THE VISIBILITY OF FBI'S CLOSE HOLD: JOHN DURHAM WILL BLAME MICHAEL SUSSMANN THAT FBI TOLD ALFA BANK THEY WERE INVESTIGATING

Thanks to those who've donated to help defray the costs of trial transcripts*. Your generosity has funded the expected costs of transcripts. But if you appreciate the kind of coverage no one else is offering, we're still happy to accept donations. This coverage reflects the culmination of eight months work.*

According to an exchange at the end of they day yesterday, John Durham's team plans to introduce "a hundred" exhibits through their paralegal acting as a summary witness today.

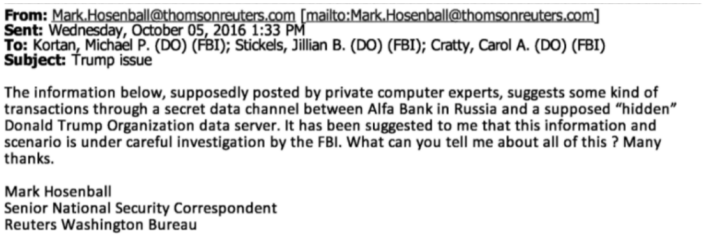
> My understanding is that the defense objects to the PowerPoint presentation style of the process. But, again, we think it just streamlines it in terms of — the alternative is to have to put literally a hundred exhibits in through Ms. Arsenault one at a time.

Given the exhibits from Monday, I assume Durham will throw a bunch of Fusion documents at the jury in an attempt to insinuate, once again, that Michael Sussmann shared with the press that the FBI was investigating the Alfa Bank anomaly.

The coming onslaught of Fusion documents

I say that because Mark Hosenball wrote the FBI for comment at 1:33PM on October 5, 2016,

attaching the Mediafire package, asking for comment and noting that, "it has been suggested to me that this information and scenario is under careful investigation by the FBI."



From: Mark.Hosenball@thomsonreuters.com [mailto:Mark.Hosenball@thomsonreuters.com]
Sent: Wednesday, October 05, 2016 1:33 PM
To: Kortan, Michael P. (DO) (FBI); Stickels, Jillian B. (DO) (FBI); Cratty, Carol A. (DO) (FBI)
Subject: Trump issue

The information below, supposedly posted by private computer experts, suggests some kind of transactions through a secret data channel between Alfa Bank in Russia and a supposed "hidden" Donald Trump Organization data server. It has been suggested to me that this information and scenario is under careful investigation by the FBI. What can you tell me about all of this ? Many thanks.

Mark Hosenball
Senior National Security Correspondent
Reuters Washington Bureau

Hosenball's email to the FBI puts it right at the beginning (in red, below) of the known universe of Fusion emails we've seen from that day, the timestamps of which Durham has repeatedly tried to obscure. (Maybe while paralegal Kori Arsenault is on the stand, Sussmann's team can ask her why Durham's exhibits misleadingly don't correct for UTC.)

That said, there's still a Hosenball email unaccounted for in which he shared one of the publicly available links to Tea Leaves packaged data. It's quite possible that email precedes Seago's question to Fritsch, which is currently the earliest email in the list, asking whether one of the i2p sites hosting the data was safe. See this post for background.

5:23PM (likely 1:23?): Seago to Fritsch, Is this safe?

1:31PM: [not included] Fritsch to Hosenball email with Alfa Group overview

1:32PM: Fritsch sends Isikoff the September 1, 2016 Alfa Group overview (full report included in unsealed exhibit)

1:33PM: Hosenball to FBI, "careful investigation by the FBI"

1:33PM [not included] Fritsch to Hosenball, "that memo is OTR – tho all open source"

1:35/1:36PM: Hosenball replies, "yep got it, but is that from you all or from the outside computer experts?"

1:37PM: Fritsch responds,

> the DNS stuff? not us at all
>
> outside computer experts
>
> we did put up an alfa memo unrelated to all this

1:38PM: [not included] Hosenball to Fritsch:

> is the alfa attachment you just sent me experts or yours ? also is there additional data posted by the experts ? all I have found is *the summary I sent you* and a chart… [my emphasis]

1:41PM: [not included] Fritsch to Hosenball:

> alfa was something we did unrelated to this. i sent you what we have BUT it gives you a tutanota address to leave questions. 1. Leave questions at: tea.leaves@tuta.io

1:41PM: [not included] Hosenball to Fritsch:

> yes I have emailed tuta and they have responded but haven't sent me any new links yet. but I am pressing. but have you downloaded more data from them ?

1:43PM: [not included] Fritsch to Hosenball, "no"

1:44PM: Fritsch to Lichtblau:

> **fyi found this published on web … and downloaded it. super interesting in context of our discussions**
>
> **[mediafire link]** [my emphasis]

2:23PM: [not included] Lichtblau to Fritsch, "thanks. where did this come from?"

2:27PM: [not included] Hosenball to Fritsch:

> tuta sent me this guidance
>
> [snip]
>
> Since I am technically hopeless I have asked our techie person to try to get into this. But here is the raw info in case you get there first. Chrs mh

2:32PM: Fritsch to Lichtblau:

> no idea. our tech maven says it was first posted via reddit. i see it has a tutanota contact — so someone anonymous and encrypted. so it's either someone real who has real info or one of donald's 400 pounders. the de vos stuff looks rank to me … weird

6:33PM (likely 2:33PM): Fwd Alfa Fritsch to Seago

6:57PM (like 2:57PM): Re alfa Seago to Fritsch

7:02PM (likely 3:02): Re alfa Seago to Fritsch

3:27PM: [not included] Fritsch to Hosenball cc Simpson: "All same stuff"

3:58PM: [not included] Hosenball to Fritsch, asking, "so the trumpies just sent me the explanation below; how do I get behind it?"

4:28PM: [not included] Fritsch to Hosenball, "not easily, alas"

4:32PM: Fritsch to Hosenball, cc Simpson:

> Though first step is to send that explanation to the source who posted this stuff. I understand the trump explanations can be refuted.

So I assume that Durham will argue that Fusion *must have* passed on the information that the FBI was investigating — and they may have! (though none of the currently public emails reflect that — and suggest that was all part of Michael Sussmann's devious plan on September 19.

When, under threat of prosecution, an attempt to prevent politicization turns into an attempt to hide political bias

That's where things will get interesting. One key dispute in this case is why one keeps secrets. Durham wants to argue that keeping secrets can only serve a political purpose.

Sussmann will argue that keeping secrets facilitates national security interests.

Sussmann will show that everyone at the FBI recognized the value, to the FBI, of stalling a newspaper article about a potentially important threat so the FBI could covertly investigate it. All the more so during election season when — investigation after investigation into the Russian investigation has shown — the FBI was, if anything, being *too* careful in an attempt to avoid impacting Trump's political fortunes, even while Jim Comey was tanking Hillary's campaign. According to Sussmann's own sworn testimony — testimony that Durham didn't bother testing before charging Sussmann — allowing the FBI the opportunity to do that was the reason Sussmann shared the Alfa Bank anomaly with the FBI. Durham wants to imprison Sussmann for giving the FBI that heads up, arguing that because he hid his purported clients, it led the FBI to open a Full Investigation more quickly than they otherwise would have (even though, as Sussmann's team has demonstrated, the FBI did nothing that would have required a Full Investigation in the short period during which they investigated).

A key part of that story Durham wants to tell — needs to tell, given all the evidence that the FBI perceived this to be a DNC-related tip — is that some of his key villains were attempting to hide the perceived political nature of the tip,

rather than ensuring the integrity of the investigation itself (or possibly, but I'm still working on this, protecting the identity of a CHS).

Central to that narrative is the changing testimony of FBI Agent Ryan Gaynor — his stated reasons for refusing to let the case agents in Chicago interview either Sussmann or Georgia Tech professor David Dagon. In an interview on October 30, 2020 (a week after Durham had been granted Special Counsel status), Gaynor explained that he had intervened to make sure agents couldn't conduct interviews that would have led to a more robust investigation to ensure the integrity of the investigation.

> Q. Okay. So you remember telling the government that you believed that the agents in Chicago would have been biased by Mr. Sussmann's perception of the issue — the source's perception of the issue if they had interviewed him before they got all of the data and analyzed it?
>
> A. Yes.
>
> Q. Okay. And that's because, at the time, you believed the DNC was the source of the information itself. Right?
>
> A. That's because, at the time, I believed that he was a DNC attorney associated with the Democratic party and it would be potentially highly-biasing information.
>
> Q. And you told the government, if you had provided the identity of the DNC as the source of the information, they would have known there was possible political motivation. rignt?
>
> A. I recall that exact statement.

Shortly after he gave this testimony, prosecutors took a break, and told his lawyer they were moving towards treating Gaynor as a

subject of, rather than just a witness in, the investigation.

> Q. Okay. Well, at or around the time you were talking about passing along the source's name or not, you took a break in the meeting. Do you remember taking breaks during the meeting?
>
> A. I do.
>
> Q. And do you remember when you broke at that point that the government told your attorney that your own status in the investigation had changed. Do you remember hearing that?
>
> A. So I didn't hear that, but when my attorney came back in, he advised me that my status was in jeopardy.

After that, Gaynor went back, looked at two sets of scribbled notes (Gaynor, because he remains at FBI, was able to review his notes, unlike a number of other Durham witnesses), and decided that now that he thought about it, Jonathan Moffa had actually instructed him to keep a close hold on Sussmann's identity. It wasn't his decision anymore, it was Moffa's, and the dastardly Peter Strzok was in on it. Once Gaynor testified that way, he became a — to Andew DeFilippis, anyway — credible witness again.

> Q. Okay. And when you told the government there was a close hold, were you told that your status changed back to being a witness?
>
> A. At the conclusion of the interview, once I had gone over all of the material that I brought and walked through what I had reconstructed and what I could recollect after doing so, I was informed that my status had changed, yes.
>
> Q. Changed back to being a witness?
>
> A. To a witness, yes.

> Q. So you go into meeting one being told you are a witness, telling them you decided not to share the agents' names among other things. Then you are told you are a subject facing criminal charges, potentially. You come back. You tell them about a close hold, and you go back to being a witness; is that right?

Politico may have been the only outlet that described this fairly shocking testimony.

These conflicting claims about the purported reasons to keep Sussmann's identity (as opposed to the investigation itself) a secret are important background to that Hosenball email on October 5, which I suspect Durham will use to claim that the Democrats were leaking about the investigation.

Starting almost immediately after getting the investigation, Chicago case agents started asking to interview the source, variously defined to be either Sussmann or the person who wrote the white paper. Gaynor kept pushing the agents to go review the logs again — though the file memorializing the contents of what it describes as a single thumb drive (Sussmann shared two) was not written up until October 4. But then, by October 5 (the same day that Hosenball asked the FBI for comment, albeit this report comes in four hours later), FBI had learned from one of their confidential human sources that David Dagon had a role in the white paper and he — *and the FBI's own source!* — would be going public pushing the credibility of the allegations.

- The aforementioned CHS, as well as David Dagan, are expected to directly contradict FBI assessments and will report that there is credible evidence of covert communications between Trump email servers and Alfa bank. Their assessments do not change ours, but pose a challenge in refuting their claims using only open source information.
- We are analyzing logs provided by Central Dynamics. So far, these logs do not show any evidence of the covert channel mentioned in the white paper. Central Dynamics provided all of the firewall logs affiliated with the 4 Alfa Bank IP addresses of interest, and in no instance is there any record of any of those IP addresses communicating with the mail1.trump-email.com IP address.
- Server logs from Listrak, the ISP that hosts the domain, are forthcoming, and should offer definitive evidence of the nature of any activity between Alfa Bank DNS servers and any email domains associated with IP address 66.216.133.29. We have also reached out to the agent in Miami to obtain more specific logs on this particular IP address, to be sure we aren't missing anything captured in the firewall logs already provided.
- We are going to speak to David Dagon, and see if he has any new information for us.
- The CHS believes the article will be published in the Washington Post and New York Times on Sunday.

In that email, newbie agent Allison Sands explained that they were going to contact Dagon.

So, among other things, on the same day Hosenball writes in reflecting an awareness that there was an ongoing investigation, the FBI hears from a CHS who says he or she has already been talking with David Dagon and was going public backing the claims (though this source was speaking to the WaPo, not Reuters).

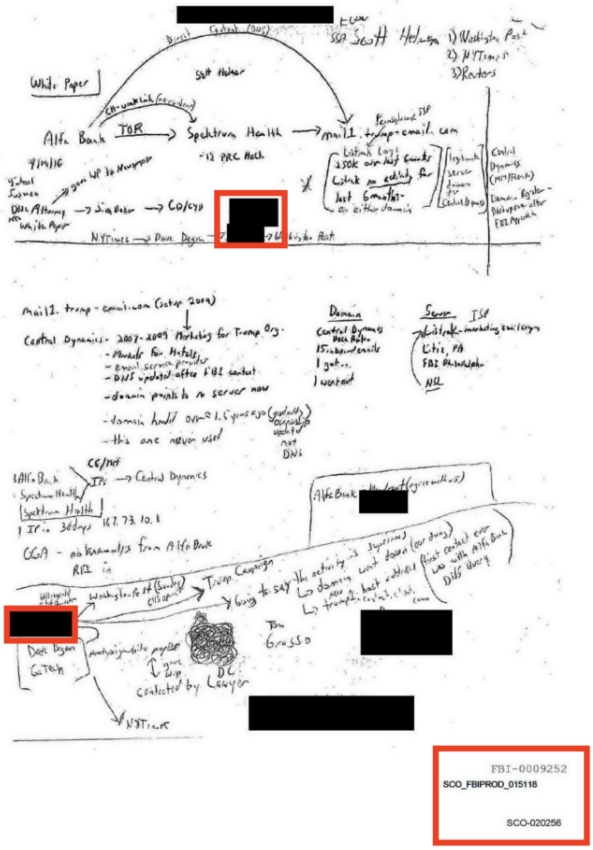
Note that, as of that date, the FBI still hadn't received logs from Listrak.

By the time Allison Sands wrote that email, it appears from Lync messages that like others probably haven't been noticed to reflect UTC time zone, had already contacted Rodney Joffe's handler to contact Dagon.

10/5/2016 18:58	txgrasso@fbi.sgov.gov	asands@fbi.sgov.gov	one other thing, I told Dagon that you would be able to protect his identity so that his name is not made public. Please take that into consideration when talking to him. It may be more forthing coming in a protect-identity type converstaion.	Message	text/html
10/5/2016 19:00	asands@fbi.sgov.gov	txgrasso@fbi.sgov.gov	does dagon have a clearance?	Message	text/html

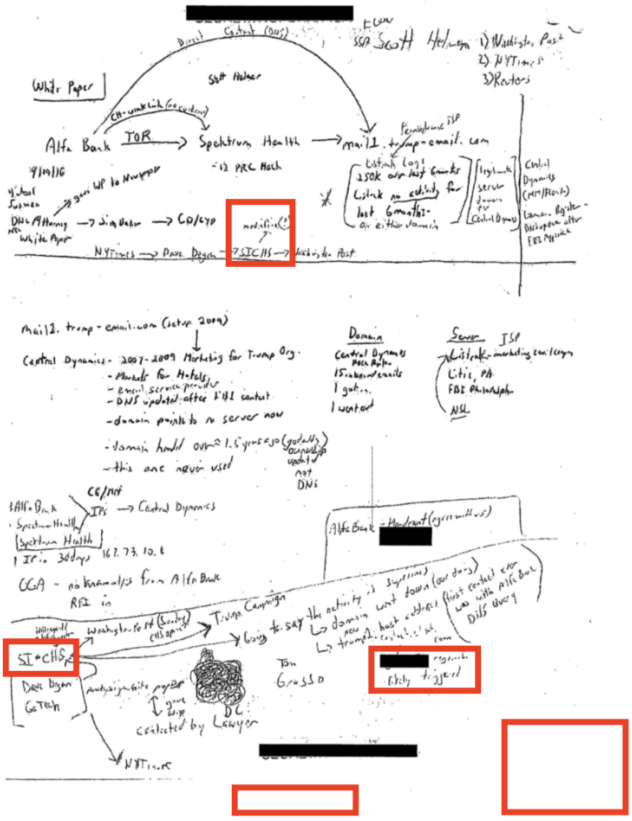
Fun with missing Bates stamps

Side note. There are actually two versions of the notes that purportedly caused Gaynor to change his mind about there being a close hold and on what source that close hold was on. There's Defense Exhibit 524, which has a slew of Bates stamps, and 7 redactions.



No. 1:21-cr-00582-CRC (D.D.C.) DX-524_0001

And then there's a page from Government Exhibit 279, which appears between a page with Bates stamp SC-6454 and one with Bates stamp SC-6456, which has no Bates stamp at all (and lacks the protective order stamp that appears on the other pages of the exhibit).



That version of the exhibit has just four redactions, one of which is smaller. The unredacted bits on the exhibit reveal discussions of the informant and recognition that the statements of the informant "likely triggered" the press attention.

Incidentally, Durham's team took an entire day to upload this set of exhibits. I'm wondering if the exhibit that was viewed by Gaynor and entered into evidence actually looked like this one does.

Calling the agent of a foreign agent to ask for comment

There's one other thing going on. On the stand, Gaynor spent a great deal of time explaining about how important it was to hide an investigation — particularly from anyone who might have a partisan interest — during an election.

Except for all the talk of a close hold, the FBI wasn't holding this very close. They were stomping around to a bunch of sources asking for data logs, even before they had checked what was on (one of) the thumb drives that Sussmann had dropped off. They fairly demonstrably were stomping around before they understood what they should be looking for.

They also were calling Mandiant, which was working for Alfa Bank, which by October 19 when they were formally interviewed discovered Alfa Bank had no logs, but which knew of the investigation by October 5.

> Q. Uh-huh. You testified about the reasons why you'd want to keep it covert, you wouldn't want to do anything that could affect the election so close to the election. Right?
>
> A. Yes.
>
> Q. The FBI, as part of the Alfa-Bank investigation, talked to a number of different individuals outside of the FBI to acquire information, to get you information so that you could investigate the allegations. Right?
>
> A. Yes.
>
> Q. Okay. You spoke to people at Central Dynamics?
>
> A. Yes, and I believe the investigative team documented in the email that I saw that they had done it in a manner to attempt to avoid it outing the allegation.
>
> [snip]
>
> A. I'm sorry?
>
> Q. And how is that that they could conduct an interview with a third party in a way that the third party wouldn't tell other people about it?
>
> A. They described it in a manner that

> they had obfuscated what their direct interest was.
>
> Q. So from the Central Dynamics' perspective, they didn't know what you were looking at?
>
> A. That is what I had in the email chain, yes. n
>
> Q. But you testified that the FBI interviewed Mandiant as part of the investigation. Correct?
>
> A. Yes. My understanding there is that was a private liaison relationship that occurred.
>
> Q. Mandiant – just to be clear – Alfa-Bank itself hired Mandiant to analyze whether there was a secret communications channel. Correct?
>
> A. Yes.
>
> Q. So Alfa-Bank paid Mandiant to look into whether there was a secret communications channel. Right?
>
> A. Yes.
>
> Q. And Alfa-Bank obviously had a relationship with Mandiant that was put at issue by hiring Mandiant. Right?
>
> A. Yes.
>
> Q. Okay. So the FBI went to Alfa-Bank's paid consultant and asked them for their view on the allegation. Correct?
>
> A. I believe the FBI had a prior relationship with one of the employees, and they utilized that in the field. Plus, I don't think the Bureau would violate policy on a sensitive investigative matter when the Chief Division Counsel of the office is involved. So I would assume that they did that in a manner that they did not feel would be alerting or go to the

media.

Q. Mr. Gaynor, the FBI in this investigation went to Alfa-Bank's paid consultant and asked them for their views of the allegations. correct?

A. Yes.

Q. And Alfa-Bank's paid consultant could have told Alfa-Bank. Correct?

A. Yes.

Q. And could have told the press for all you know. Correct?

A. Yes. And I don't know how Chicago mitigated that.

Q. And is it your testimony that going to Alfa-Bank, the Russian bank that is the focus of this investigation, and asking their paid consultant for their views on the matter wasn't going to overt?

A. Again, I don't know how Chicago mitigated that issue.

[snip]

Q. Did you ever have a conversation with anybody at headquarters about whether to provide the names of the source to the Chicago agents?

A. Yes. There was a conversation about the close hold, as I mentioned, although it wasn't correctly, I guess, documented between Pete Strzok, myself and Mr. Moffa at some point during that time period.

[snip]

Q. And the reason that you say no one talked to him is because, as of that point, October 6th, you had already concluded that there was nothing to these allegations. Right?

> A. As of October 5th, evening of October 5th, we had come to a pretty solid conclusion that these allegations did not have merit and there wasn't a national security threat.
>
> Q. Are you aware that the agents first interviewed Alfa-Bank's paid consultant, Mandiant, merely two weeks later on October 19th?
>
> A. So I'm aware that we had information from Mandiant as of October 5th that they had looked at this allegation and found that it didn't have merit. And then I'm also aware that there was an interview that was conducted later, October 19th or so, when I was made aware of it, yes.

A text between Allison Sands and Scott Hellman reflects the FBI had contact with Alfa Bank by October 4.

7827	10/4/2016	13:28:32	From: asands To: sjhellman	we are going through and looking for any Alfa bank activity at all, but we got a report on the Alfa Bank side that they also think this is nothing

It appears that contact occurred in London — a place where Mark Hosenball has strong source ties since the time in 1976 when he got expelled for reporting on Northern Ireland.

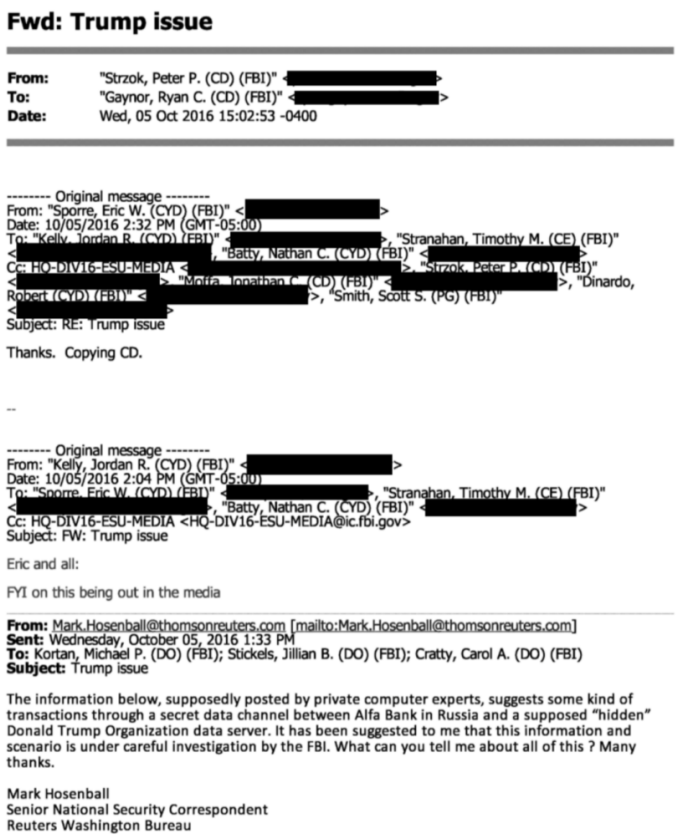
7840	10/4/2016	13:30:56	From: asands To: sjhellman	it looks like the clearing house in London received the same/ similar white paper
7841	10/4/2016	13:30:57	From: sjhellman To: asands	I'm working with LA on them too
7842	10/4/2016	13:31:01	From: sjhellman To: asands	omg
7843	10/4/2016	13:31:09	From: asands To: sjhellman	and contacted their reps at alfa bank

In other words, Gaynor's currently operative stance is that case agents couldn't contact David Dagon — much less Rodney Joffe, who had business ties with the FBI — to find out what was going on, because that would present a conflict.

But it was okay for the FBI to contact the agent of the subject of the investigation overtly.

Agent Gaynor belatedly rediscovers the Mediafire package

Incidentally, when that original request for comment from Hosenball came in, it got transferred to people in the cyber division, then shared with the investigative team. In response, the senior-most person on that team sent it to Peter Strzok. Strzok forwarded it, at 3:02 on October 5, to Ryan Gaynor.



Fwd: Trump issue

From: "Strzok, Peter P. (CD) (FBI)" <[redacted]>
To: "Gaynor, Ryan C. (CD) (FBI)" <[redacted]>
Date: Wed, 05 Oct 2016 15:02:53 -0400

-------- Original message --------
From: "Sporre, Eric W. (CYD) (FBI)" <[redacted]>
Date: 10/05/2016 2:32 PM (GMT-05:00)
To: "Kelly, Jordan R. (CYD) (FBI)" <[redacted]>, "Stranahan, Timothy M. (CE) (FBI)" <[redacted]>, "Batty, Nathan C. (CYD) (FBI)" <[redacted]>
Cc: HQ-DIV16-ESU-MEDIA <[redacted]>, "Strzok, Peter P. (CD) (FBI)" <[redacted]>, "Moffa, Jonathan C. (CD) (FBI)" <[redacted]>, "Dinardo, Robert (CYD) (FBI)" <[redacted]>, "Smith, Scott S. (PG) (FBI)" <[redacted]>
Subject: RE: Trump issue

Thanks. Copying CD.

--

-------- Original message --------
From: "Kelly, Jordan R. (CYD) (FBI)" <[redacted]>
Date: 10/05/2016 2:04 PM (GMT-05:00)
To: "Sporre, Eric W. (CYD) (FBI)" <[redacted]>, "Stranahan, Timothy M. (CE) (FBI)" <[redacted]>, "Batty, Nathan C. (CYD) (FBI)" <[redacted]>
Cc: HQ-DIV16-ESU-MEDIA <HQ-DIV16-ESU-MEDIA@ic.fbi.gov>
Subject: FW: Trump issue

Eric and all:

FYI on this being out in the media

From: Mark.Hosenball@thomsonreuters.com [mailto:Mark.Hosenball@thomsonreuters.com]
Sent: Wednesday, October 05, 2016 1:33 PM
To: Kortan, Michael P. (DO) (FBI); Stickels, Jillian B. (DO) (FBI); Cratty, Carol A. (DO) (FBI)
Subject: Trump issue

The information below, supposedly posted by private computer experts, suggests some kind of transactions through a secret data channel between Alfa Bank in Russia and a supposed "hidden" Donald Trump Organization data server. It has been suggested to me that this information and scenario is under careful investigation by the FBI. What can you tell me about all of this ? Many thanks.

Mark Hosenball
Senior National Security Correspondent
Reuters Washington Bureau

On October 13, just over a week after he had originally received it, Gaynor sent the Mediafire package to the case team, noting that the observations in it reflected actions taken in response to their investigation, but asking for their technical opinion.

From: GAYNOR, RYAN C. (CD) (FBI) <[redacted]>
Sent: Thursday, October 13, 2016 5:45 PM
To: WIERZBICKI, DANIEL S. (CG) (FBI) <[redacted]>; HEIDE, CURTIS A. (CG) (FBI) <[redacted]>; SANDS, ALLISON (CG) (FBI) <[redacted]>
Cc: PIENTKA, JOE (WF) (FBI) <[redacted]>; MOFFA, JONATHAN C. (CD) (FBI) <[redacted]>
Subject: FW: Online information --- [redacted]
Attach: [Untitled].pdf

Classification: [redacted]

Classified By: [redacted]
Derived From: FBI NSIC dated 20120629
Declassify On: 50X1-HUM

TRANSITORY RECORD

CG,

I am interested on your thoughts on the attached paper. This was found online at the address noted at the top of the paper (mediafire.com). Looks like the argument in this paper is largely supported by activity likely caused by our investigation and other acts by [redacted] but I would like your technical opinion on this paper. Is this related to the [redacted] and do we have information which can you help explain the 'new' trump email domain now pointed at the original server?

As Always, Thank you for the great work on this,
-Ryan

He included Moffa and Joe Pientka on that email.

But not Strzok, who knew he had received it 8 days earlier.

OTHER SUSSMANN TRIAL COVERAGE

Scene-Setter for the Sussmann Trial, Part One: The Elements of the Offense

Scene-Setter for the Sussmann Trial, Part Two: The Witnesses

The Founding Fantasy of Durham's Prosecution of Michael Sussmann: Hillary's Successful October Surprise

With a Much-Anticipated Fusion GPS Witness, Andrew DeFilippis Bangs the Table

John Durham's Lies with Metadata

emptywheel's Continuing Obsession with Sticky Notes, Michael Sussmann Trial Edition

Brittain Shaw's Privileged Attempt to Misrepresent Eric Lichtblau's Privilege

The Methodology of Andrew DeFilippis' Elaborate Plot to Break Judge Cooper's Rules

Jim Baker's Tweet and the Recidivist Foreign Influence Cheater

That Clinton Tweet Could Lead To a Mistrial (or Reversal on Appeal)

John Durham Is Prosecuting Michael Sussmann for Sharing a Tip on Now-Sanctioned Alfa Bank

Apprehension and Dread with Bates Stamps: The Case of Jim Baker’s Missing Jencks Production

Technical Exhibits, Michael Sussmann Trial

Jim Baker’s “Doctored” Memory Forgot the Meeting He Had Immediately After His Michael Sussmann Meeting

The FBI Believed Michael Sussmann Was Working for the DNC … Until Andrew DeFilippis Coached Them to Believe Otherwise