

# ALFA-TRUMP REDUX: FULL SPECTRUM CIRCUMSTANCE

The Trump Tower – Alfa Bank story is back!

Back in October 2016, Franklin Foer wrote about some metadata analysis showing that a marketing server paid for by Trump Organization was messaging with a server at Russia's Alfa Bank. The story, as Foer presented it, was quickly challenged. I myself focused on a side angle to the story: that in addition to communications with Alfa Bank, the Trump marketing server was also communicating with Grand Rapids' Spectrum Health, which (the original public pitch of the story suggested) might show a tie between the DeVos family – or maybe Erik Prince – and Trump. From the vantage of October 2016, that didn't make sense, as the DeVoses (as distinct from Betsy's brother Erik) were actually remarkably hesitant to support Trump until after the DNS lookups ended.

Dexter Filkins has now reexamined the story. It concludes – via a proliferating set of academics and cybersecurity experts departing from the norm in both those fields and insisting on hiding their identities – that there must be some kind of communication going on.

(Max and his colleagues did not see any D.N.S. evidence that the Trump Organization was attempting to access the server; they speculated that the organization was using a virtual private network, or V.P.N., a common security measure that obscures users' digital footprints.)

If this was a communications mechanism, it appeared to have been relatively simple, suggesting that it had been set up spontaneously and refined over time. Because the Trump Organization did not have administrative control of the

server, Paul and Leto theorized that any such system would have incorporated software that one of the parties was already using. "The likely scenario is not that the people using the server were incredibly sophisticated networking geniuses doing something obscure and special," Max said. "The likely scenario is that they adapted a server and vender already available to them, which they felt was away from prying eyes." Leto told me that he envisioned "something like a bulletin-board system." Or it could have been an instant-messaging system that was part of software already in use on the server.

Kramer, of Listrak, insisted that his company's servers were used exclusively for mass marketing. "We only do one thing here," he told me. But Listrak's services can be integrated with numerous Cendyn software packages, some of which allow instant messaging. One possibility is Metron, used to manage events at hotels. In fact, the Trump Organization's October, 2016, statement, blaming the unusual traffic on a "banking customer" of Cendyn, suggested that the communications had gone through Metron, which supports both messaging and e-mail.

The parties might also have been using Webmail—e-mail that leaves few digital traces, other than D.N.S. lookups. Or, Paul and Leto said, they could have been communicating through software used to compose marketing e-mails. They might have used a method called foldering, in which messages are written but not sent; instead, they are saved in a drafts folder, where an accomplice who also has access to the account can read them. "This is a very common way for people to communicate with each other who don't want to be detected," Leto told me.

I hope to return to some of the moves Filkins makes in his story generally after I come home from this trip. But for now, I just want to look at how Filkins deals with the Spectrum Health tie, which Filkins focuses on even more than Foer. Here's how he introduces the connection:

Only one other entity seemed to be reaching out to the Trump Organization's domain with any frequency: Spectrum Health, of Grand Rapids, Michigan. Spectrum Health is closely linked to the DeVos family; Richard DeVos, Jr., is the chairman of the board, and one of its hospitals is named after his mother. His wife, Betsy DeVos, was appointed Secretary of Education by Donald Trump. Her brother, Erik Prince, is a Trump associate who has attracted the scrutiny of Robert Mueller, the special counsel investigating Trump's ties to Russia. Mueller has been looking into Prince's meeting, following the election, with a Russian official in the Seychelles, at which he reportedly discussed setting up a back channel between Trump and the Russian President, Vladimir Putin. (Prince maintains that the meeting was "incidental.") In the summer of 2016, Max and the others weren't aware of any of this. "We didn't know who DeVos was," Max said.

This is a remarkable paragraph, repeating a lot of the shitty link analysis that people always do when they try to explain the Spectrum tie. In it, a children's hospital named after Dick DeVos' mother is the smoking gun in an international spy plot. Then, having utterly ignored the status of the relationship between the DeVoses and Trump *at the time of the DNS lookups*, Filkins looks at what has happened since: the appointment of close Mike Pence ally and leading GOP education ideologue Betsy to be Education Secretary, and Erik Prince's covert meeting with an entirely different – and far

more suspect – bank, using means that are precisely the kinds of means you’d expect Erik Prince to use (and not using the network of a hospital that his brother-in-law chairs but doesn’t run, because why the fuck would a Navy Seal use more covert methods that Navy Seals know well instead of using a server with an easily subpoenaed footprint in the US??).

The paragraph misses some other details of note. For example, after Dick got on a commercial puddle jumper to fly to interview with Trump, he was appointed to the FAA Advisory Board, another position for which he is an obvious and arguably well-qualified pick. It also doesn’t note that Prince – who is a separate political entity from his sister and brother-in-law – was threatening anti-Trump Republicans both before and after the election, something that might support this theory except for all the other more obvious ways Prince accomplished such efforts.

Which is to say that, while the piece acknowledges that to conclude the Trump – Alfa Bank records are suspect, you also have to explain why the Spectrum ones would be, it does no reporting to discern why that would be the case.

Later in the piece, after trying to explain DNC lookups involving a third entity that had previously only been alluded to (and only alluded to because without explanation, it would have and did problematize past claims), Filkins strains further to suggest the ties between Spectrum and Trump have been proven by events that have taken place since.

In one tranche of data that he gave them, they noticed that a third entity, in addition to Alfa Bank and Spectrum Health, had been looking up the Trump domain: Heartland Payment Systems, a payments processor based in Princeton. Of the thirty-five hundred D.N.S. queries seen for the Trump domain, Heartland made only seventy-six—but no other visible entity made more than two.

Heartland had a link to Alfa Bank, but a tenuous one. It had recently been acquired by Global Payments, which, in 2009, had paid seventy-five million dollars for United Card Services, Russia's leading credit-card-processing company; two years later, United Card Services bought Alfa Bank's credit-card-processing unit. (A spokesperson for Global Payments said that her company had never had any relationship with the Trump Organization or with Alfa Bank, and that its U.S. and Russia operations functioned entirely independently.)

Spectrum Health has a similarly indirect business tie to Alfa Bank. Richard DeVos' father co-founded Amway, and his brother, Doug, has served as the company's president since 2002. In 2014, Amway joined with Alfa Bank to create an "Alfa-Amway" loyalty-card program in Russia. But such connections are circumstantial at best; the DeVos family seems far more clearly linked to Trump than to Russia.

It's this sentence – "the DeVos family seems far more clearly linked to Trump than to Russia" – that exemplifies this story, and its epistemology, for me. It treats the DeVos family – Dick, his wife Betsy Prince DeVos, his brother Doug, his charitable mother Helen, and his brother-in-law Erik Prince, to say nothing of the hospital administrators that actually run Spectrum – as a monolith they're simply not, reads their current varied relationships with Trump back into a history where only Erik's relationship resembled his current one, and then concludes that a link with Dick through Helen-Betsy-Erik is all you need to explain why these presumed conspirators would use a hospital rather than any of the many entities the DeVoses privately hold (and therefore more directly manage) or the Prince entities that already have built-in covert channels with a proven past

ability to reach out to oligarchs discretely.

I mean, I absolutely think there's a place for more journalism on what Erik was doing during the election, his role as a cut-out to Trump, and how he has helped to discipline the Republican party since. Or, if you want to pursue some theory of nefarious plot explaining how the originally reluctant DeVoses came to become close Trump associates, you'd explore far more about Mike Pence's obvious role in it all (to say nothing of Pence's frequent meetings with the DeVoses since), something Jean Camp is well situated to do from Indiana.

But one thing any such journalism would show is that Prince has the ability to conduct covert communications via much more effective channels, and Betsy and Dick DeVos have the network to achieve their political goals via means that don't require hijacking a hospital server they don't directly control.

Meanwhile, the story doesn't explore the tangential role of Alfa Bank, via Alex van der Zwaan, in the Skadden Arps part of the Paul Manafort story, and doesn't explain that any focus on Alfa Bank prior to Trump's inauguration might have distracted from the sanctioned Russian banks that, at least as far as is currently known, are the actual key players in the Trump Russia story. It also doesn't explain that key events in any conspiracy between Trump and Russia were communicated via insecure Trump Organization hosted email, often (in Manafort's case, for long after he had been indicted) backed up to the iCloud.

This Trump Tower – Alfa Bank story continues to spin journalists, not to mention academics and infosec experts, into uncharacteristic habits that don't appear to be leading to any real clarity about the topic at hand.