FD-1057 (Rev. 5-8-10)

[redacted]

FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: [redacted] Opening EC - ALFA BANK **Date:** 09/23/2016

CC: JONATHAN C. MOFFA
Joe Pientka III
John F. Stofer
Paul M. Maric
STRZOK PETER P II

From: CHICAGO
CG-CY-1
Contact: Allison Sands, 312-829-8628

Approved By: SSA Daniel S. Wierzbicki
A/CDC STEVEN MOLESKY
ASAC John A. Brown
SAC Michael J. Anderson

Drafted By: Allison Sands
Curtis A. Heide

Case ID #: [redacted] [redacted] ALFA BANK;
FCI RUSSIA - CONTACTS / AGENTS
SENSITIVE INVESTIGATIVE MATTER

Synopsis: [redacted] Documents the opening of a Full Field Investigation into the network communications between a US-based server and the Russian ALFA BANK organization.

Reason: 1.4(b)
Derived From: National Security Information SCG
Declassify On: 20261231

Full Investigation Initiated: 09/23/2016

Enclosure(s): Enclosed are the following items:
1. (U//FOUO) White Paper

[redacted]

GOVERNMENT EXHIBIT
0200
21-CR-582 CRC

FBI_ALFA_000001
SCO_FBIPROD_000001
SCO-001600

[redacted]

Title: [redacted] Opening EC - ALFA BANK
Re: [redacted], 09/23/2016

Details:

[redacted] On or about September 19, 2016, FBI received a referral of information from the US DEPARTMENT OF JUSTICE, detailing an unusually configured email server in Pennsylvania belonging to the TRUMP ORGANIZATION. In that referral, the DEPARTMENT OF JUSTICE provided the FBI with a whitepaper that was produced by an anonymous third party. According to the whitepaper, a U.S.-based server that is owned by the TRUMP ORGANIZATION has been communicating with the Russian-based ALFA BANK organization in Moscow, Russia. The third party identified that some of the communications were utilizing a TOR node, which is a means of obfuscating a user's true network location on the Internet. The TOR node was identified at an organization called SPECTRUM HEALTH, located in the State of Michigan. Additionally, the servers are reportedly configured for direct and exclusive communication between the TRUMP ORGANIZATION and the ALFA BANK entity. Additional details from the predicating report are listed as follows:

[redacted] On approximately July 28, 2016, a lookup in global DNS returned 15 unique hostnames containing "mail," "smtp," "relay," or "mta" that were registered to the TRUMP ORGANIZATION. A computerized and manual scan revealed anomalous data on one the the domains: mail1.trump-email.com [IP address 66.216.133.29]. An open source WHOIS lookup confirmed that the parent domain for mail1.trump-email.com is registered to the TRUMP ORGANIZATION.

[redacted] In the 90 day period May 4, 2016 to September 4 2016, only 19 external IP addresses conducted an A Record search for mail1.trump-email.com, a much smaller number of IP addresses than expected in normal traffic. Of the 19 IP addresses, the vast majority of the lookups came from the same three IP addresses: 217.12.97.15 [ALFA BANK], 217.12.96.15 [ALFA BANK], 167.73.110.8 [SPECTRUM HEALTH]. The SPECTRUM HEALTH IP address has been identified as a TOR exit node that is used exclusively by the Russian ALFA BANK entity. Notably, the majority of the lookups for this mail server by ALFA BANK were not for the MX [mail record], indicating that the server was set up to

[redacted]

masquerade as a regular (non-mail) server. Also, mail1.trump-email.com is configured to only accept email from pre-approved IP addresses.

[redacted] Based on the information above, FBI Chicago has predicated a Full Field Counterintelligence investigation into the activities of ALFA BANK, in order to conduct further investigation regarding the extent and nature of the network communications between ALFA BANK and the TRUMP ORGANIZATION. This investigation will attempt to determine the validity of the information that was provided by the third-party entity, and to assess whether or not pose a threat to either the TRUMP ORGANIZATION, or United States national security.

[redacted] In addition, FBI investigation [redacted] [CROSSFIRE HURRICANE] was predicated based on an allegation that a member of the TRUMP campaign had received a suggestion from the Russian Government, indicating that the Russian government could assist the TRUMP campaign with an anonymous release of information during the campaign, which would be a detriment to the HILLARY CLINTON campaign. Investigation in [redacted] has surfaced additional ties between the TRUMP campaign team and the Russian government.

[redacted] Investigation of the communications between the Russian ALFA BANK and the TRUMP ORGANIZATION could provide additional insight about the connections between the TRUMP ORGANIZATION and Russia, and help to determine whether those ties pose a threat to United States national security.

[redacted] This matter is being treated as a Sensitive Investigative Matter based on the fact that the TRUMP ORGANIZATION is affiliated with a current U.S. Presidential candidate. As such, FBI Chicago requests that FBIHQ/NSLB coordinate with the US DEPARTMENT OF JUSTICE to provide all appropriate notifications required by the DIOG.

♦♦

[redacted]

White Paper #1 - Auditable V3

Findings:

The Trump Organization is using a very unusually-configured "secret" email server in Pennsylvania for current and ongoing email communications with Alfa Bank (Moscow), and with Alfa Bank (Moscow) through another unusually-configured server (a "Tor exit node") at Spectrum Health in Michigan.

These servers are configured for direct communications between the Trump organization and Alfa Bank to the exclusion of all other systems.

The only plausible explanation for this server configuration is that it shows the Trump Organization and Alfa Bank to be using multiple sophisticated layers of protection in order to obfuscate their considerable recent email traffic.

Discussion:

1. On approximately July 28, 2016, a lookup in global DNS for all the hostnames with a domain name that has the word "Trump" in it yielded 1,933 domains. [File: PTR-Contains-Trump-1933.txt]

2. Another look-up for all domains registered by the Trump organization yielded 3,352 domains. [Filename: Trump-Domains-Registered-3352.txt]

3. Searching the data set in #1 for hostnames containing "mail," "smtp," "relay," or "mta" yielded 537 unique hostnames (i.e., machine names). (Includes irrelevant results such as "Trumpets for America.") [Filename: Trump-And-Mail-MTA-Relay-Etc-537.txt]

4. Of the 537 unique hostnames in #3, 15 were registered by the Trump Organization. [Filename: Trump-Owned-And-Mail-Systems-15.txt]

5. Manual verification (by manually looking at the hosting location, the name servers and the domain ownership details) confirmed that the 15 hostnames registered by the Trump Organization (in #4) were owned and controlled by the Trump Organization. [Filename: Trump-Owned-And-Mail-System-WHOIS-15.txt]

6. A search of global nonpublic DNS activity revealed from which IP addresses in the world systems looked up these 15 domains, in the 90 day period from May 4 - Sept. 4, 2016. [Sample of output of search - Filename: MX-Lookups-For-15-Trump-Related-Domains.txt]

7. A computerized and manual scan of those results for anomalous data of any kind to identify anomalous data was undertaken.

8. That search yielded 14 domains with no anomalous data (e.g.,trump-mail.com, trumpuniversity.com, and trumpsoho.com) and 1 that *did* contain anomalous data:

    mail1.trump-email.com (IP address 66.216.133.29)

    [Filename: Log-Of-DNS-Lookups-For-mail1.trump-email.com-851.txt]

9. trump-email.com, the "parent" domain for mail1.trump-email.com, is registered to the Trump organization, so mail1.trump-email.com is a Trump-controlled mail server. [*See* following WHOIS lookup and file referenced in #4]

GoDaddy™ All Products Domains Websites Hosting Web Secu

WHOIS search results for:
TRUMP-EMAIL.COM
(Registered)

Domain Name: TRUMP-EMAIL.COM
Registry Domain ID: 1565681481_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: http://www.godaddy.com
Update Date: 2016-06-29T14:27:44Z
Creation Date: 2009-08-14T20:06:37Z
Registrar Registration Expiration Date: 2017-07-01T03:59:59Z
Registrar: GoDaddy.com, LLC
Registrar IANA ID: 146
Registrar Abuse Contact Email: abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4806242505
Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited http://www.icann.org/epp#clientUpdateProhibited
Domain Status: clientRenewProhibited http://www.icann.org/epp#clientRenewProhibited
Domain Status: clientDeleteProhibited http://www.icann.org/epp#clientDeleteProhibited
Registry Registrant ID:
Registrant Name: Trump Orgainzation
Registrant Organization: Trump Orgainzation
Registrant Street: 725 Fifth Avenue
Registrant City: New York
Registrant State/Province: New York
Registrant Postal Code: 10022
Registrant Country: US
Registrant Phone: +1.2128322000
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: emcmullin@cendyn.com
Registry Admin ID:

10. Over the 90-day period from May 4 - Sept. 4, 2016, there were 19 external IP addresses (in yellow) from which *A record* searches originated for mail1.trump-email.com:

326 look-ups from 217.12.97.15 [Alfa Bank]
288 look-ups from 217.12.96.15 [Alfa Bank]
230 look-ups from 167.73.110.8 [Spectrum Health]
98 look-ups from 50.207.241.62 [Domo, Inc., Salt Lake City. VPN provider]
4 look-ups from 66.155.252.34 [malware on it]
4 look-ups from 63.118.233.31 [malware on it]
4 look-ups from 192.216.142.4 [malware on it]
3 look-ups from 63.118.233.30 [malware on it]
2 look-ups from 74.217.49.226 [malware on it]
2 look-ups from 69.74.121.66 [malware on it]
2 look-ups from 198.175.230.159 [malware on it]
2 look-ups from 198.175.230.158 [malware on it]
2 look-ups from 109.110.227.141 [malware on it]
2 look-ups from 69.30.221.250 [malware on it]
2 look-ups from 69.30.210.242 [malware on it]
1 look-up from 79.134.218.13 [Obit ISP, St. Petersburg, owned by Alfa Bank]
1 look-up from 69.30.198.202 [malware on it]
1 look-up from 203.12.160.3 [malware on it]
1 look-up from 204.101.0.66 [malware on it]

(These are the outside servers looking to send email to mail1.trump-email.)

11. A number of things about mail1.trump-email.com and the activity surrounding it stood out as being very unusual.

i. This is a *very* small number of source IP addresses: the number of IP addresses looking up the mail1.trump-email.com host name is minuscule—only 19 over ninety days. A normal mail server would have look-ups over a 90-day period coming from thousands to tens-of-thousands of different IP addresses.

ii. This is a *very* unusual distribution of source IP addresses: 4 IP addresses have significantly more lookups (97%) than the other 15 (3%). A normal distribution for mail look-ups would be fairly uniform in range, i.e., from each IP address would come a similar number of look-ups for any given domain name.[1]

iii. The majority of lookups for this *mail server* are for the A (regular) record by Alfa Bank and not the MX (mail record). This is significant because it shows a mail server set up to masquerade as a regular (non-mail) server. (An *A record* search

---

[1] mail1.trump-email.com is hosted by a Pennsylvania-based company, Listrak, which is a reasonably well known CRM (Customer Relationship Management) company that provides large-scale distribution of marketing emails (usually sending email messages to thousands of recipients hundreds of times a day). Most email systems receiving email from a CRM company would do an *A record* look-up of the connecting mail system (in this case, from mail1.trump-email.com) in order to verify its reputation, location, etc. before accepting the inbound connection. Hence the expected nearly equal distribution of IP address counts, and the expectation that there would be tens or hundreds of thousands of lookups.

is the appropriate look-up for another form of communication (such as a VPN or secure connection, a text connection, etc).)

- The top 2 IP addresses are the 2 main DNS servers belonging to Alfa Bank.
- Of the 975 total look-ups from the 19 IP addresses, 87% are from Alfa Bank or Spectrum Health (an Alfa Bank pass-through, discussed below).
- Add the suspicious look-ups from Domo, and 97% of the look-ups are suspect.

iv. mail1.trump-email.com is configured to only accept email from pre-determined and pre-approved IP addresses. When one tries to connect to mail1.trump-email.com (using telnet to port 25, the mail submission port), you get the response "lvpmta14.lstrk.net does not accept mail from you ([incoming IP address])." ["lvpmta" stands for "listrak virtual private mail transfer agent"]

This shows mail1.trump-email.com to be an active mail server (since there was a response from port 25) but one that highly restricts the sources from which it will accept email.

v. The Spectrum Health IP address is a TOR exit node used exclusively by Alfa Bank, i.e., Alfa Bank communications enter a Tor node somewhere in the world and those communications exit, presumably untraceable, at Spectrum Health. There is absolutely no reason why Spectrum would want a Tor exit node on its system.[2] (Indeed, Spectrum Health would not *want* a TOR node on its system because, by its nature, you never know what will come out of a TOR node, including child pornography and other illegal content.)

vi. The 4th most active IP address (after Alfa Bank and Spectrum Health) belongs to DOMO, a commercial cloud and VPN service provider located in Utah. VPNs to public VPN providers such as DOMO are often used to obfuscate the source of Internet traffic.

vii. The Alfa Bank name servers are not respecting the TTL for the mail1.trump-email.com hostname. The requires either modification of standard configuration (which takes skill and effort) or it indicates a manual loop-up. This is highly unusual because Alfa Bank is a large sophisticated global organization, i.e., this was not done in error. (Fingerprinting of the name severs at Alfa Bank indicate modern resolver code; all of the modern resolvers respect TTL.) [Filename: DNS-Lookups-For-mail1.trump-email.com-Through-9-14.txt]

---

[2] We discovered that Spectrum Health is the victim of a network intrusion. Therefore, Spectrum Health may not know what it has a TOR exit node on its network. Alternatively, the De Vos family may have people at Spectrum who know there is a TOR node, i.e., the TOR node could have been placed there with inside help.

12. An updated search on Sept. 14, 2016 of the prior 90 days (i.e., June 17-Sept 14) shows a total of 3,553 look-ups for mail1.trump-email.com from only 9 IP addresses:

- 2,817 look-ups from the two Alpha Bank IP addresses;
- 729 look-ups from the Spectrum Health Tor node; and
- 7 look-ups from miscellaneous sources (3 internal and 4 from malware).

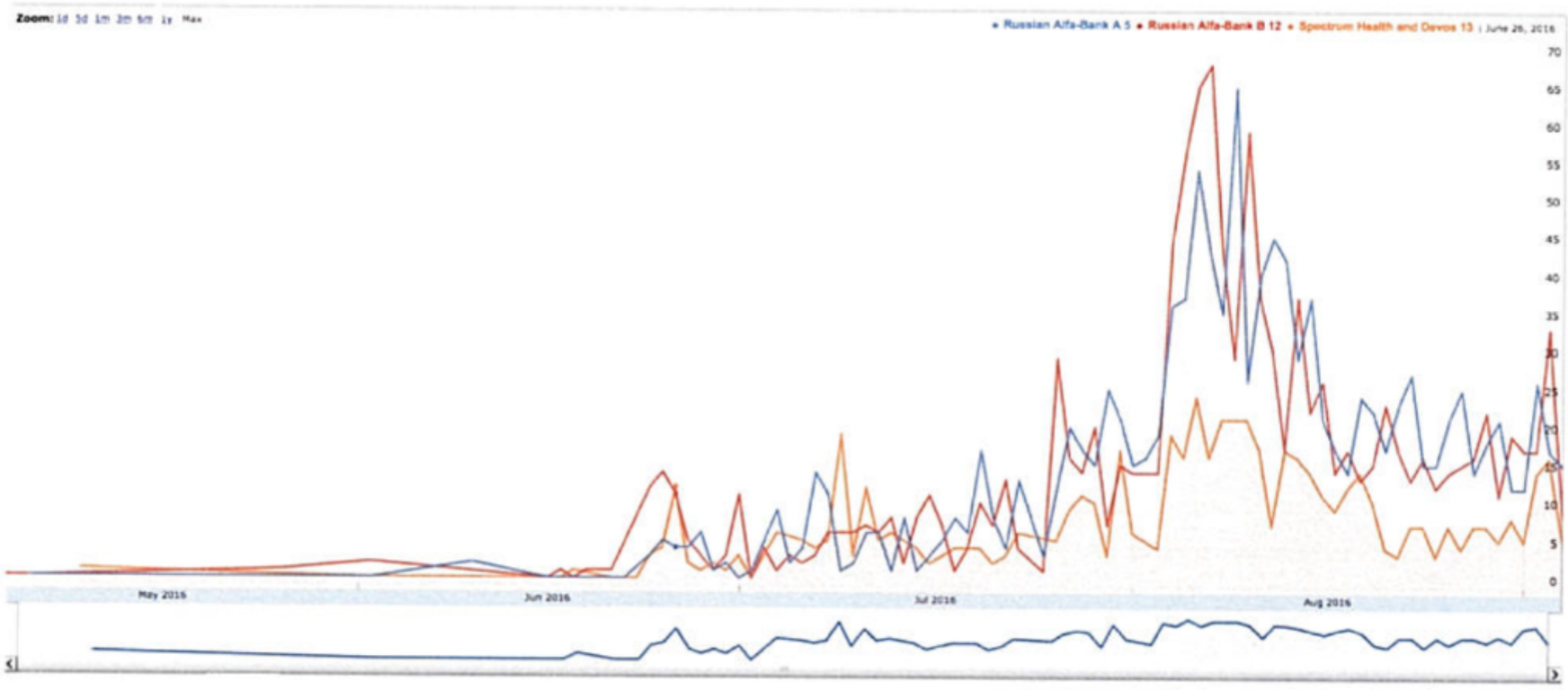
During this period, 99.8% of the look-ups for mail1.trump-email.com came from Alfa Bank or the Spectrum Tor node.

[Filename: DNS-Lookups-For-mail1.trump-email.com-Through-9-14.txt]

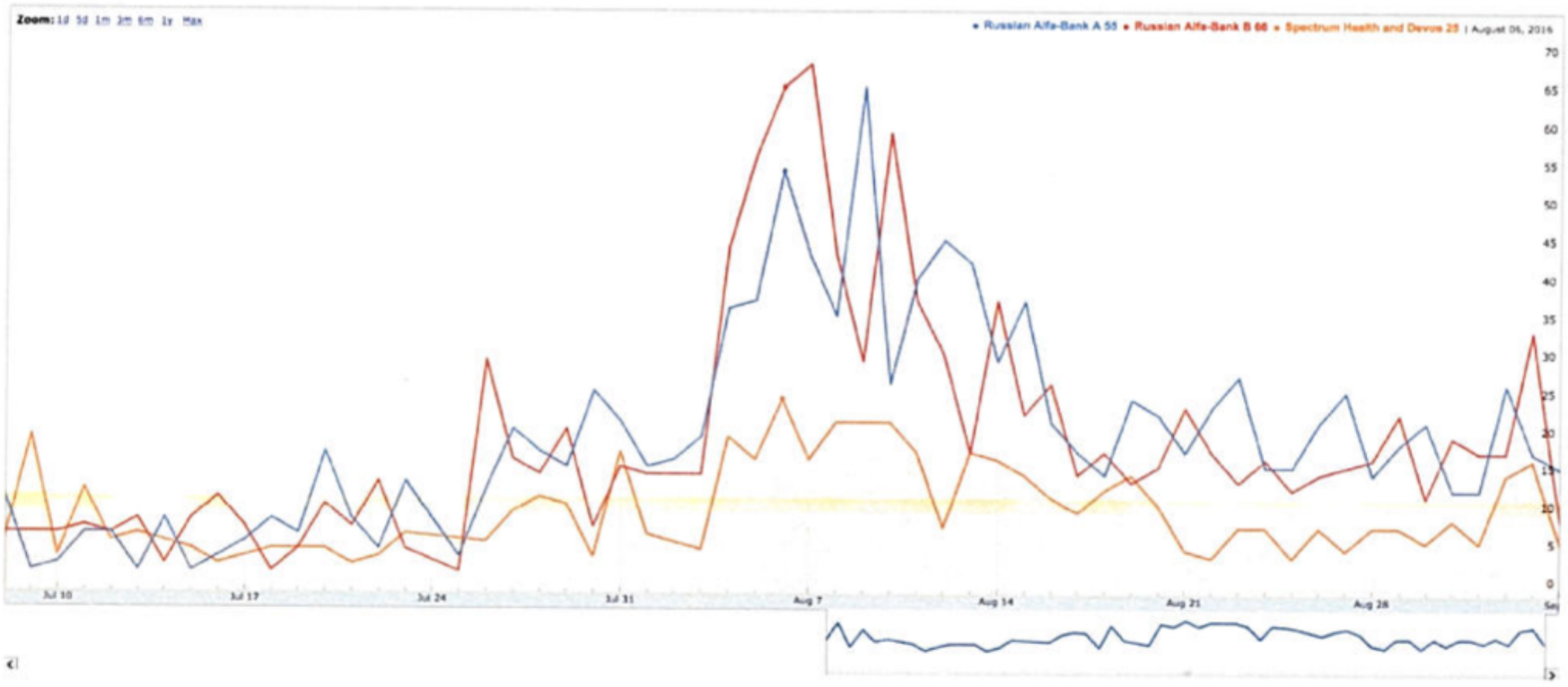
Conclusion:

While there may be *possible* explanations for the configurations of mail1.trump-email.com and the Spectrum Health TOR node, there is no *plausible* explanation other than that Alfa Bank and the Trump Organization are using multiple sophisticated layers of protection to obfuscate their communications.

This histograph shows the connections to mail1.trump-email from the two Alfa Bank IP addresses (326 and 288 connections) and the Spectrum Health IP address (230 connec-



tions) over time, and shows that the connections overlap over the same days.



This histograph shows the same information over an excerpted period of time.

Whitepaper Comments:
Time Series Analysis of Recursive Queries

September 19, 2016

1 Introduction

This document provides independent comments on a whitepaper entitled *White Paper #1 - Auditable V3* (hereinafter, "the whitepaper"). The whitepaper details various domains owned by the Trump Organization, and identifies patterns of DNS queries demonstrating network connections between a Trump owned domain, Spectrum Health (a medical service provider in Michigan), and Alfa Bank (a Russian bank).

This document attempts to use alternative data sources to verify the conclusions of the whitepaper. In relevant parts, this study agrees with the whitepaper's core findings: there is a significant interaction between a domain operated by a presidential candidate, and a Russian bank. The interactions appear to be related to email delivery, using a secured server, whose messages are evidently only accessible to Spectrum Health in Michigan, Alfa Bank, and a VPN provider in Utah.

This report also shows how others can verify these conclusions themselves, using various public data sources.

2 SPF Analysis

Public online passive DNS databases, such as the Chinese DNS informational site dnsdb.io [1], show several RRsets in the `trump-email.com` zone. In relevant part these include:

```
mail1.trump-email.com A 66.216.133.29

trump-email.com TXT |v=spf1 ip4:198.91.42.0/23 ip4:64.135.26.0/24
 ip4:64.95.241.0/24 ip4:206.191.130.0/24 ip4:63.251.151.0/24
 ip4:69.25.15.0/24 mx ~all
```

The last line is a Sender Policy Framework (or "SPF") record [4], and identifies domains and address ranges used in outbound email. While complex, the SPF record essentially lists the machines authorized to send outbound email on behalf of the `trump-email.com` domain. The listed IP address ranges have mail servers that send

emails, such as office correspondence. Using SPF, recipient mail servers can verify and discard fake messages (e.g., spam from 3d party networks claiming to come from `trump-email.com`). If the sending host claims to come from `trump-email.com`, but is not inside one of the listed SPF ranges, the message delivery may "soft fail", under the SPF protocol.

Significantly, the SPF CIDR ranges ***do not*** encompass `66.216.133.29`, the address for `mail1.trump-email.com` (hereinafter the "`mail1` host"). Thus, it is unlikely that `mail1` is used for sending messages on behalf of the parent zone, `trump-email.com`, since many recipients might discard them, or score them as likely spam [1]. Instead, if the `mail1.trump-email.com` host sends mail, it likely is on behalf of the child zone `mail1`. (As noted below, the host may instead be a outbound server or forwarder.)

In effect, `mail1` is a "punch out" domain in the larger Trump zone. It has its own mail policy, separate from the parent zone which appears designed for more robust, scaled messaging. While emails do originate through `trump-email.com`, and the six listed IP address ranges, the host `mail1.trump-email.com` has its own sending policy.

These DNS records can be found in most any passive DNS data source, and there are no contrary records in any online passive DNS database, from 2010 forward. And a current DNS lookup for these records yields the same results.

3 mail1 Host Operation

One can determine the purpose of `mail1.trump-email.com` by contacting the mailserver directly, and checking if it operates an SMTP server. Novice users can even check using several online mail services themselves. For example, Pingability [6] lets one interact with the mail server through a web interface:

```
DEBUG: getProvider() returning
 javax.mail.Provider[TRANSPORT,smtp,
 com.sun.mail.smtp.SMTPTransport,Oracle]
DEBUG SMTP: useEhlo true, useAuth false
DEBUG SMTP: trying to connect to host
 "mail1.trump-email.com", port 25, is SSL false
521 lvpmta14.lstrk.net does not accept
  mail from you (72.249.37.67)
DEBUG SMTP: could not connect to host
  "mail1.trump-email.com", port: 25, response: 521
```

[1] In more detail: While there is a "soft fail" flag in the SPF record, there is no wildcard SPF record at the zone apex. Thus the child zone `mail1.trump-email.com` would need its own SPF record to facilitate delivery, and its address must be included in an appropriate ip4 stanza. Despite not having a covering SPF record, the host `mail1.trump-email.com` could still send small-scale direct messages, on behalf of `mail1.trump-email.com` (but not the parent zone), if recipients whitelist it or are configured to specifically accept the mail.. But the `mail1` domain would prove problematic for mass mailings such as newsletters, hotel customer contact, vendor communications, and such.

The line starting with "521" is from the Trump server, and lines starting with "DEBUG" are generated by the Pingability testing service. Other online services may show slightly different output, but the message from the `mail1` host is always the same. The 521 reply code means the host is refusing to accept incoming email, per RFC 1846 and subsequent revisions [2].

In detail, the response indicates the Trump host refused mail, identifying itself as a "Listrack" virtual mail transfer agent (or "lvpmta"). The host is likely configured as an "outbound server", where users of in the Trump organization send emails, while using another email server to receive messages. The Listrak service is powered by "Port25 powerMTA", a commercial vendor of high quality SMTP software, which offers an "access control list" (ACL) capability. This permits the `mail1` host to filter based on user IP. In this case, it appears the Trump host is private, and was configured to only permit connections from specific hosts.

4 Query Rates

The whitepaper provides query logs for the `mail1` DNS record, in an ancillary file called "Log-Of-DNS-Lookups-For-mail1.trump-email.com-851.txt". The data is plotted in the whitepaper, which appears to show similar query frequencies originating from Alfa Bank and Spectrum Health networks. We note that, using old, well-known cache inspection techniques [3], it might be possible for users to iteratively query for such data themselves, to construct a similar pattern of usage. This would be time consuming, and was not attempted.

So using just the log files in the whitepaper, we consider whether the DNS lookups were for email delivery. This appears to be the case, because of these established facts:

- The host `mail1.trump-email.com` has two domain labels often associated with SMTP operation.
- The `mail1` host is colocated in a commercial network often used for managed email handling.
- The `mail1` host listens on port 25, and responds with an error message found only in Listrak mail servers.

The lack of MX lookups may be associated with the configuration of the Listrak host (e.g., being used for secure relay to a specific host, using a `relay-domain` option in the Port25 software), though this is not certain.

Because the log file has time stamps with precision down to the second, it is possible spot patterns of DNS lookups from Alfa Bank and Spectrum networks. Significantly, we note that there are very few source networks resolving the `mail1` host: just Alfa Bank, Spectrum Health, and (at a distant third) the VPN provider in Utah. The whitepaper analysis rightly dismisses the handful of other DNS lookups as noise, e.g., originating from infected hosts that just do a single lookup, and never interact further. A check of various online DNSBL sources [5] confirms this diagnosis.

We can therefore look for patterns among the three major resolver networks (Alfa, Spectrum and the VPN), and create a time series analysis. Consider:

1. If these DNS lookups are human-driven email message delivery attempts, one would see a pattern often associated with normal email threads: quick replies in some cases, and slight delays in some replies.

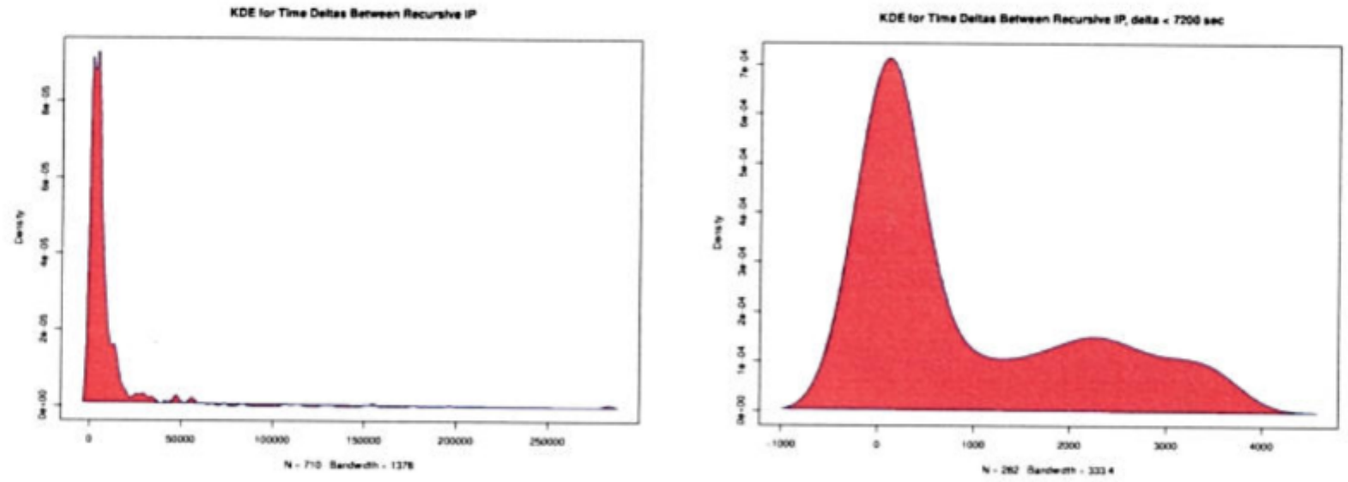
2. If these DNS lookups are instead associated with malware or some infection vector, one would expect to see a more automated lookup pattern. (Indeed, one would likely see the resolution of a 3d party command-and-control domain, instead of just a Michigan hospital and a Russian bank.) The lookup volume and paucity of qname diversity likely rules out this theory.

3. If these DNS lookups were associated with bulk email delivery newsletters, or customer contact, one would expect to see a more distributed period of lookups, with an exponential rate. (That is, regular high volume resolutions, followed by low volume periods.) As noted above, the SPF records significantly complicate the use of `mail1` for anything like this. But we can investigate this alternative theory.

We first calculate the inter-arrival time between DNS lookups from the Spectrum and Alfa Bank resolvers using a simple time series analysis. Using a stateful window, we note which network resolved the `mail1` host last, and at what time. When a different network (AlfaBank, Spectrum, or the Utah VPN) resolves the `mail1` host, we note the length of time, δ, between the recursive change, and update the state window. Informally, this measures the speed or pace of any message exchanges, or the "tick-tock" of humans sending messages back and forth. That is, when both Alfa Bank and Spectrum's recursives no longer have `mail1` in local cache, we can measure the speed of the "reply" to the first message putting `mail1` back in cache on the other network. Since the data spans a lengthy period, and the `mail1` TTL cache period is short, we have many such observations.

In traditional network analysis, spam, viruses or scheduled bulk newsletter deliveries exhibit less "back-and-forth", where a sending network is contacted by the recipient. Indeed users seldom reply to spam, viruses or even newsletters. And if both Spectrum and Afla Bank were automating their lookups, then the time delta distribution would peak around the greatest common divisor for both lookup periods, and with minimal heteroscedasticity (informally, with little dispersion or "flatness"), due only to nework lag.

After processing the time stamps in the log file, we plot the inter-arrival of queries from different recursives. Figure 1(a) and (b) show the kernel density estimate (KDE) for the distribution of these time deltas. We use a KDE instead of a traditional bin distribution plot, because the latter easily skew results based on bin size. Here, the optimal bin size is calculated algorithmically, with the smoothing parameter, h, reported as "bandwidth" in the plot. Figure 1(a) shows a wide distribution of times, suggesting these are unlikely to be "cron'd" or automated lookups. Figure 1(b) zooms in on the distribution (where $\delta < 7200$ seconds), showing the distribution of paired DNS lookups just seconds and minutes apart. (I.e., short episodes, when another network put `mail1` back in cache, perhaps in reply to a message.) In other words, there are many instances where the conversations are active, rapid-fire, and other instances where the cache refresh changes appear to take hours.



(a) (b)

Figure 1: Distribution of inter-arrival of networks querying `mail1` host. (a) KDE of time between all changes in source networks. (b) Distribution of short-period changes, $\delta < 7200$ seconds.

These results are consistent with human-driven email interactions with the `mail1` domain. As noted, if this were instead automated, or driven by an infectious or spamming process, the rate, volume and frequencies would be more periodic for the former, or random for the latter.

One can further constrast this result for `mail1` with the volumetric network graphs for the domain `trump-mail.com`. **Nota Bene:** here, we refer to `trump-mail.com`, not `trump-`**`e`**`mail.com`. We note that the `trump-mail.com` domain has distinct whois data, and even may have separate owners. The `trump-mail.com` domain is hosted in a colocation facility often abused by spammers. In contrast, the `mail1.trump-`**`e`**`mail.com` domain (note the 'e' in email) has the correct contact information for the Trump Organization, and is hosted in a facility commonly used for legitimate enterprise mail handling.

Since the MikroTik router on `trump-mail.com` is public facing, anyone can look at the volume of traffic on the two interfaces. Figure 2 shows the network graphs for `trump-mail.com` external interface, available from its public web page. It shows a periodic spike for inbound traffic (green peaks), with no spikes on the weekends. Further, the spikes always occur at the same hour, every weekday. This is classically found in automated network use, such as backups, newsletter delivery, and the like. This automated, periodic pattern provides a useful contrast for the human-driven `mail1` trump server interactions.

5 Conclusions

This paper verified some statements in a whitepaper describing DNS interactions with `mail1.trump-email.com`, offering other sources of data were possible. This

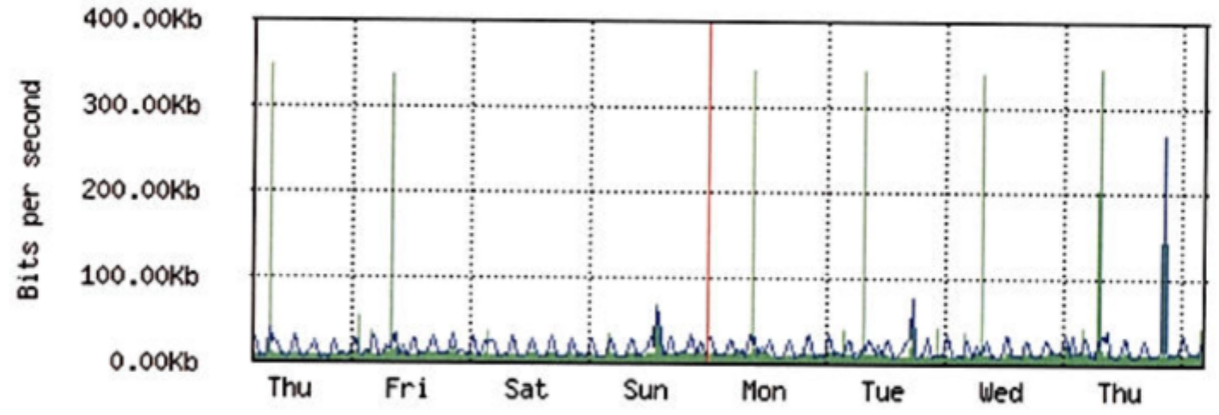


Figure 2: Periodic network traffic on `trump-mail.com`, consistent with bulk receiving and cron backup. Green lines indicates inbound, and blue represent outbound traffic.

analysis concludes:

- The domain `mail1.trump-email.com` has a distinct mail policy from the parent zone `trump-email.com`. It is unlikely the `mail1` could effectively send mail on behalf of `trump-email.com`, without delivery complications.
- The `mail1` host operates its own SMTP, a Listrak server. The server appears configured for secure communications or forwarding. It clearly permits connections only from a set of authorized hosts.
- Resolvers in Alfa Bank, Spectrum Health, and a Utah-based VPN provider are the only hosts resolving `mail1.trump-email.com`. A few other hosts around the Internet resolving `mail1` are low in volume (e.g., once in a month period), or exhibit infectious behaviors, and are not relevant. On the whole, only Alfa Bank (in Russia), Spectrum Health (in Michigan) and a VPN provider in Utah interact with or consume messages from the specialized Trump mail server, in any volume.
- There are many DNS lookups for `mail1` from these networks, and the timing pattern is consistent with human driven email resolutions. The resolution patterns are not consistent with automation, backups, or infectious behavior.
- Alfa Bank, Spectrum Health, and Trump's networks interact with each other regularly, evidently sending email to a secured server, `mail1.trump-email.com`.

This analysis has not addressed a few statements in the whitepaper, not considered material to the overall analysis. These include:

- The nature of the host in the Spectrum Health network and whether it was operated as a Tor exit node. The status as a Tor exit node can be verified by other sources (e.g., the Tor project), but did not appear dispositive on the core question of a messaging nexus between key networks.

- The whitepaper commented on Alfa Bank's recursive resolvers, which did not appear to "respect caching behavior". While this observation is clearly supported by the data, we speculate the explanation is quite mundane. Likely, Afla runs a caching farm, which does not share cache results among individual resolvers. (This type of resolver configuration is efficient and inexpensive, and common in enterprises the size of Alfa Bank.) While more analysis could prove this, or even estimate the number of independent cache lines behind the Alfa Bank egress IP, this did not appear material to the core question in the white paper.

- We have not reviewed the accuracy of the other data files, which generally just provide lists of domain names with "trump" substrings, or show registration information. Given that one can use public DNS sources to find the anomalous SPF records around `mail1.trump-email.com`, these steps were not necessary. If needed anyone can trivially query for the listed domains or use public passive DNS databases to verify the reported RRsets.

- We do not comment on any associated materials or analysis about Spectrum, their interest in Trump or Russian banks, Alfa Bank or its organization or operation, or its connection (beyond frequent messaging) with Trump owned networks. Other experts may look at the timing of the query volumes, in relation to other exogenous events associated within these organizations, e.g., investments of funding activities, [7]. Such details are beyond the narrow technical focus of this whitepaper.

References

[1] QQ Group 437080096. Dnsdb. https://dnsdb.io/en/search?q=trump-email.com, 2016.

[2] A. Durand and F. Dupont. Smtp 521 reply code. https://www.ietf.org/rfc/rfc1846.txt, September 1995.

[3] Luis Grangeia. Dns cache snooping or snooping the cache for fun and profit. http://cs.unc.edu/~fabian/course_papers/cache_snooping.pdf, February 2004.

[4] M. Kucherawy. Email authentication status codes. https://tools.ietf.org/html/rfc7372, September 2014.

[5] The Spamhaus Project Block List. SBL - spamhaus DNSBLs. http://www.spamhaus.org/sbl/, 2004.

[6] Pingability. Web check and alert service. https://pingability.com/smtptest.jsp, 2016.

[7] Irina Reznik. Russian oil billionaires' next big investment - american health care. http://www.bloomberg.com/news/articles/2016-07-14/russian-billionaires-plan-u-s-health-push-with-d-c-insiders, july 2016.

Russia's Alfa Group

Overview

Alfa Group is a $20-billion Russian conglomerate involved in banking and energy that maintains extremely close ties to the Kremlin, and President **Vladimir Putin**. Alfa operates in the US with more success and sophistication than any other Russian business group. The Alfa Group shareholders also control an international energy and telecommunications empire through Luxembourg-registered **LetterOne Holdings**.

Mikhail Fridman, a Ukrainian by birth, founded the group as a commodities trader in 1989. He soon recruited former government minister **Pyotr Aven** to develop Alfa Bank. With Russian partners, Alfa Group established control over Siberian oil company TNK, which they merged with BP's Russian assets. Alfa's shareholders gained more than US$9 billion when the company was sold at the top of the market in 2013. Much of these funds were re-invested internationally through LetterOne.

Fridman and Aven are legendary for their aggressive tactics, which include espionage and harassment of adversaries. Alfa Group is perhaps most notorious for an alleged campaign of intimidation, harassment and espionage against BP in an effort to pressure the British oil giant to sell its Russian oil interests. The "orchestrated campaign of harassment," which allegedly included Alfa-instigated police raids and spying, famously resulted in the 2008 departure of **BP executive Robert Dudley**, an American citizen, from Moscow.[1] Dudley is today BP's CEO.

According to a US court ruling in 2005, the two men "have been dogged by allegations of corruption and illegal conduct. Russian newspapers have published repeated claims that Aven and Fridman have rigged the auction of state assets through government connections, threatened the lives of government officials, ordered the assassination of a mobster, and engaged in narcotics trafficking and money laundering."[2] Despite the allegations, the men have avoided visa bans and other sanctions imposed on oligarchs with similarly colorful pasts, such as **Oleg Deripaska**.

As Minister of Foreign Economic Relations, Aven worked with Russian President Vladmir Putin in the government of St. Petersburg in the early 1990s and is credibly accused of involvement in some of Putin's earliest corruption schemes. Not least, Aven ignored corruption accusations leveled against Putin for false registration of licenses in his role as the head of the city's Committee for Foreign Economic Liaison[3]. Critics allege this is suggestive of collusion between Aven and Putin, and point to Alfa's subsequent charmed fortunes in Moscow -- including successful campaigns against two of Putin's closest Kremlin allies with no retaliation whatsoever.

---

[1] https://www.theguardian.com/business/2008/jul/25/bp.oil
[2] https://www.gpo.gov/fdsys/pkg/USCOURTS-dcd-1_00-cv-02208/pdf/USCOURTS-dcd-1_00-cv-02208-0.pdf
[3] "Putin's Kleptocracy: Who Owns Russia," Karen Dawisha, accessed electronically.

Alfa enjoys high-level contacts in Washington, keeps influential figures on retainer, funds American political campaigns through its US network, and has sponsored numerous individuals who now serve in government and the media. Alfa is a particularly skilled practitioner of deep lobbying through numerous influential US think tanks and several "fellowship" programs that build loyalty among policymakers.

Aven sits on the board of directors of **Moscow's New Economic School**, Russia's only privately-funded university, which Alfa funds generously. **Carter Page**, a foreign policy adviser to Republican presidential nominee **Donald Trump**, addressed the school's graduating ceremony on July 8, 2016 – a trip criticized by Senate minority leader Harry Reid, among others. His speech was supportive of Putin and harshly critical of the U.S. and President Barack Obama. Obama addressed the school's graduating class in 2009.

US Influence

Alfa's leading American political adviser is former diplomat **Richard Burt**, who has confirmed that he contributed material to an April 27 foreign-policy speech by Donald Trump but denies acting as a Trump campaign advisor.[4] Burt, a former U.S. ambassador to Germany, works for **McLarty Associates**.

Alfa's other major advisor in Washington for many years was the Republican lobbyist **Ed Rogers** of BGR. Lobbying records show that Alfa quietly terminated BGR in the spring of 2015 as Trump was launching his presidential campaign. Rogers is a frequent critic of Trump.

White House records show that Fridman and Aven made multiple visits to the White House complex in 2009-2012, meeting privately with top US national security and foreign policy officials. The meetings, which were arranged by Rogers and Burt, ended as relations between the Obama administration and the Putin regime soured. Sources have indicated that Fridman and Aven were tasked by the Kremlin with negotiating Russia's accession to the WTO with the White House – a strong indication of Putin's trust in the executives as government proxies.

In an effort to avoid economic sanctions and a poor domestic investment climate, Fridman and Aven in 2014-15 moved tens of billions of dollars of capital to Europe into a fund called **LetterOne Holdings SA**, based in Luxembourg. The fund nonetheless became entangled in controversy in 2015 over its acquisition of oil blocks in the North Sea -- which the UK threatened to force the group to divest. It is believed among Russia watchers that Fridman and Aven are almost as eager as the Kremlin to get US and EU sanctions on Russia lifted.

Alfa has long sought to buy more major assets in the US, and is believed to have made a sustained but ultimately unsuccessful attempt to buy a US financial institution during the early years of the Obama administration. It is likely the bid was blocked by US regulatory

---

[4] http://www.reuters.com/article/us-usa-election-trump-adviser-idUSKCN0YU2I9

concerns. In June of 2016, LetterOne announced it would invest $2-3 billion in the US health care industry.[5]

Alfa Group Background

Fridman founded commodity trader Alfa Eko – the core of the future Alfa Group – in 1989 with two university friends, **German Khan** and **Alexey Kuzmichev**. In 1991, they launched Alfa Capital and Alfa Bank. Former government minister Peter Aven joined the group in 1993. The identity of the group's beneficial shareholders in the early years remains a mystery.[6]

Aven brought crucial and lasting government ties to the group, as did the recruitment of **Leonid Vid**, the former head of Gosplan, the Soviet planning agency, and he helmed Alfa Bank during its critical early years of growth. Another key hire was **Vladislav Surkov**, a former military intelligence officer who later served President Putin as his chief spin-doctor in a series of senior positions (today he is an advisor)[7]. Fridman himself became a key political figure during the 1996 re-election campaign of President **Boris Yeltsin**, when he was one of architects of the media blitz that helped defeat the surging communists.

In the late 1990s, Alfa Group recruited a number of Western-trained executives, many with Russian backgrounds. These included such figures as bankers **Alex Knaster and Mikhail Alexandrov**, the latter a former Credit Suisse banker who had advised the Russian government on privatization. Alfa Bank in particular became known for hiring top Western talent. These moves were spun as signs of an overall 'Western' approach to business.

At the same time, Alfa Group employed a range of tactics that earned it a reputation as one of Russia's must successful 'raiders'. In a common tactic, Alfa would acquire a minority shareholding in companies it knew or suspected to be acquisition targets by foreign or domestic groups, and carried out more or less classic greenmail.

It also made frequent use of Russia's flawed bankruptcy laws, acquiring debt in an enterprise or one of its subsidiaries then using local courts to obtain default and bankruptcy judgments. Most famously, these tactics were used at oil-production subsidiary **Chernogorneft** to gain a blocking stake in oil company **Sidanco** in the late 1990s[8].

Alfa Group also faced much graver allegations regarding its conduct in this era. **The Center for Public Integrity (CPI)** published an article in 2000 repeating claims made in 1999 in Russian newspapers, as well as allegations made by a senior Russian parliamentarian, and backed by additional sources. The CPI article claimed Fridman and Aven were involved in drug trafficking, money laundering and association with organized crime. Fridman and Aven filed a defamation suit in 2005, which nearly bankrupted the group but was eventually tossed

---

[5] http://www.letterone.com/our-businesses/l1-health
[6] http://www.ft.com/cms/s/0/b47de3d4-c325-11e4-ac3d-00144feab7de.html#axzz4IwVVcBT6
[7] https://lenta.ru/lib/14159273/full.htm
[8] http://www.nytimes.com/1999/08/13/business/russia-with-bankruptcy-high-cost-for-bp-amoco-s-investment-oil-concern.html?pagewanted=all

out on the grounds they were public figures[9]. Separately, Alfa was also condemned by the United Nations for violating sanctions in the Iraq oil-for-food program[10].

Entering the Putin era, Alfa Group was firmly established as one of the country's most powerful business groups and would only grow more powerful under the new president. Spin-doctor Surkov became the president's new deputy chief of staff, launching the regime's youth group and other ideological projects[11]. And Aven, who has had a relationship with Putin going back to at least 1992, solidified his position as one of his closest advisors. In addition, Fridman became a member of the Public Chamber, a high profile if cosmetic project close to the president's heart.

During the 2000s, Alfa Group would demonstrate the strength of its political ties by taking on close associates of Vladimir Putin and consistently winning. The first example was the defeat of long-time Putin associate and then telecommunications minister, **Leonid Reiman**, in a fight for control over Megafon, one of Russia's top cellular carriers[12]. Notably, Alfa launched this fight and prevailed in the aftermath of the collapse of Yukos and exiling of its shareholders.

Alfa Group achieved its greatest success in a battle with **Igor Sechin**, the head of state oil giant Rosneft and a member of Putin's circle. This fight emerged from Alfa's war with joint venture partner BP, first in 2008 and later in 2011, for strategic control over their TNK-BP joint venture. Alfa's strong arm tactics, including the bugging of the office of Robert Dudley, then head of the Russian venture and now BP CEO, did not bring any recriminations from the Kremlin[13].

In 2011, Alfa initiated fresh hostilities to force BP to meet its demands and push Rosneft to buy it out on the most favorable terms possible. The group had installed US-trained oil executive **Stan Polovets** as the head of the Alfa-BP joint venture and he led a brutal PR campaign against BP[14]. Simultaneously, Alfa sponsored third party lawsuits in obscure Siberian courts seeking billions of dollars in damages to tie up BP and Rosneft for months to improve their negotiating position[15].

Alfa Group used these trademark tactics in a series of other conflicts with foreign business partners, including Norway's Telenor and Turkey's Cukurova. They also took on powerful Russian business figures, including billionaire oligarch **Alisher Usmanov** over Megafon and billionaire oligarch **Yevgeny Yevtushenkov's** MTS over a Kyrgyz operator, Bitel. These

---

[9] https://www.gpo.gov/fdsys/pkg/USCOURTS-dcd-1_00-cv-02208/pdf/USCOURTS-dcd-1_00-cv-02208-0.pdf

[10] http://www.foxnews.com/projects/pdf/final_off_report.pdf

[11] http://www.theatlantic.com/international/archive/2014/11/hidden-author-putinism-russia-vladislav-surkov/382489/

[12] http://www.wsj.com/articles/SB112856247619561303

[13] http://www.telegraph.co.uk/finance/newsbysector/energy/8286767/TNK-BP-Bob-Dudley-and-the-billionaire-Russian-partners.html

[14] http://www.reuters.com/article/bp-rosneft-aar-idUSLDE70R0WT20110128

[15] http://www.nytimes.com/2011/11/12/business/global/bp-wins-legal-victory-for-its-russian-joint-venture.html?_r=0

moves indicate Alfa has serious clout: Both Usmanov and Yevtushenkov are classified as suspected organized crime figures by Western law enforcement agencies.

In almost every dispute, the Alfa group has prevailed and the Russian authorities have remained silent. The recruitment of prominent Western figures, such as Vodafone founder **Sir Julian Horn-Smith** and former UK foreign secretary **Lord Douglas Hurd** for Dutch telecommunications holding Altimo in 2006, have provided the crucial appearance of respectability for Western audiences and regulators[16].

The well-timed sale of TNK-BP to Rosneft in 2013 netted Alfa Group more than US$9 billion. It appears the shareholders invested much of these funds into LetterOne, reportedly owned by Fridman and Khan[17], where former **BP boss Lord Browne** was made executive chairman of energy projects[18]. Even ahead of sanctions in 2014, the group put out a clear message that it was focusing on investments abroad[19].

In fact, the group was acting in line with a new policy of the Putin regime to encourage Kremlin-friendly Russian conglomerates invest abroad in a variety of sectors, including energy and telecommunications. This strengthens Russia's ability to exert soft power influence in Europe and the Middle East, the two key regions to date for Alfa Group internationally. Fridman claims to spend most of his time abroad, but this claim may be more to ease concerns of European regulators (such as the UK's effort to force Fridman to sell North Sea oil fields in 2015)[20].

Today, Alfa Group and LetterOne appear to have deliberately distanced themselves from each other in terms of branding and promotion, despite their underlying common shareholding structures.

As the face of Alfa Bank, Peter Aven remains the group's key interface with the Kremlin. It appears his importance has only grown. Alfa Group, and specifically Alfa Bank, have a long-standing presence in the US and the UK. Aven has the ability to be a back channel to government actors as he and Fridman were representing the Kremlin in WTO accession negotiations in 2010-2012. And Alfa has long invested in lobbying in the US, an investment that is paying dividends during the current US elections.

Alfa Group continues to consist of several shareholders, but Fridman and Aven are the key players in both business and political terms. They are among the richest men in Russia. Fridman was ranked the second richest man in Russia in 2016, with a fortune of US$13.3

---

[16] http://www.ft.com/cms/s/0/512fda9c-46b2-11db-ac52-0000779e2340.html#axzz4IwVVcBT6

[17] http://www.bloomberg.com/news/articles/2015-10-14/eon-to-sell-norwegian-oil-and-gas-assets-to-dea-for-1-6-billion

[18] http://www.institutionalinvestor.com/article/3450336/banking-and-capital-markets-emerging-markets/alfas-mikhail-fridman-skirts-russian-sanctions-to-invest-abroad.html#/.V8c5WmVlt3I

[19] http://www.institutionalinvestor.com/article/3450336/banking-and-capital-markets-emerging-markets/alfas-mikhail-fridman-skirts-russian-sanctions-to-invest-abroad.html#/.V8c5WmVlt3I

[20] http://www.ft.com/cms/s/0/e258a2b0-e76c-11e4-a01c-00144feab7de.html#axzz4IwVVcBT6

billion, narrowly behind gas tycoon **Leonid Mikhelson**[21]. Aven is ranked 19th in Russia with a fortune of US$5.1 billion[22].

Fridman and Aven are among the last surviving oligarchs who emerged in the 1990s, alongside such Kremlin allies as Oleg Deripaska, Vladimir Potanin and Mikhail Prokhorov. While the latter three oligarch have at times in recent years been forced by the Kremlin to publicly play the role of vassal, the Alfa tycoons are far more powerful, and are among the rare businessmen who do not require an intermediary to deal with President Putin.

Having exited the Russian oil sector, they also do not have any common interests or conflicts with the so-called Petersburg clan around the president, consisting of such KGB-linked figures as the **Kovalchuk brothers and Gennady Timchenko**. Similarly, they do not have dealings with rougher types such as **Suleiman Kerimov or Zivyadun Magomedov**, who have prospered from links to the prime minister and members of his cabinet. This lack of domestic conflicts, enormous financial resources and powerful Kremlin support put them in a unique position.

Mikhail Fridman Background

Mikhail Fridman was born on April 21, 1964 in Lviv, Ukraine. He attended the Moscow Institute of Steel and Alloys, where he met two of his future business partners, Gref and Kuzmichev. In the late 1980s, according to various accounts, Fridman launched cooperative businesses to deliver packages and wash windows[23]. In later interviews, Fridman would emphasize that he was an outsider in Moscow, in particular because he was Jewish[24].

The rapid growth of Alfa Group in the early 1990s was made possible by Fridman's ability to recruit politically connected figures, such as Aven, and later recruit Western-trained managers. By the mid-1990s, however, Fridman was not in a position to compete with many of the leading oligarchs of the time, who parlayed political connections and capital to engineer the infamous 'loans for shares' deals that essentially privatized giant industrial and natural resources assets for a few pennies on the dollar.

The fact that Fridman missed this opportunity meant Alfa would have to fight incumbent owners, such as Vladimir Potanin, for energy and natural resource assets. It appears this strategy, born of necessity, would become Fridman's trademark in all of his dealings.

Fridman emerged politically in 1995, when he joined other major oligarchs in a project to ensure the re-election of President Boris Yeltsin. The president was in ill health and losing badly in polls to a resurgent Communist Party. His role in this successful effort also earned him a seat on the board of Russia's largest television network, ORT (now called Channel

---

[21] http://www.forbes.com/profile/mikhail-fridman/
[22] http://www.forbes.com/profile/pyotr-aven/
[23] http://www.ft.com/cms/s/0/b47de3d4-c325-11e4-ac3d-00144feab7de.html#axzz4IwVVcBT6
[24] See 'Sale of the Century' (2000) by former Financial Times Moscow Correspondent Chrystia Freeland

One), alongside Vladislav Surkov. Notably, the state-owned station was under the *de facto* control of tycoon Boris Berezovsky at the time.

After Putin came to power, Fridman was positioned in the Russian media as a liberal figure. It is claimed that Fridman's picture was even carried by anti-regime protestors in 2007, underlining his ambiguous public position. Yet it was precisely at this time that Fridman was spearheading some of Alfa Group's harshest shareholder disputes and taking advantage of political cover from the Kremlin.

In terms of outright criminality, as outlined above, the Center for Public Integrity article accused Fridman of participating in crimes ranging from trafficking in narcotics to association with organized crime. Russian investigative journalist Oleg Lurie had also published these claims, although he was forced to retract them.

Civil Liberties Fund, a group linked to Berezovsky, accused Fridman of masterminding the brutal murder of Ukrainian journalist Grigory Gongadze[25]. A Moscow newspaper was successfully sued for libel in 2004, when it linked Fridman to the murder of Paul Klebnikov, a US citizen writing for the Russian edition of Forbes[26]. Both crimes remain unsolved.

It is likely impossible to ever uncover the truth regarding the early activities of Fridman and Alfa Eko and most observers credit him with appearing to have relatively clean hands in terms of physical violence. However, it is clear that Fridman has been the mastermind of Alfa Group's combative style of doing business. He has also been willing to pay top dollar to recruit respected businesspeople and politicians to the boards of his companies to buy respectability and leverage Western institutions for his own ends.

It has been important for Alfa Group for Fridman to appear to be the one in charge and mastermind of its projects. However, most political observers view Aven as the one with the critical political relationship with President Putin going back to the early 1990s. As Aven leads Alfa Bank, the "clean" asset in the group, he has not been publicly involved in Alfa's contentious deals. In this view, it is important Fridman appear to be the colorful figure and dealmaker.

Peter Aven Background

Peter (Pyotr) Aven was born on March 16, 1955 in Moscow to a relatively prominent family. His father, Oleg Aven, was a leading Russian mathematician who died in 1992. His father was a department head at the Institute of Problems of Management of the Academy of Sciences of the USSR. His paternal grandfather, Ivan Aven, served in the famous Latvian Rifle Division, which played a crucial role in the 1917 revolution.

Aven completed his studies at the Moscow School of Physics and Mathematics 2, one of the most prestigious schools in the USSR. He trained as an academic Economist and gained a

---

[25] http://www.rferl.org/content/article/1070338.html
[26] http://spitfirelist.com/news/alfa-bank-wins-libel-case-over-klebnikov-murder-claims/

PhD in Econometrics from Moscow State University. His faculty adviser was Stanislav Shatalin, who later became an economic advisor to Soviet leader Mikhail Gorbachev and Russian President, Boris Yeltsin.

As a young economist in this era, Aven quickly developed ties with emerging reform figures. He was reportedly close to Yegor Gaidar, a former university classmate and Russia's first post-Soviet prime minister. In turn, Gaidar introduced Aven to Anatoly Chubais, the head of an informal 'club' of economists based in Leningrad in 1985 that included such figures as Alfred Kokh (future head of the State Property Committee) and Alexei Kudrin (finance minister and presidential advisor)

In 1989, Aven was appointed Economic advisor in the Ministry of Foreign Affairs of the USSR. From 1991 to 1992, he was the Minister for Foreign Economic Liaison of the last Soviet and Russian government. In this role, he appointed Vladimir Putin, at that time head of the Committee of Foreign Economic Relations of St Petersburg, the ministry's "representative in St Petersburg". This allowed Putin the autonomy to register independently new joint ventures to conduct foreign trade – in essence delegating the ministry's functions to Putin on an exceptional basis. As Karen Dawisha has chronicled, Aven intervened more than once to support Putin when he came into conflict with other government bodies[27].

During his short tenure in government, Aven's deputy was Mikhail Fradkov. In 2004, Fradkov replaced Mikhail Kasyanov as Russian prime minister, a position he held until September 2007. Fradkov is currently head of the powerful Foreign Intelligence Service (SVR) and is today believed to be a key Alfa Group ally in senior Russian government circles.

After leaving government in 1992, Aven briefly went to work for early post-Soviet oligarch Boris Berezovsky, who was his former university supervisor and later became president of the automobile dealership network LogoVAZ. LogoVAZ was the main dealer for AvtoVAZ, the Tolyatti-based producer of Lada automobiles and the country's largest automobile manufacturer. Berezovsky later went into exile in Britain and his actions at LogoVAZ were central to Russia's extradition request to the UK in 2003[28].

Aven joined Alfa Group in 1993 and became president of Alfa Bank in 1994. He brought no capital, but had powerful political connections and working knowledge of how financial markets functioned. Notably, with the help of his political contacts, Alfa Eko became a major exporter of oil and Petroleum products by 1993 and made use of sophisticated transfer pricing arrangements.

Since the beginning of his tenure, Aven's role as president of Alfa Bank has always been strategic, and he has delegated day-to-day operations to a series of CEOs. He also brought in Andrei Gafin, an old friend with no banking experience, to do PR for the bank. Notably, Aven was given credit for seeing Alfa Bank through the financial crisis, having anticipated the currency crash if not the sovereign default.

---

[27] "Putin's Kleptocracy: Who Owns Russia," Karen Dawisha, accessed electronically

[28] http://www.nytimes.com/2003/03/26/world/britain-arrests-russian-expatriate-billionaire-and-a-colleague.html

In the 2000s, Aven has positioned himself as the president of Alfa Bank and the chairman of various, uncontroversial media and retail ventures. He has sought to play down his close relationship with the Kremlin. He received an award in 2015 for "Services to the Fatherland" along with four other business figures[29].

Notably, Financial Times journalist Andrew Jack noted in his book Inside Putin's Russia that during an interview in which Aven was downplaying any government connections, Aven received a call about a senior resignation in the government that was not made public until three days later.

It is clear that Aven remains the key political figure in Alfa Group, with multiple current links to the government and security services, as outlined above. He has also driven the development of international links through the expansion of Alfa Bank in the US and Europe. The bank has carried out careful outreach, running an international Alfa Fellows program and maintaining a high profile. Although not itself a target, the bank has suffered from sanctions however, and has a particular interest in lifting sanctions[30].

Aven has spent years cultivating relationships in Washington, both as an envoy of Vladimir Putin on trade matters and a representative of the interests of Alfa Group. He is well prepared to support and promote a political agenda in the US if it suits Russia and Alfa.

Richard Burt

Burt plays a big role in Alfa's "deep lobbying" program of spreading donations to influential groups in the US. A former top BGR executive, he is now a managing director of McLarty Associates and a member of Alfa's International Advisory Council. He is also the owner of a small consultancy, **IEP Advisors**, with historical links to Alfa. Burt, a former US Ambassador to Germany, also works with **Deutsche Bank**, the only major bank still willing to lend substantial sums to the Trump Organization despite Trump's multiple bankruptcies.

---

[29] http://www.gazeta.ru/business/news/2015/05/29/n_7241257.shtml
[30] http://www.bloomberg.com/news/articles/2014-08-22/sanctions-free-no-shield-for-alfa-in-wary-market-russia-credit

RICHARD BURT

AT A GLANCE

- Managing Director, Europe & Eurasia Practice
- Former US Ambassador to Germany
- Former Assistant Secretary of State for European and Canadian Affairs
- Chief Negotiator in the Strategic Arms Reduction Talks with the Soviet Union
- Former partner with McKinsey & Company

Richard Burt, Managing Director, has led the firm's work in Europe and Eurasia since 2007.

From 1992 to 1995, Ambassador Burt was a partner with McKinsey & Company, the global management consulting firm. Ambassador Burt came to McKinsey after successfully concluding a nuclear arms treaty as the US Chief Negotiator in the Strategic Arms Reduction Talks with the former Soviet Union.

Prior to this, Ambassador Burt was US Ambassador to the Federal Republic of Germany from 1985 to 1989. Before Ambassador Burt served in Germany, he worked at the State Department as Assistant Secretary of State for European and Canadian affairs from 1983 to 1985. From 1981 to 1983, Ambassador Burt was the Director of Politico-military Affairs in the Department of State.

From 1977 to 1980, Ambassador Burt worked in Washington as the National Security Correspondent for . From 1973 to 1977, he worked for the International Institute for Strategic Studies (IISS) in London, first as a Research Associate and then as Assistant Director.

Ambassador Burt serves on the board of Deutsche Bank's closed-end fund group and is also a trustee of the UBS family of mutual funds (New York board). In addition, he is an Advisor to EADS North America's board and a member of the Alfa Bank's Senior Advisory Board in Moscow.

Ambassador Burt also serves as a Senior Advisor to the Center for Strategic and International Studies and is a member of the Council on Foreign Relations. He is a board member of the Center for the National Interest and a member of the executive board of the Atlantic Council. Ambassador Burt serves as Chairman of Global Zero USA, an organization focused on developing a viable plan for eliminating nuclear weapons worldwide.

Ambassador Burt earned his bachelor's degree in government from Cornell University and his master's degree in international relations from the Fletcher School of Law and Diplomacy at Tufts University. Upon receiving his MA,

Burt has acknowledged that he played a significant role in writing Trump's first major foreign policy speech. "I was asked to provide a draft for that speech. And parts of that - of my draft -- survived into the final," he told NPR.[31]

In the April 27 "America First" speech, Trump laid out an isolationist foreign policy. He criticized NATO and promised he would pursue better relations with Russia-- skipping over its invasions of its neighbors and human rights abuses.[32]

Burt has extensive ties to both Alfa and the Kremlin-backed aluminum oligarch Oleg Deripaska. Like Paul Manafort and Carter Page, Burt was a foreign policy advisor to Sen. John McCain for his 2008 presidential campaign. As has been widely reported, Manafort has had extensive business dealings with Deripaska and stands accused of absconding with at least $19 million of Deripaska's money. The true amount is believed to by much higher.

Burt's ties to Alfa stretch back to the early years of the George W. Bush presidency when he was working for Barbour Griffith & Rogers. BGR first landed Alfa as a client in December of 2002 for "monitoring economic development and policy issues." In its lobbying reports for 2011, BGR reported receiving $570,000 in fees from Alfa. While that is a generous sum,

---

[31] http://www.npr.org/2016/05/14/478040422/trump-s-america-first-foreign-policy-as-a-strategy-to-pursue-national-interests-

[32] http://www.nytimes.com/2016/04/28/us/politics/transcript-trump-foreign-policy.html

it likely understates by a large margin the fees BGR took in. BGR claimed in its filings that it lobbied for Alfa regarding "US-Russian and WTO negotiations," an elastic term.

When the lobbying firm BGR decided to form a private intelligence consultancy in 2003 called **Diligence LLC**, it installed Burt as the president. One of the firm's first assignments was working for Alfa, which at the time was pursuing a libel suit against an NGO called the **Center for Public Integrity**.

A former journalist working for CPI, **Knut Royce**, published an article linking Alfa to criminal activity. The article and subsequent court case involved a KGB report on Alfa provided to CPI by Rick Palmer, a former CIA official, alleging narcotics trafficking and other criminal activity.

Diligence also investigated a reporter from *The Wall Street Journal* who had contacted the CPI regarding the Alfa libel case. Private investigators for Diligence conducted a trash-stealing operation against the personal residence of the journalist. The operation was eventually exposed by an insider at Diligence. The affair caused high-level consternation in Washington due to a bizarre snafu: Unknown to the Diligence investigators, the reporter had vacated his home and rented it to a top White House official. That led to a confidential national security investigation of possible espionage by Alfa.

The lawsuit was dismissed, no charges were brought, and the controversy eventually blew over. In 2007, Burt sold his personal stake in Diligence and left BGR for McLarty Associates.

Burt continued to cultivate influence in Washington for Alfa, working closely with the **Wilson Center**, which bestowed awards on Fridman and Aven and feted them at annual dinners. Burt also helped run the Alfa Fellowship Program, which sponsored internships in US agencies including the State Department.[33]

Aven and Fridman in May 2008 also obtained a private meeting with US Treasury Sec. Henry Paulson at the Treasury headquarters building next to the White House. After Obama took office, a series of additional meetings took place. The meetings were arranged by Alfa's two top lobbyists, former diplomat Richard Burt and former White House official Ed Rogers. While they now run separate firms, Burt and Rogers have long collaborated closely to advance Alfa's interests in Washington, including aggressive intelligence gathering operations against journalists and others who threaten Alfa's interests.

The first meeting took place on May 13, 2010. Fridman and Aven visited a top White House official named David Lipton. They were accompanied by a former diplomat named Stephen Rademaker, now a lobbyist working for Ed Rogers. On May 12, 2011, Fridman, Aven, and Richard Burt were admitted to the Old Executive Office Building a second time. They were signed in by a White House special assistant named Groslyn Foster Burton. But it is likely they visited a more senior official whose name was kept off the records, probably David

---

[33] http://www.culturalvistas.org/alfa-fellowship/russia-alfa-fellowship-program-celebrates-10th-anniversary

Lipton again, given that Ms. Burton is his assistant. Lipton is a longtime associate of Leonard Blavatnik (See below). He recently took a new position at the International Monetary Fund.

The 2011 Meeting Record

NAMEFIRST	NAMELAST	TOA	TOD	visitee1	visitee2
Richard	Burt	5/12/2011 15:44	5/12/2011 16:55	Groslyn	Burton
Mikhail	Fridman	5/12/2011 15:45	5/12/2011 16:55	Groslyn	Burton
Peter	Olegovich	5/12/2011 15:47	5/12/2011 16:55	Groslyn	Burton

It is notable that the three high-level visits all occurred in May, suggesting the possibility that Fridman and Aven visit Washington annually in May for a charitable event. One charitable event held annually in May is the annual fundraising dinner for the Kennan Institute at the Woodrow Wilson International Center for Scholars. Access Industries and Alfa lawyers Akin Gump are both supporters of the Wilson Center, while Blavatnik is vice chairman of the Kennan Institute.

The final Fridman visit to the White House took place around the same time in 2012 (May 8), suggesting it was also in conjunction with the Wilson Center annual event. Attendees were Mikhail Fridman, Petr Aven, Richard Burt, and John W. Roberts. They met with **Alice Wells,** Special Assistant to the President for Russia and Central Asia and former executive assistant to Sec. of State Hillary Clinton.

NAMELAST	NAMEFIRST	NAMEMID	UIN	APPT_START_DATE	APPT_END_DATI
Aven	Petr	O	U05460	5/17/12 15:00	5/17/12 23:5
Burt	Richard	R	U05460	5/17/12 15:00	5/17/12 23:5
Fridman	Mikhail	M	U05460	5/17/12 15:00	5/17/12 23:5
Roberts	John	W	U05460	5/17/12 15:00	5/17/12 23:5

The White House-Treasury meetings in 2008 are somewhat remarkable: US agencies possess substantial information alleging criminal activity by Aven and Fridman, including organized crime and narcotics trafficking. Alfa was also the subject of a lengthy money-laundering and stock manipulation investigation by the Manhattan District Attorney that was ultimately shelved. While the allegations against Alfa and its founders are considered to be unsubstantiated, the mere existence of such derogatory allegations – some of which have even been aired publicly – is often enough to preclude entry into the executive complex.

But unlike many of their Russian peers, Aven and Fridman are not officially listed in US law enforcement files as organized crime figures. This has given them largely unfettered access to the United States, and they make frequent visits to Washington to appear at policy forums and other events. It is believed that these trips sometimes include small dinners with top Washington officials or other similar types of "off the record" encounters.

Akin Gump

The Alfa libel case against CPI nearly bankrupted the CPI. Ultimately, it was dismissed by a federal judge in 2005. The law firm for Alfa in the libel case was Akin Gump, where top lawyers **James Langdon** and **Mark MacDougall** represent the group. Langdon is an influential Republican with intelligence connections while MacDougall is a Democrat with Justice Department connections and a fierce litigation style.

Akin Gump lobbied for Alfa/Vimpelcom/Altimo during its lengthy battle with Telenor, and also advised Altimo on various legal matters.

Akin Gump handed Alfa its biggest political victory in Washington in connection with Tyumen Oil loan guarantees from the Export-Import Bank. BP Amoco mounted a sustained campaign to delay or block those loan guarantees, but TNK prevailed thanks to deft lobbying by Langdon, a former Navy intelligence officer and member of President George W. Bush's Foreign Intelligence Advisory Board, a high-level external advisory group to the White House. During the controversy, information was provided to US officials alleging illegal oil dealings between Alfa and Saddam Hussein. The information was later substantiated by the United Nations. Blavatnik played a major role in this battle, which was chronicled in an unusually detailed Washington Post article.[34]

Blavatnik's Ties to Democrats

While Rogers is a well-known Republican, the group has very powerful Democratic ties through Blavatnik, who is particularly close to Secretary of State Hillary Clinton through extensive donations to her campaigns and causes. The Blavatnik family have also contributed heavily to the campaigns of Vice President Joe Biden.

Records show the Blavatnik family have given more than $300,000 in contributions since 1996. Employees of Renova and Access have given another $700,000. Emily Blatanik gave $35,800 to the Obama campaign in August of 2011.

Blavatnik also enjoys influence through is longstanding ties to a group of Harvard economists including former Treasury Sec. Larry Summers (who chaired the Obama White House economic council until 2010), Jeffrey Sachs, David Lipton, and Andrei Shleifer. Sachs, Shleifer, Lipton and Sachs were the subject of a criminal fraud investigation involving Harvard's dealings in Russia during the privatization era. This matter was detailed in a major 2006 investigative report in a business magazine.[35]

Access is represented in Washington by the lobbying firm Brownstein Hyatt, which reported receiving $330,000 to lobby on tax issues and various other matters. Brownstein Hyatt is a top Democratic lobbying firm.

---

[34] http://www.washingtonpost.com/wp-srv/WPcap/1999-10/27/085r-102799-idx.html
[35] http://janinewedel.info/harvardinvestigative_InstInvestorMag.pdf

Alfa's Soft Lobbying

Donations by Alfa/Access to influential US think tanks include large sums to the Rand Institute, which is affiliated with the Pentagon, the Center for Strategic & International Studies, the Wilson Center, the Council on Foreign Relations, and the Atlantic Council.

Alfa also maintains a well-funded fellowship program whose recipients often land important jobs in the US. Alumni include:

- Marcy Fowler, now at the IAEA.
- James Lindley, US Dept. of Commerce
- Rachel Mikeska, Department of State (currently in Kuwait).
- Francoise Schorosch, Council of the Americas
- Scott Schrum, National Nuclear Security Administration
- Nadezhda Mouzykina, National Democratic Institute
- Raisa Sheynberg, Treasury Department
- Ilona Tservil, Justice Department
- David Wright, Treasury Department
- Michael Kreidler, State Department

Alfa also maintains the Altimo Foundation, which maintains primarily a UK focus but employs the influential US lobbying firm APCO.

-0-