FD 1057 (Rev. 5 8 10)

[redacted]

FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: (U) To Close Case **Date:** 01/18/2017

CC: AUTEN BRIAN JAMES
GAYNOR RYAN C
Joe Pientka III

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

Approved By: SSA Daniel S. Wierzbicki

Drafted By: Allison Sands
Curtis A. Heide

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

Synopsis: (U) To Close Case

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

GOVERNMENT EXHIBIT
0233
21-CR-582 CRC

Full Investigation Initiated: 09/23/2016

Details:

[redacted] Chicago opened captioned Preliminary Investigation on alleged covert communications between Russian based ALFA BANK and an email domain affiliated with the TRUMP ORGANIZATION. On or about September 19, 2016, FBI received a whitepaper that was produced by an anonymous third party from the US DEPARTMENT OF JUSTICE. According to the whitepaper, an usually configured U.S. based server affiliated with the TRUMP ORGANIZATION was communicating with ALFA BANK evidenced by inexplicable DNS queries to the domain mail1.trump email.com from IP [redacted]

[redacted]

Title: (U) To Close Case
Re: [redacted] 01/18/2017

addresses registered to ALFA BANK. The third party identified that some of the communications were utilizing a TOR node identified at Michigan based SPECTRUM HEALTH. The servers were reportedly configured for direct and exclusive communication between the TRUMP ORGANIZATION and ALFA BANK.

(U) After speaking to CENDYN ONE (CENDYN), the registrant of the mail1.trump email.com domain in question, investigators discovered that the domain has had very limited traffic over it's lifespan. The domain received approximately 14 e mails over several years, all of which were blocked as spam or malware. CENDYN released control of the domain back to the TRUMP ORGANIZATION over a year ago, however the TRUMP ORGANIZATION had not updated the contact information for the administrative and technical points of contact on the internet registration information. The domain was still active in the CENDYN DNS tables but following FBI inquiry, was deleted from CENDYN DNS tables.

(U) Logs provided by LISTRAK, the Internet Service Provider that hosted the email server in question, revealed that the server had been used to send emails to 30,817 domains residing in 107 countries. Russian based domains were discovered as well, but none affiliated with ALFA BANK or any of the IP addresses referenced in the white paper. Communications with SPECTRUM HEALTH resolved to marketing emails sent to two "@spectrumhealth.org" email address along with another 584 email addresses with "health" in the domain name. There was no evidence that ALFA BANK was using SPECTRUM HEALTH as an "exclusive" TOR node as alleged in the whitepaper. Furthermore, LISTRAK IT personnel confirmed that this particular server was configured as an outbound server only and was not set up to receive emails. Based on the data provided from LISTRAK, there was no conclusive record that this mail transfer agent was used for covert communications.

[redacted]

[redacted]

[redacted]

Title: (U) To Close Case
Re: [redacted] 01/18/2017

[redacted]

Examination of communications between the two parties and subsequent preventative steps led FBI Chicago to assess with high confidence that ALFA BANK and TRUMP ORGANIZATION servers did not communicate intentionally or covertly. This assessment was based on a highly reliable sensitive source with excellent access and corroborated FBI investigative activity.

(U//FOUO) Finally, an interview with [redacted] at MANDIANT and [redacted], confirmed rumors that MANDIANT was hired by ALFA BANK in mid September to investigate an allegation that ALFA BANK was engaged in covert communications with the TRUMP ORGANIZATION. [redacted] confirmed that the issue was brought to the attention of ALFA BANK by the New York Times. MANDIANT's investigation concluded that the data in the whitepaper was inconclusive and did not indicate an financial link between ALFA BANK and the TRUMP ORGANIZATION. MANDIANT's analysis did not reveal any communications beyond DNS queries, and specifically did not see any activity indicating communication between the two parties.

[redacted] To date the investigation has not revealed any evidence to support allegations made in the white paper or any indication of covert communications between ALFA BANK and TRUMP ORGANIZATION servers. There is also no evidence to support the allegation that ALFA BANK is using SPECTRUM HEALTH as an exclusive TOR node. Chicago will continue to monitor ALFA BANK's activities as they relate to U.S. interests through national technical means. Chicago recommends closing captioned investigation.

[redacted]

[redacted]

Title: (U) To Close Case
Re: [redacted] 01/18/2017

♦♦

[redacted]