional integrity controls (such as providing voters with additional confirmation numbers throughout the voting process) to ensure ballots are cast-as-intended and counted-as-cast can oftentimes increase the opportunity for breaches of ballot secrecy, and could compromise the confidentiality of voters' choices. It is part of my role as a security assessor to understand and consider such trade-offs made by systems architects to achieve an appropriate level of security for their information technology systems.

B. The BallotPoint-Administered 2016 APFA National Officer Election

My understanding of the following background facts is derived from my review of the Complaint and other documents provided to me by Bredhoff & Kaiser, including the expert disclosure of Gerry Feldkamp, and from information discovered during a site visit to the BallotPoint facilities conducted from May 15, through May 19, 2017.

[9] NIST's *Security Considerations for Remote Electronic UOCAVA Voting* recognizes that the extent a security property can be met must be measured against "the cost and usability of implementing that property." NIST IR 7770, *Security Considerations for Remote Electronic UOCAVA Voting*, at 13.

The Association of Professional Flight Attendants ("APFA") conducted an election of officers ending January 9, 2016, for the positions of National President, National Vice President, National Treasurer, and National Secretary ("the January 2016 National Officer Election"). APFA's election was conducted over a thirty-day period beginning on December 10, 2015. There were over twenty thousand eligible voters. APFA members are geographically dispersed across the United States, and they are absent from their homes (and, sometimes, the United States) for periods throughout the 30-day election period depending on their flying schedules.

The APFA engaged the services of a contractor, BallotPoint Election Services, owned by CCComplete, to administer the January 2016 National Officer Election using an Internet-based and phone-based remote electronic voting system. Pursuant to its contract with APFA, BallotPoint administered the election from December 10, 2015 through January 9, 2016. At the beginning of the election, Allied Media, another third-party contractor of APFA, mailed eligible APFA members a voting credential consisting of a unique access code each voter could use to access the voting system. With that individualized credential, each voter could access a ballot on BallotPoint's website via a computer or smart-phone web browser, or could access a ballot over the phone by dialing a toll-free number. Once voters successfully voted, BallotPoint maintained their votes on one computer server, the Election Server ("ES"), and maintained member identifying information on another server, the Member Registration and Notification Server ("MRNS"). Both servers were owned by BallotPoint but physically located in a secure co-location facility in Portland, Oregon operated by Lightpoint, an independent company. Once a voter successfully cast a ballot, the BallotPoint system presented the voter with a confirmation code and emailed the voter a message informing the voter that his or her vote had been cast successfully, or, alternatively, read out a confirmation code over the phone if the voter had cast his or her ballot via phone. A chart summarizing the interactions between voters and the BallotPoint voting system is attached to this report as Exhibit A.

On January 9, 2016, at the end of the election, the BallotPoint system electronically tallied the cast ballots and transmitted the results to the APFA Union Hall.

C. My Security Assessment of the BallotPoint System

I performed a qualitative security assessment of the BallotPoint election system based on a predefined scope and over the period of two (2) weeks. In particular, I assessed the confidentiality and integrity of voter selections made using the electronic voting system; the development, operations, and maintenance of the voting system; and the integrity of the application and its source code. I conducted my assessment against the background of the assessment methods published by the National Institute of Standards and Technology ("NIST"), in NIST Special Publication ("SP") 800-30, *Guide for Conducting Risk Assessments*, and NIST SP 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*. These standards are used by the federal government to secure information systems and they provide detailed guidance for systems and data of all risk levels. In addition to this general NIST guidance on risk assessments, my assessment of the BallotPoint electronic voting system was conducted against the background of NIST IR 7770, *Security Considerations for Remote Electronic UOCAVA Voting*.

My specific assessment approach was tailored based on previously reported system security concerns, professional experience as an auditor of government and non-government computing systems, and professional experience conducting numerous penetration tests of government and non-government systems.

Following federal information system assessment methods, and drawing on professional experience, I gathered information and performed analysis of various aspects of the system to answer the following questions:

1. Do I understand what the system is supposed to do, how it is put together, how it is maintained, and how it works?
2. Do I understand the technical details surrounding the voter confidentiality issue raised following the January 2016 APFA election?
3. Do I understand the changes that have been made because of the issue raised following the January 2016 APFA election?
4. Do I understand the protections built into the system to protect the integrity of voters' choices of candidates?

I analyzed each step of the electronic voting process, and where there were conditions that warranted security controls to protect the confidentiality and integrity of election information, I analyzed the types of protections in place, and how closely those controls adhered to accepted guidelines. The scope of my analysis did not include investigation of the system's controls related to availability of the information because I understood that neither party in the litigation had raised concerns about the availability of vote information.[10]

III. PRINCIPAL OPINIONS

Based on the work that I have performed, my site visit to BallotPoint, my review of portions of the BallotPoint source code, and my review of the documents provided to me by Bredhoff & Kaiser, along with my professional skill, experience, and training, I have concluded that, given its individual risk profile, the BallotPoint remote electronic voting system, as it

[10] Although I did not extensively assess availability concerns raised by the 2016 APFA National Officer Election, I note that remote electronic voting offers significant accessibility benefits to a highly mobile population like the flight attendants represented by APFA. In its review of security considerations related to UOCAVA voting, NIST specifically noted the availability benefits remote electronic voting offered to another highly mobile population, overseas military voters. NIST IR 7770, *Security Considerations for Remote Electronic UOCAVA Voting*, at 38-40.

existed at the time of the 2016 APFA National Officer Election, provided an appropriate level of control over the information stored on the system. In particular, as explained in more detail below, I have concluded that (A) the system appropriately protected confidentiality because the system, as designed, did not allow the identities of voters to be matched to the content of their votes by matching IP addresses associated with votes to IP addresses associated with member identifying information, or through the transmission of confirmation emails. In addition, I have determined that (B) the system appropriately protected the integrity of voting information because the system had controls in place at each step of the voting process to ensure that votes were cast-as-intended and counted-as-cast.

A. The BallotPoint Electronic Voting System did not permit voters' identities to be linked with their votes.

As it existed at the time of the 2016 APFA National Officer Election, the BallotPoint remote electronic voting system did not permit voters' identities to be linked to the content of their votes. Based on the documents I reviewed in preparation for rendering this opinion, I understand that the Department of Labor ("DOL") was ultimately able to match voters' identities with approximately 4,082 cast ballots (out of a total of 9,355 first-round ballots) by using IP address and timestamp information stored on BallotPoint's servers. Specifically, after the BallotPoint system was altered in response to a DOL subpoena, DOL was able to match certain IP address data stored on the ES and associated with individual votes to IP address data stored on the MRNS and associated with voter identities. Below, I explain why the system as it existed during the 2016 APFA National Officer Election did not permit the matching of votes with voters in this manner and maintained controls to protect against unauthorized alterations such as those eventually performed at DOL's demand.

The hardware setup of the BallotPoint system consists of two servers: the MRNS stores member identifying information (but does not store voters' votes), and the ES stores cast ballots (but does not store individual identifying information). BallotPoint does not have unfettered physical access to these servers; they are hosted by a third-party co-location facility, Lightpoint, which maintains its own security protocols over physical access to BallotPoint's servers. Communication between the two servers is conducted only via the internet, and there is no direct communication link between the two servers. In addition to this hardware architecture, the BallotPoint system consists of the software applications for both servers. The software portion of the system is an integral part of the overall system because the software dictates what information each server collects and stores, what the server can do with that information, and what access users of the system (to include BallotPoint administrators, APFA election officials, and voters) have to information stored on the servers.

In order to determine what information was stored by the two servers, and what information was accessible to users of the BallotPoint system as of the 2016 APFA National Officer Election, I reviewed the application code running on both servers. I conducted this review by searching the application code for "oem_access_" to catch all references to either "oem_access_from" or "oem_access_when," and searched for "addr," to catch all references to "ipaddr." These were the BallotPoint data fields that were used to store IP address and timestamp information. Based on this review, I was able to determine that both servers stored IP address information throughout the 2016 APFA National Officer elections; the ES associated stored IP addresses with cast ballots, while the MRNS stored IP addresses with member information, including member names. In addition, both servers stored timestamp information;

the MRNS timestamped users' votes in 8-hour windows, while the ES provided timestamps of cast ballots to the second.

My review of the application source code also determined that the system did not provide a mechanism by which users (including BallotPoint administrators, APFA election officials, and voters) could access the IP address information stored on the MRNS. By way of explanation, an information system can collect and store data, but, without a software mechanism for accessing that data, or physical access to the server combined with a software tool to compile the data stored on that server, the data will remain internal to the system, and users will not be able to access that information. There are ways in which stored data can be made accessible to a user of the system without physical access to the server, including display via a web page or inclusion of that data in a report that the software is designed to generate. By searching for references to the "oem_access_from" and "oem_access_when" data fields and the "addr" variable in the MRNS application source code, I was able to determine that the software, as it existed at the time of the 2016 APFA National Officer Election, did not include such a mechanism. Therefore, although this data was being collected by the system, it would not have been accessible to BallotPoint engineers or to any other authorized users of the system.

Of course, software can be changed. Given that this information existed on the system, it was possible for BallotPoint engineers to change the software to make this data accessible to one or more categories of users. For example, BallotPoint could write software to generate a report that would list the IP address information stored in the "oem_access_from" field next to the other voter identifying information stored on the MRNS, including voter name. Because of this possibility that a BallotPoint engineer could change the software to make this data accessible, my assessment is that the system's greatest vulnerability to the "confidentiality" information-protection concept was the internal threat posed by BallotPoint systems administrators.[11]

It is my opinion, however, that voter confidentiality was adequately protected during the 2016 APFA National Officer Election because of a series of controls and limits included on the system to limit BallotPoint's own ability to alter the application software. Specifically, BallotPoint has designed the MRNS so that BallotPoint itself cannot make changes to the application software running on the MRNS; rather, all changes to the application software can only be made by the third-party server host, Lightpoint. In order to effect a software change on the MRNS, BallotPoint sends an encrypted CD to Lightpoint, which then installs the software update via its terminal without physically accessing the BallotPoint server. Lightpoint maintains a log of all such changes, and BallotPoint maintains an identical log at its offices.[12]

As part of my site visit, I reviewed the BallotPoint logs of changes made to the MRNS application software during the 2016 APFA National Officer Election, as well as the application code of each change. There were two such changes made during the election. Based on that review, I was able to determine that neither software update made any reference to the data stored in the "oem_access_from" or "oem_access_when" fields, *i.e.*, the IP address and timestamp data that was ultimately used by the DOL to match voter identifying information with cast ballots. Therefore, I conclude that the information stored in these fields was not available to

[11] NIST's *Security Considerations for Remote Electronic UOCAVA Voting*, describes generally the threats posed by systems administrators in all remote electronic voting systems. NIST IR 7770, *Security Considerations for Remote Electronic UOCAVA Voting*, § 2.3.1, at 10-11. In the BallotPoint system, there is very low risk that other authorized users (voters and election officials) could make the requisite software change because those users do not have the necessary level of system access to make a change to the application software.

[12] This separation of duties ensures that two independent contractors must collude in order to make undetected changes to the MRNS application code, and is a recommended control for ensuring ballot secrecy. NIST IR 7770, *Security Considerations for Remote Electronic UOCAVA Voting*, § 4.4.4, at 21.

BallotPoint system administrators (or other system users) through the end of the 2016 APFA National Officer Election.

Based on my experience conducting risk assessments for information systems, I consider the controls BallotPoint has put in place to protect against an unauthorized software change by a system administrator adequate to protect against the threat to voter confidentiality posed by such a change. Although BallotPoint has the ability to make software changes that would cause the system to collect identifying information or to make that data accessible to system administrators or other users, the making of such changes would ultimately leave a forensic trail (at least on the Lightpoint versions of the change logs), which would disclose in a subsequent investigation (be it by DOL or a user organization) that such identifying information had been collected/made accessible.[13] Moreover, because of the existence of this trail, I am able to state confidently that no software changes were made to the MRNS that would have made this data accessible during the election.

Therefore, it is my opinion that, in connection with the 2016 APFA National Officer Election, the BallotPoint electronic voting system included reasonable controls of the kind that would be expected to protect ballot secrecy in a remote-electronic voting system from the possibility that votes could be linked to voters via IP address information associated with both the content of votes and voter identifying information.

*   *   *

[13] Such logging of software changes provides an effective means to deter and detect attacks on an information-technology system. U.S. Dep't of Commerce, National Institute of Standards and Technology, Special Publication 800-123, *Guide to General Server Security*, (July 2008), at 6-1 ("Logging is a cornerstone of a sound security posture. . . . [L]og files are often the only record of suspicious behavior. Enabling the mechanisms to log information allows the logs to be used to detect failed and successful intrusion attempts and to initiate alert mechanisms when further investigation is needed.")

I note separately that the ability of the BallotPoint system to send voters confirmation emails or to provide them with confirmation that their votes have been successfully cast in no way demonstrates that the system as designed enabled voters' identities to be associated with the content of their votes. The system provides voter confirmations as follows.

Once a voter checks into the voting system (via the MRNS) with his or her unique voting credential, the MRNS indicates to the ES the voter profile of the voter who just checked in (ensuring that the voter is presented with the appropriate ballot; in the 2016 APFA National Officer Election, voter profiles corresponded to each member's domicile). But although the voter profile is communicated to the ES, by design, no individual voter identifying information is shared other than a randomly generated one-time password that is identified with that voting session. After the voter successfully casts a vote and it is recorded to the ES, the ES informs the MRNS that the voting session associated with that one-time password has been successfully completed, but it does not send the content of the vote to the MRNS. In the member table, the MRNS marks the member identity associated with that one-time password as having voted, and then permanently deletes the one-time password. The MRNS then informs the voter that he or she has voted successfully, a function it can perform without ever possessing the information necessary to associate the content of a vote with that voter's identity.

Thus, the MRNS sends confirmation emails based only on the *fact* that a vote was successfully cast, and completely independent of the *content* of that vote. The ability of the system to send confirmation emails is not evidence that the system was designed to enable voters' identities to be matched with the content of their votes.

B. There is no reasonable possibility that the tally of ballots communicated by BallotPoint to APFA at the end of the election incorrectly reflected the winners of the election selected by the voters.

Based on my review of the overall system architecture, and the controls BallotPoint instituted at each step of the voting and tallying process, in connection with the 2016 APFA National Officer Election, it is my opinion that there is no reasonable possibility that the BallotPoint system failed to perform as intended to ensure that voters' votes were cast-as-intended and counted-as-cast. In particular, controls at each step of the process exist to ensure that vote integrity is maintained when the voter's vote is (1) cast and transmitted from the user's machine to BallotPoint; (2) recorded on the ES; (3) maintained on the ES during the remainder of the election period; and (4) correctly tallied at the end of the election. Although no information system can be considered 100% secure, the protections in place in the BallotPoint system used in the 2016 APFA National Officer Election include many controls recommended by NIST for systems of this type and purpose, and together ensure that there is no reasonable possibility that the reported results of the election failed to reflect voters' intentions.

I have included a flowchart, attached as Exhibit A to this report, that illustrates the voter-system interactions in the BallotPoint voting process. I have also included a flowchart, attached as Exhibit B to this report, that illustrates the server-to-server interactions, including the encryption and hashing of data performed by each server. What follows is a review of the adequacy of the controls BallotPoint introduced at each step of the voting process to ensure vote integrity.

1. Casting of votes.

In the first step of the voting process, a voter casts his or her ballot using a web application (on a computer or smartphone) or over the telephone. For computer-based votes, the primary threat at this stage is the risk that malicious software on client systems could interfere with the casting of a vote, preventing the vote from being cast-as-intended. The threat of malicious software on a user's machine (as opposed to the servers maintained by the election systems administrator) is often referred to as a client-side threat.[14] A personal computer or smartphone infected with malicious software targeting the election could potentially steal the victim's authentication credentials or could, in theory, change a user's vote without the victim noticing.[15]

Ensuring the security of personally owned computers is one of the most difficult aspects of securing any information system in which users are permitted to access the system from their personal machines.[16] To mitigate this threat, BallotPoint has implemented a recommended control, the use of a secondary communication channel.[17] Specifically, in BallotPoint-administered elections, voter credentials are distributed through the postal mail, instead of through an electronic communication channel. Use of the postal mail ensures that an infected computer cannot intercept the voting credential and use it to cast a ballot without the voter ever becoming aware that he or she had been sent a credential. However, the voter must still enter his or her credential before casting a ballot, introducing the credential to the potentially infected system and the possibility of manipulation by malicious software.

However, despite the conceptual vulnerability represented by client-side infection of the user's machine, in my opinion, the risk that such infection could have affected the outcome of the 2016 APFA National Officer Election is very low. Each successful attack on a voter's computer can impact only one or an extremely small number of voters.[18] Moreover, a piece of

[14] NIST IR 7770, *Security Considerations for Remote Electronic UOCAVA Voting*, § 5.3.4, at 29.

[15] NIST IR 7770, *Security Considerations for Remote Electronic UOCAVA Voting*, § 5.3.4, at 29.

[16] NIST IR 7770, *Security Considerations for Remote Electronic UOCAVA Voting*, § 5.5, at 37.

[17] NIST IR 7770, *Security Considerations for Remote Electronic UOCAVA Voting*, § 5.4.9, at 35.

[18] NIST IR 7770, *Security Considerations for Remote Electronic UOCAVA Voting*, § 5.3 at 30.

malicious software capable of manipulating the BallotPoint voting process would need to be sophisticated and would require in-depth knowledge of BallotPoint's processes. Security assessors consider the notoriety of the purpose to which a system is being put when assessing the risk presented by a particular vulnerability, including client-side vulnerabilities; in general, the more well-known the purpose to which an information technology system is put, the greater the likelihood (and therefore the risk) that an attacker will invest the time and resources required to affect a sufficient number of client-side systems.[19] Given the relatively low notoriety of the APFA 2016 National Officer Election (as compared to say, a national or statewide political election),[20] and in the absence of any evidence (in the form of suspicious voting patterns or irregular voter activity) of client-side malicious interference with votes, in my opinion, there is not a significant possibility that a sufficient number of voters' machines could have been infected with malicious software capable of altering the content of a vote (such that the vote was not cast-as-intended) to have affected the outcome of the National President general election, the election with the smallest margin of victory (582 votes).[21]

2. Transmission and recording of a vote on the BallotPoint server.

Once a voter selects his or her voting choice, BallotPoint has instituted strong controls to ensure, with a high degree of likelihood, that the vote will be successfully transmitted to BallotPoint without interception or manipulation. The primary control BallotPoint uses to ensure

[19] For example, in Ben Adida et. al, *Electing a University President using Open-Audit Voting: Analysis of real world use of Helios*, June 25, 2009, at 2, because of client-side risks, the authors declined to endorse the use of a remote-electronic voting system in "large, high-stakes, governmental elections where the threat of a targeted virus would be far more realistic."

[20] For comparison's sake, NIST's assessment of the use of remote electronic voting systems for overseas military voters suggested that it would be difficult for attackers to "successfully target the relatively small percentage of individuals in the world that are eligible to vote as overseas or military voters." NIST IR 7770, *Security Considerations for Remote Electronic UOCAVA Voting*, § 5.5, at 37. The individuals voting in the 2016 APFA National Officer Election are likewise a relatively small percentage of the computer-using public.

[21] The 582-vote margin of victory describes the margin between the second- and third-place finishers, because, in this first-round election, the top two finishers advanced to the final round of voting.

successful transmission is encryption via secure-socket-layer (SSL) protocol, a commonly used form of cryptographic protection for both data integrity and confidentiality.[22] In a transaction conducted according to the SSL protocol, the server hosting the web application (here, BallotPoint's server) and the user's web browser must agree on an encryption algorithm and an encryption key before any information is sent from the user's machine to the web server. Once that agreement is reached, the information is encrypted and can only be decrypted by a party possessing both the algorithm and the key. Thus, even if someone successfully intercepted transmission of the data, he or she would not be able to manipulate it (or even view it) unless he or she possessed both the algorithm and key.[23] SSL encryption, which is widely used for a variety of everyday commercial and financial transactions, is very effective at protecting data in transit.[24] Accordingly, once a voter successfully selects candidates and authorizes the system to submit his or her ballot (that is, once he or she casts his or her ballot), there is a very high likelihood that it will arrive at BallotPoint's servers without interference, effectively ensuring that the vote will be transmitted-as-cast.

Once it arrives at the BallotPoint servers, the vote must be recorded. At this stage, the most significant threat is an insider attack by a BallotPoint system administrator, potentially taking the form of intentional installation of malicious code that can change election data.[25] Despite the possibility that a BallotPoint system engineer could, theoretically, alter the application code to manipulate the content of a vote at the moment it arrives at the BallotPoint server, before the vote is encrypted or hashed (see Section III.B.3, below), there is no evidence to

[22] NIST IR 7770, *Security Considerations for Remote Electronic UOCAVA Voting*, § 4.4.1, at 19-20.

[23] TechRadar.com, *How SSL and TLS works*, (Jan. 2, 2012), *available at* http://www.techradar.com/news/software/how-ssl-and-tls-works-1047412.

[24] NIST IR 7770, *Security Considerations for Remote Electronic UOCAVA Voting*, § 5.4.1, at 31.

[25] Such insider "attacks have the potential to change a large number of votes and can be difficult to detect." NIST IR 7770, *Security Considerations for Remote Electronic UOCAVA Voting*, § 5.3.2, at 28.

suggest that such intentional manipulation occurred in the 2016 APFA National Officer Election. In conducting risk assessments, it is appropriate to consider both the motivations of users who constitute a threat to one of the information-protection concepts, and the opportunity such a user has to do harm. In the BallotPoint electronic voting system, there is little to no motivation for BallotPoint system administrators to manipulate the outcome of an election in this way. Indeed, because the value of the BallotPoint product is tied almost entirely to its perception as an impartial electoral tool, even an unfounded allegation of such manipulation could undermine BallotPoint's entire business model. Moreover, the opportunity of any BallotPoint system administrator to make such a change without alerting one of the other two system administrators is very limited due to the closed nature of the application and the level of familiarity all three system administrators have with the entire code.

In sum, BallotPoint has put in place controls to ensure the integrity of the vote will be maintained during transmission to its servers, and, based on my experience conducting risk assessments of information systems, I can state with a high degree of confidence that the BallotPoint system is designed to record accurately votes once they arrive at the BallotPoint server.

3. Maintenance of a vote on the BallotPoint server.

Once a vote has been successfully recorded to the ES, additional sophisticated controls exist to ensure that the integrity of that vote is maintained throughout the duration of the election. Like at the transmission phase, the BallotPoint servers store encrypted votes to ensure vote integrity is maintained while the votes are at rest on the server (while also helping to preserve voter confidentiality). The BallotPoint server employs two levels of encryption. First, the ES encrypts a vote using a standard encryption key common to the entire election (the "election key”). The now-encrypted vote (a “singly encrypted vote”) is then sent to the MRNS, which encrypts the vote again using an encryption key unique to that vote (creating a “doubly encrypted vote”). This double-encryption process provides additional protection for the integrity of the cast ballot because each level of encryption requires a different key to decrypt the vote, and those keys are stored on different servers, providing a level of separation in the event an attacker obtained access to one of the encryption keys. Exhibit B, the flowchart illustrating server-to-server interactions, summarizes these processes.

After the doubly encrypted vote is created by the MRNS, an algorithm is run on the doubly encrypted vote to create a SHA256 hash value.[26] The doubly encrypted vote is sent to the ES and the SHA256 hash value of the doubly encrypted vote is stored on the MRNS. The hash value factors in both the vote itself and certain ancillary data, so that each hash value is unique to that vote. But, because the hash value generated from the doubly encrypted vote consists of a (seemingly random) string of characters, a person viewing the hash values cannot (during the election or afterwards) determine the content of the underlying vote from the hash value. However, if any changes are made to the underlying vote (or the ancillary data that is factored into the hashing algorithm), a completely new hash value will be created, and the original hash value could not be generated.[27] Therefore, if, at the time of the tally, the hash

[26] SHA256 refers to a “Secure Hashing Algorithm” resulting in a 256-bit message digest, a commonly used cryptographic algorithm for which it is “computationally infeasible 1) to find a message that corresponds to a given message digest, or 2) to find two different messages that produce the same message digest.” NIST, *Federal Information Processing Standards Publication* 180-4 (March 2012), at iv.

[27] NIST explained this process in connection with the release of an additional SHA standard:

> Hash algorithms are broadly useful in the world of electronic communications. They transform a digital message into a short ‘message digest’ for use in digital signatures and other applications. Even a small change in the original message creates a change in the digest, making it easier to detect accidental or intentional changes to the original message. Hash functions can be used in a variety of security applications such as message authentication.

values generated from a given vote string on the ES do not match those on the MRNS, BallotPoint system administrators would be alerted that the record of the vote stored on one or the other system had been tampered with.

The generation and storage of the doubly encrypted vote and hash value in two different places (one on each server) provides an effective way to ensure that there is no tampering (intentional or otherwise) with the content of the vote between the time the hash value is generated and the time of the vote tally—if a generated hash value for a vote does not match a previously generated hash value, at least one of the vote data files has been tampered with, providing notice that the vote might be inaccurate. In particular, if any of the hash values present on the earlier tables of vote digests are not present on the final, post-tally table, it will alert officials or investigators to potential tampering or other interference with the content of saved votes between the time the table of vote digests was downloaded and the time the ballots were tallied.

As part of my review of the BallotPoint system, I compared a table of vote digest values that had been downloaded by Cindy Horan during the 2016 APFA National Officer Election and a table of vote digests generated after the conclusion of the election. This review disclosed no changes to vote digest values, indicating that no changes were made to recorded vote selections. From this evidence, I can conclude that there was no tampering or other interference with the integrity of votes while they were at rest on the BallotPoint system from the point when the vote digest table was generated. Based on the consistency of the downloaded table of vote digests and my understanding of the hashing process used by BallotPoint, I concluded that there is no reasonable probability that any of the votes were altered between the time they were recorded

Press Release, NIST, NIST Releases SHA-3 Cryptographic Hash Standard (August 5, 2015), *available at* https://www.nist.gov/news-events/news/2015/08/nist-releases-sha-3-cryptographic-hash-standard.

and encrypted in the BallotPoint system, and the time at which they were tallied at the end of the election.

4. Counting of the Ballots.

The final step in ensuring that voters' votes are counted-as-cast is the actual tallying of the ballots. To ensure that the BallotPoint system was accurately tallying the cast ballots, I reviewed the portion of the application code responsible for counting the cast ballots. This is a very straightforward program, and is functionally similar to tallying programs used in all manner of computer applications. Based on my experience designing and reviewing similar systems, there is no reasonable possibility that the BallotPoint application would make an error tallying the votes. Based on this review of the application code, I concluded that the tally of the vote totals sent by BallotPoint to APFA accurately reflected the sum of recorded votes for each candidate at the moment of the tally.

In addition, the BallotPoint application is capable of generating a report (referred to as a "Votes Table") that lists the plain-text vote string of all recorded ballots at the time of the tally. A person (or someone using a familiar computer program like Microsoft Excel) could count the number of votes cast for each candidate by reviewing these plain-text vote strings in order to verify independently that the BallotPoint-reported vote totals accurately reflected the recorded ballots at the time of the tally. By using simple Excel commands, I was able to conduct an automated recount of the vote strings stored in the Votes Table, and I independently confirmed that the recorded vote totals for each election choice matched the totals reported by BallotPoint to APFA.

Conclusion as to Principal Opinion B

The security architecture and security controls BallotPoint implemented and maintained during the 2016 APFA National Officer Election protected the integrity of: the authentication credentials sent to voters, ballot selections transmitted from voters to the election system, ballot selections made by voters at rest within the election system, and the tally results generated by the election system. These controls were sufficient to protect from any inadvertent or malicious attempts by credible, motivated attackers to manipulate or alter the results of the APFA election.

Once a voter submitted his or her ballot selections, it is very unlikely that those selections could have been changed after a voter had cast them and before they reached the election system because that communication was sufficiently encrypted by an industry-standard cryptographic protocol.

It is also very unlikely that the BallotPoint system would have captured and recorded voters' ballot selections incorrectly because the application code BallotPoint designed to perform those functions is well organized, mature, and maintained by a very small number of experienced BallotPoint employees.

Once a ballot has been cast and recorded by the BallotPoint system, it is very unlikely that modifications can be made to an existing vote without such a modification being noticed by BallotPoint employees and election officials because BallotPoint has implemented a sophisticated suite of encryption and hashing protocols designed to alert system administrators if such a modification occurs.

Finally, the method used to tally election results guarantees that only votes whose information found in one server (MRNS) matches vote information found in another server (ES) are counted. It is likewise very unlikely that the program would have mis-tallied the recorded votes because the portion of the code that performs the tallying is, again, well-organized, mature, and maintained by a very small number of experienced BallotPoint employees.

Throughout the voting, recording, and tallying process, there are very few opportunities to mishandle or manipulate votes. There are three (3) BallotPoint employees that have privileged access to the application source code; given this privileged status, these employees would have had the greatest opportunity to attempt to maliciously introduce application source code changes that could have affected the outcome of the election. These three employees represent a distinct threat because of their unique profile: insider, privileged, and skilled. However, it is very unlikely that such a malicious attempt to interfere with the results of the election could occur and go unnoticed, as it would likely require collusion between more than one employee. Moreover, the motivation of each of these employees to interfere with the election in this manner was very low. None of the BallotPoint privileged insiders are members of the APFA, and my assessment is that it is very unlikely that they would have been motivated to risk their livelihood on an attempt to throw the election. My assessment is that it is far more likely that the BallotPoint system administrators are highly motivated to ensure the proper function and unvarnished perception of the election system: accurate election results and user trust are vital to BallotPoint employees' success and future employment. Therefore, I assess the likelihood of intentional manipulation of the source code that is responsible for recording votes to be very low.

In sum, given the assessed security architecture, the threats to vote integrity, and the security controls in place to protect against those threats, the residual risk of manipulation of the election results, or of inadvertent system error that affected the election results, is very low. It is unreasonable to believe that the result of the election did not reflect the votes cast by the voting users of the system.

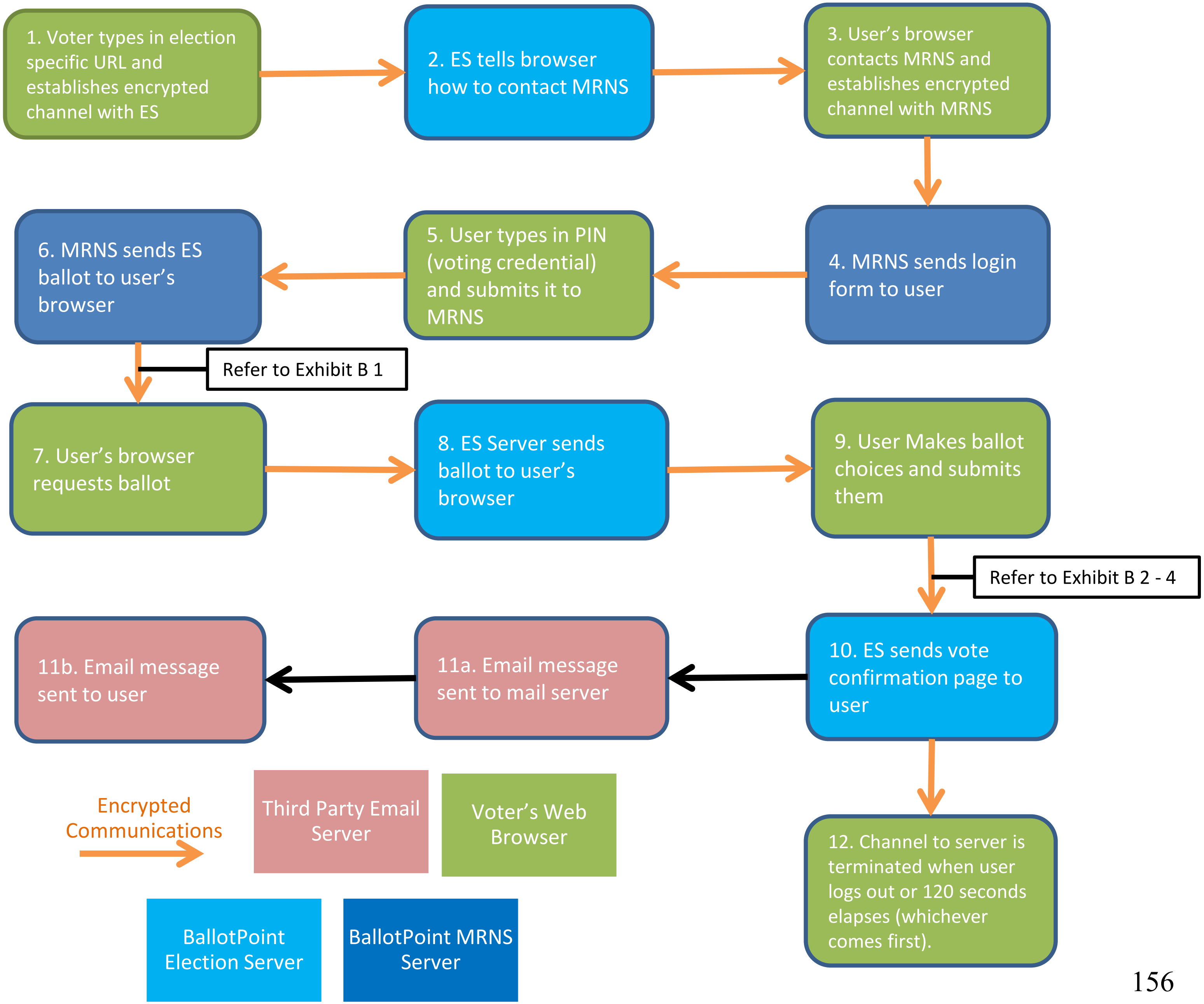
Curt Stapleton

Curt Stapleton

DATED: June 30, 2017

EXHIBIT A

Voter-Server Interactions



1. Voter types in election specific URL and establishes encrypted channel with ES

2. ES tells browser how to contact MRNS

3. User's browser contacts MRNS and establishes encrypted channel with MRNS

4. MRNS sends login form to user

5. User types in PIN (voting credential) and submits it to MRNS

6. MRNS sends ES ballot to user's browser

Refer to Exhibit B 1

7. User's browser requests ballot

8. ES Server sends ballot to user's browser

9. User Makes ballot choices and submits them

Refer to Exhibit B 2 - 4

10. ES sends vote confirmation page to user

11a. Email message sent to mail server

11b. Email message sent to user

12. Channel to server is terminated when user logs out or 120 seconds elapses (whichever comes first).

Encrypted Communications

Third Party Email Server

Voter's Web Browser

BallotPoint Election Server

BallotPoint MRNS Server

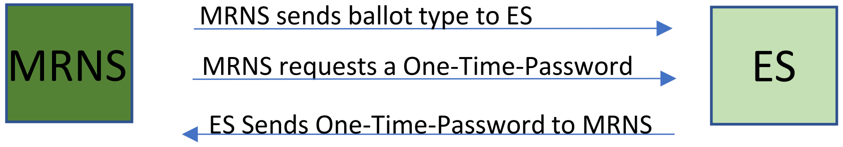
EXHIBIT B

Server-Server Interactions

Establish Voting Session

System Determines Voter Type

1



MRNS sends ballot type to ES

MRNS requests a One-Time-Password

ES Sends One-Time-Password to MRNS

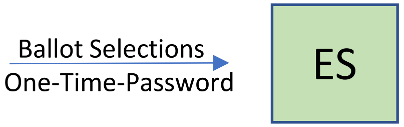
1. ES Generates One-Time-Password
2. ES Presents Ballot to User + One Time Password

The One-Time-Password is a random code that is never stored on disk
It allows the MRNS to associate messages sent with it to a distinct voter

Submit Vote

Voter submits ballot

2



Ballot Selections
One-Time-Password

Once the ballot has been submitted, ES knows:

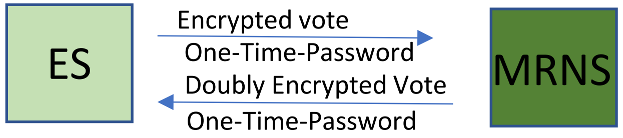
- The ballot selections made by the voter
- The one-time-password associated with this voting session

Record Vote

System encrypts and stores ballot

3

1. ES generates a new, unique code for vote.
2. The ballot selections and unique code are combined, and that combined information is encrypted.
3. The combined information is encrypted using the ES election key, and the result is the "Encrypted Vote".



Encrypted vote
One-Time-Password

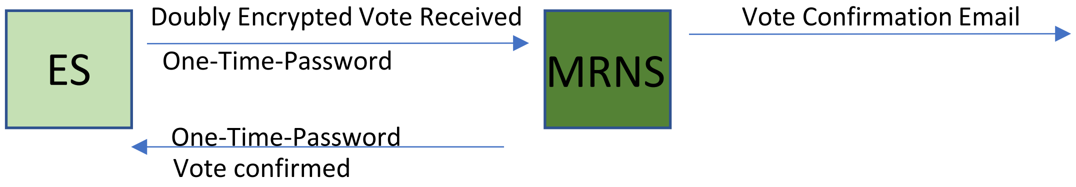
Doubly Encrypted Vote
One-Time-Password

1. MRNS generates a new key unique to the encrypted vote.
2. MRNS encrypts the Encrypted Vote using the new unique key, and the result is a "Doubly Encrypted Vote".
3. MRNS calculates a HASH value of the Doubly Encrypted Vote which is guaranteed to be unique.
4. MRNS stores the HASH value, and key locally.
5. MRNS sends the Doubly Encrypted Vote to the ES.

Confirm Vote Record

System confirms recording of vote

4



Doubly Encrypted Vote Received
One-Time-Password

One-Time-Password
Vote confirmed

Vote Confirmation Email

1. Once ES receives "Vote Confirmed" message, the one-time-password is destroyed and the 12 digit PIN cannot be used again to vote.

EXHIBIT C

Authoritative Literature

U.S. Dep’t of Commerce, National Institute of Standards and Technology, Special Publication 800-30, *Guide for Conducting Risk Assessments* (Sept. 2012).

U.S. Dep’t of Commerce, National Institute of Standards and Technology, Internal/Interagency Report 7770, *Security Considerations for Remote Electronic UOCAVA Voting* (Feb. 2011).

U.S. Dep't of Commerce, National Institute of Standards and Technology, Special Publication 800-123, *Guide to General Server Security*, (July 2008).

Ben Adida et. al, *Electing a University President using Open-Audit Voting: Analysis of real world use of Helios*, 2009 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (June 25, 2009).

TechRadar.com, *How SSL and TLS works*, (Jan. 2, 2012), *available at* http://www.techradar.com/news/software/how-ssl-and-tls-works-1047412.

U.S. Dep't of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards Publication 180-4, *Secure Hash Standard (SHS)* (March 2012).

Press Release, National Institute of Standards and Technology, *NIST Releases SHA-3 Cryptographic Hash Standard* (August 5, 2015), *available at* https://www.nist.gov/news-events/news/2015/08/nist-releases-sha-3-cryptographic-hash-standard.

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
FORT WORTH DIVISION

THOMAS E. PEREZ [now R. ALEXANDER ACOSTA], Secretary of Labor,

Plaintiff,

v.

ASSOCIATION OF PROFESSIONAL FLIGHT ATTENDANTS,

Defendant.

Civil Action No. 4:16-cv-1057-A

DECLARATION OF CINDY HORAN IN SUPPORT OF APFA'S MOTION FOR SUMMARY JUDGMENT

I, Cindy Horan, hereby declare as follows:

1. I am over the age of eighteen and am competent to testify as to all of the facts contained in this Declaration, of which I have first-hand, personal knowledge, or know from the business records of the Association of Professional Flight Attendants ("APFA").

2. The APFA is the largest independent flight attendant union in the United States. APFA represents over 26,000 flights attendants employed by American Airlines, and APFA members live in nearly all of the 50 states as well as several foreign countries.

3. APFA is administratively divided into 14 local units known as bases. The bases correspond generally to airports that serve as American Airlines hubs, although there are two bases at Reagan Washington National Airport (DCA), one representing legacy American Airlines flight attendants and one representing legacy U.S. Airways flight attendants. Each

APFA-represented flight attendant is assigned to a base, although many APFA members are "commuters" who do not live in close proximity to their assigned base. APFA also maintains three "satellite" bases (Atlanta (ATL), Minneapolis-St. Paul (MSP), and San Diego (SAN)), near which many flight attendants live and from which they might disembark for flights.

4. I have been employed by American Airlines as a flight attendant for over 25 years. I have been a member of the APFA for the length of my employment with American Airlines. Although I live in Round Hill, VA, I am currently assigned to the Miami, FL (MIA) base.

5. I was elected and served as APFA Base Vice Chair for Reagan Washington National Airport – International Flights from 1998 until 2003. I was elected and served as APFA Base Chair for Reagan Washington National Airport – International Flights from 2003 until 2007, and again for a period in 2008.

6. In 2010, I was appointed by the APFA Board of Directors to serve as a member of the National Ballot Committee ("NBC"). I served as a member of the NBC until August 2011, when I was elected by the other NBC members to serve as Chairperson of the NBC. I was reappointed as a member of the NBC and then re-elected as its Chairperson in 2014, and I served as Chairperson during the 2016 APFA National Officer Election. In 2016, after the conclusion of the National Officer Election, I was again reappointed by the APFA Board of Directors to the NBC and was again re-elected to serve as its Chairperson, and I continue to serve in that capacity today.

7. The NBC is a five-member committee established by the APFA Constitution that has responsibility for overseeing all facets of APFA elections and referenda. The duties of the NBC include but are not limited to: (1) supervising election and balloting procedures; (2)

determining eligibility of nominees; (3) overseeing the preparation of the ballots; (4) determining ballot validity; and (5) certifying the results of the balloting to the National Secretary or certifying contract referenda in accordance with the APFA Constitution.

8. When I first became a member of APFA, APFA conducted its elections via mail ballot. APFA continued to use mail ballots through about 2009, when APFA began using an electronic ballot system through which voters could cast their votes over the phone or via the internet. Sometime before my 2010 appointment to the NBC, APFA engaged BallotPoint Election Services to serve as APFA's third-party election administrator. Throughout my tenure on the NBC, APFA has used BallotPoint to administer both its officer elections and its contract referenda.

9. Through my service on the NBC, as well as my employment as a flight attendant, I have become familiar with the manner in which other unions with large, national memberships conduct their elections. In particular, I am familiar with the manner in which airline pilots and other flight attendant unions conduct elections. In each such instance of which I am aware, those unions conduct their elections via electronic ballot or mail ballot anytime the election requires the union to poll its entire membership (that is, in directly elected national officer elections and national contract referenda). Before the advent of electronic balloting, each such union of which I am aware conducted elections requiring a poll of the entire membership via mail ballot.

10. APFA-represented flight attendants are a highly mobile population. On any given day, approximately 40% of APFA members are flying on assigned international or domestic trips. Depending on these flight attendants' schedules, it can be difficult or impossible for flight attendants on trips to appear in-person at a voting booth to cast a ballot, even if APFA maintained and staffed voting booths at each of its 13 separate bases and 3 satellite bases.

11. Therefore, the practical effect of APFA conducting in-person balloting would be that, on any given day, a substantial percentage of APFA's membership would be unable to cast a vote and would be effectively disenfranchised.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Executed in Round Hill, VA, this 18 day of August, 2017.

Cindy Horan
Cindy Horan

Alderson®

COURT REPORTING

Transcript of **Cindy Horan**

July 27, 2017

Perez v. Association of Professional Flight Attendants

Alderson Reporting
1-800-367-3376
info@aldersonreporting.com
http://www.aldersonreporting.com

Alderson Reference Number: 71545

Page 1

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF TEXAS

FORT WORTH DIVISION

```
- - - - - - - - - - - - - - - - X
R. ALEXANDER ACOSTA,           :
Secretary of Labor             :
    Plaintiff,                 :  Civil Action No.
          v.                   :  4:16-cv-1057-A
ASSOCIATION OF PROFESSIONAL    :
FLIGHT ATTENDANTS,             :
    Defendant.                 :
- - - - - - - - - - - - - - - - X
```

Washington, D.C.

Thursday, July 27, 2017

Deposition of CINDY HORAN, a witness herein, called for examination by counsel for Plaintiff in the above-entitled matter, pursuant to notice, the witness being duly sworn by ANGELA K. MCCULLOUGH, RPR, a Notary Public in and for the District of Columbia, taken at the offices of Bredhoff & Kaiser PLLC, 805 15th Street, Northwest, Suite 1000, Washington, DC, at 9:52 a.m., Thursday,

Page 2

July 27, 2017, and the proceedings being taken down by Stenotype by ANGELA K. MCCULLOUGH, RPR, and transcribed under her direction.

Page 3

APPEARANCES:

On behalf of the Plaintiff:

BRIAN W. STOLTZ, ESQ.
JENNIFER FREY, ESQ.
U.S. Department of Justice
United States Attorney's Office
Northern District of Texas
1100 Commerce Street, Suite 300
Dallas, Texas 75242
(214) 659-8626
brian.stoltz@usdoj.gov

and

TAMBRA LEONARD, ESQ.
U.S. Department of Labor
Office of the Solicitor
200 Constitution Avenue, Northwest
Washington, DC 20210
(202) 693-5744
Leonard.tambra@dol.gov

Page 4

APPEARANCES (Continued):

On behalf of the Defendant:

ANDREW D. ROTH, ESQ.
ANDREW MILLER, ESQ.
Bredhoff & Kaiser, PLLC
805 15th Street, Northwest, 10th Floor
Washington, DC 20005
(202) 842-2600
aroth@bredhoff.com

ALSO PRESENT:

Ellen Kresha, DOJ Intern

Page 29

work, we have an employee number.

Q. You also mentioned a ballot as being uploaded to the BallotPoint website. And I take it the ballot -- let's say, for example, for the presidential race, the ballot would say who the candidates are; is that right?

A. That correct.

Q. And then is each -- I think I've seen one of these notices. But my understanding is that each candidate is assigned a number; is that right?

A. That's correct.

Q. So if a -- is the procedure that if a -- essentially the union members are instructed that in the presidential race, if you want to vote for candidate Joe Smith press or select 1; is that how it works?

A. That's correct.

Q. And, likewise, if you want to vote for candidate William Smith he would be candidate 2; is that right?

A. That's correct.

Q. Okay. So you had -- you mentioned that

Page 104

Notice Date: August 8, 2017

Deposition Date: July 27, 2017

Deponent: Cindy Horan

Case Name: Perez v. Association of Professional Flight Attendants

Page:Line Now Reads Should Read

______ ________________________ ___________________

______ ________________________ ___________________

______ ________________________ ___________________

______ ________________________ ___________________

______ ________________________ ___________________

______ ________________________ ___________________

______ ________________________ ___________________

______ ________________________ ___________________

______ ________________________ ___________________

______ ________________________ ___________________

______ ________________________ ___________________

______ ________________________ ___________________

______ ________________________ ___________________

______ ________________________ ___________________

______ ________________________ ___________________

______ ________________________ ___________________

Page 105

CERTIFICATE OF DEPONENT

I hereby certify that I have read and examined the foregoing transcript, and the same is a true and accurate record of the testimony given by me. Any additions or corrections that I feel are necessary, I will attach on a separate sheet of paper to the original transcript.

____

Signature of Deponent

I hereby certify that the individual representing himself/herself to be the above-named individual, appeared before me this _____ day of ___________, 2017, and executed the above certificate in my presence.

____

NOTARY PUBLIC IN AND FOR

____

County Name

MY COMMISSION EXPIRES:

CERTIFICATE OF REPORTER

UNITED STATES OF AMERICA) ss.:
DISTRICT OF COLUMBIA)

I, ANGELA MCCULLLOUGH, the officer before whom the foregoing proceedings were taken, do hereby certify that the foregoing transcript is a true and correct record of the proceedings; that said proceedings were taken by me stenographically to the best of my ability and thereafter reduced to typewriting under my supervision; and that I am neither counsel for, related to, nor employed by any of the parties to this case and have no interest, financial or otherwise, in its outcome.

Angela K. McCullough
Notary Public in and for
The District of Columbia

My commission expires: 1/31/2020

ANGELA K. MCCULLOUGH
NOTARY PUBLIC
DISTRICT OF COLUMBIA
MY COMMISSION EXPIRES 01-31-2020