# *Israeli Snoop-for-Hire Posed as a Fox News Journalist for a Spy Operation*

**Adam Rawnsley** Senior Researcher

**An Israeli private intel firm constructed two fake personas, a Fox News reporter and an Italian journalist, tasked with digging up info on people feuding with a UAE emirate.**

Operatives from an Israeli private investigations company posed as a Fox News journalist and an Italian reporter in an attempt to dig up dirt on lawsuits against the emirate of Ras Al Khaimah in the UAE, The Daily Beast can reveal.

In early 2020, individuals masquerading as a Fox News researcher and a reporter for Italy's La Stampa newspaper approached two men involved in litigation against Ras Al Khaimah, one of the seven emirates that make up the United Arab Emirates. The imposters sought to trick their targets into revealing information about their feuds with the emirate's leadership and learn more about lawsuits against it.

After The Daily Beast shared information about the impersonators with Facebook's security team, Facebook took action and was able to attribute two of the bogus personas they used to an Israel-based "business intelligence" firm named Bluehawk CI. Bluehawk CI was founded by Guy Klisman, a former Israeli military intelligence officer, and describes itself as an intelligence firm staffed by "alumni from special units in the Israeli intelligence community." The firm's website boasts its "specialization is in litigation support by providing answers to complex queries" and markets services from "social engineering & PR campaign management" to cybersecurity services for its clients.

Bluehawk CI did not respond to email requests from The Daily Beast requesting comment.

Facebook's attribution of the intelligence-gathering effort to a private company highlights the legal and ethical challenges surrounding the intelligence-for-hire industry, which offers a range of services to deep-pocketed clients.

The impersonators first reached out to Oussama El Omari, an American citizen who had worked as the CEO of the Ras Al Khaimah Free Trade Zone and sued the emirate in 2016 for what he says was a lump-sum payment owed to him at the end of his service as part of his contract. The suit was subsequently dismissed in 2017.

In February 2020, "Samantha" emailed El Omari and introduced herself as "a journalist and researcher at the FOX news channel in New York" who was interested in writing about "the many cases of immigration and detention between the borders of the Emirates and the Arab Peninsula."

Samantha's English seemed clumsy (she wrote that she was "conducting a research about the situation in the Emirates"), but it appeared as though she had reached out from a legitimate Fox News email address. She was familiar with El Omari's case so he welcomed her outreach, thinking it could bring some press attention to his feud with the leadership of Ras Al Khaimah. El Omari had enjoyed his career at Ras Al Khaimah's free trade zone, where he'd worked alongside Faisal bin Saqr al Qassimi, a member of Ras Al Khaimah's royal family. But in court papers, El Omari said he found himself "caught in a Royal family conflict and power play" when Faisal's father, Saqr, the former ruler of Ras Al Khaimah, passed away and Faisal's brother, Saud, took the throne.

In his 2016 lawsuit, El Omari claimed that after Faisal was removed from the free trade zone's leadership, he was unjustly fired from the organization "and remains today, persecuted in the RAK Rulers Court, in absentia, without due process of law," according to a complaint in the suit. A 2015 conviction against El Omari in Ras Al Khaimah for embezzlement, he has claimed, was a politically motivated false charge.

"Samantha" was familiar with El Omari's legal fight, and in a Skype interview with him, projected sympathy. "I want really to uncover the wrongdoing in all aspect I can really, you know, find," she said in stilted, heavily accented English. Hiding behind a Fox logo, she pumped him for information on his "knowledge about allegations found in three lawsuits" against Ras Al Khaimah and the parties involved, according to a lawsuit filed by El Omari in March of 2020.

Then, just as quickly as she appeared, "Samantha" ceased to exist. The Fox News email address she had used to contact El Omari—foxnews-middleeast.com—turned out to be a fake, unrelated to the real Fox News. A phone number listed at the bottom of her email was, in fact, Fox News' public customer support line.

In the March 2020 suit filed by El Omari, he claimed that “Samantha” had been “based on the stolen identity of a real young woman, similar in age and appearance,” who had previously worked at the news channel.

The fake Fox reporter’s approach resembles a similar ruse in which a Facebook user pretending to be an Italian reporter approached Khater Massaad, a Lebanese-Swiss citizen who had worked as the chief of Ras Al Khaimah’s sovereign wealth fund, RAKIA, until he left in 2012. In 2015, a court in Ras Al Khaimah convicted Massaad in absentia of embezzlement from RAKIA and accused him of having pocketed millions from the organization.

Like El Omari, Massaad has claimed that the charges against him were false and politically motivated—a result of Ras Al Khaimah viewing him as an ally of Faisal, and an opponent to the emirate’s current government.
The fake Italian reporter approached Massaad via Facebook message asking to discuss his relationship with the government of Ras Al Khaimah. Massaad did not engage with the attempt. As it turns out, he had good reason not to: the curious Italian reporter was an imposter linked to Bluehawk CI.

Bluehawk CI has few traces online. Its CEO, Guy Klisman, lists himself as a 25-year Israeli Military Intelligence veteran, and has been referred to as a “former cyber spy.” Another potential employee described himself as Bluehawk CI’s “UAE regional business development manager,” writing that he was “an expert in the UAE and the Arabian Gulf” as well as a veteran of the Israeli military’s much-respected cybersecurity and signals intelligence outfit, Unit 8200.

What’s less clear is who may have hired Bluehawk CI to carry out the campaign, and why. El Omari filed a lawsuit in federal court alleging that employees at a range of firms retained by Ras Al Khaimah were behind the fake Fox reporter. In court, the defendants have all denied El Omari’s allegations that they had anything to do with the hoax.

El Omari and Massaad’s run-ins with fake personas highlight what critics of Ras Al Khaimah say are the obstacles they face when trying to sue the emirate in court.

In a separate incident, a fake philanthropist reached out to Radha Stirling, an attorney who has represented both El Omari and Massaad in court cases involving Ras Al Khaimah. Unlike the fake reporters linked to Bluehawk CI, it’s unclear who was responsible for this attempt as there is insufficient evidence to attribute it to any specific actor. But the incident, which involved a crude attempt to hack the attorney’s phone, shows the lengths that some are apparently willing to go to seek information about lawsuits against Ras Al Khaimah.

Last year, “Justine Dutroux” showed up in Stirling’s inbox and introduced herself as an assistant to a wealthy philanthropist, hinting that she might be interested in funding Stirling’s work on cases involving Ras Al Khaimah (RAK).
Stirling, however, was suspicious from the start.

“They were very keen for me to give them information pertaining to which ‘players’ I was in contact with, within the various lawsuits involving RAK,” she told The Daily Beast. “They asked if I could establish contacts who are currently in RAK, close to the royal family, that I could introduce to them. In other words, they wanted me to oust those who may be traitors.”

*“We are ensuring that those*

*responsible are held to full account.”*

**— Radha Stirling, attorney.**

“Justine” had other interests, too. Specifically, she was curious about Haya bint Hussein, the Jordanian princess who married the ruler of Dubai, Sheikh Mohammed bin Rashid Al Maktoum, in 2004 but left the UAE and her husband for the U.K. two years ago, eventually filing for divorce and causing a scandal in the royal court.

“They wanted to know whether I was in touch with Princess Haya and whether I could introduce them to Lady Shackleton, Haya’s lawyer,” Stirling said.

“Justine,” according to Stirling, “wanted to know in particular about Princess Haya’s personal assistant,” whether she still worked for the princess, and if Stirling could help make an introduction to the princess and her entourage.

Throughout the conversations, “Justine” used the lure of money as bait to gain Stirling’s confidence. She offered Stirling a private jet trip to Morocco to meet with her employer and asked her to send an invoice for payment.

And then the conversation took an altogether more sinister turn. Screenshots reviewed by The Daily Beast show that “Justine” sent Stirling two apps labeled “PaymentsApp” and “CapitalControl” through WhatsApp, explaining that the apps would allow her to monitor the billionaire’s payments to her firm and make future payments easier.

The programs would have done nothing of the sort. The Daily Beast shared the two applications with the University of Toronto's Citizen Lab, a research organization focused on the intersection of human rights and cybersecurity, for analysis.
“This is remote access malware built on the publicly available Metasploit framework”—a cybersecurity site that produces a range of malicious software available to researchers—John Scott-Railton, a senior researcher at Citizen Lab, told The Daily Beast. He explained that the malware sent to Stirling is “not at all sophisticated, but if the social engineering works, then it would be a viable way to monitor somebody.”

In this case, it wasn’t. The hackers had mistakenly sent malware designed for an Android operating system to an iPhone, where it wouldn’t have worked.

But Stirling’s suspicions had still served her well. As “Justine” dangled money and malware, she quietly reached out to cybersecurity experts who helped her embed a script inside a document which, when opened, reached out to a server, giving her team the IP address of the computer which had opened the file.
The code, known as a “canary token,” showed that the file was opened at least three times—twice from computers connected to IP addresses in Australia and once on a computer connected to an Israeli IP address.

Stirling, a citizen of the U.S., UK, and Australia, says she is determined to find out who was behind the attempt to hack her. “We are ensuring that those responsible are held to full account,” she told The Daily Beast in a text exchange. “Hacking is a serious crime, and it’s important that the FBI take such crimes against U.S. citizens seriously.”