NATIONAL SECURITY

Russian Influence Campaign Extracted Americans' Personal Data

Operators used social media to pitch fake business directories, petitions in return for information

By Shelby Holliday and Rob Barry
March 7, 2018 5:30 a.m. ET

All the Facebook account Black4Black asked for was some personal information about Ajah Hales and other Cleveland-area small-business owners. In exchange, she was told her cosmetics company, and her fellow African-American entrepreneurs, would receive free promotion on social media and in a new and influential directory of black-owned businesses.

Ms. Hales soon turned over basic information about her company, as well as names, phone numbers, email addresses and websites of dozens of black business owners in and around Cleveland.

"I was actually really excited about the opportunity," she said.

That was in early 2017. It wasn't until recently, after being contacted by The Wall Street Journal, that Ms. Hales would learn that Black4Black and "partner" groups, including BlackMattersUS, were among hundreds of Facebook and Instagram accounts set up by a pro-Kremlin propaganda agency to meddle in American politics, Facebook records show.

The fake directory is one example of the elaborate schemes that Russian "trolls" have pursued to try to collect personal and business information from Americans, the Journal has found. Leveraging social media, Russians have collected data by peddling niche business directories, convincing activists to sign petitions and bankrolling self-defense training classes in return for student information.

It isn't clear for what purpose the data were collected, but intelligence and cybersecurity experts say it could be used for identity theft or leveraged as part of a wider political-influence effort that didn't end with the 2016 election. That operation is a focus of special counsel Robert Mueller's wide-ranging probe, which has returned more than a dozen indictments of Russians as well as several American associates of now-President Donald Trump.

Russia has denied trying to influence the election, and Mr. Trump has said his campaign didn't work with Moscow.

A spokesman for Facebook Inc., which also owns Instagram, said the company allows users to find out whether they have "liked" or "followed" any Russia-backed accounts through an online tool. However, the tool doesn't notify users who exchanged messages with or turned over information to the accounts.

Facebook, along with other tech companies, has pledged to crack down on foreign interference ahead of this year's midterm elections, although the social media behemoth has been criticized for being slow to understand the depth of the problem and its role in it.

In addition to shutting down hundreds of accounts operated by Russian operatives, Facebook said it is hiring 10,000 new safety and security employees, verifying that buyers of political

advertisements are in the U.S. and working to root out the online promotion of phony news reports.

Federal charges leveled last month as part of the Mueller probe hint at the value of such personal and business data. Russian operators used stolen American identities to open bank and PayPal accounts, create fake driver's licenses, post messages online and buy political advertisements before the 2016 election, according to the indictment.

The operators allegedly kept a list of more than 100 Americans and their political views to "monitor recruitment efforts," Mr. Mueller's office said. Their targets included niche groups ranging from Texas secessionists and "Southern heritage" proponents to the lesbian, gay, bisexual and transgender community and the Black Lives Matter movement.

Some of the Facebook and Instagram ads linked to a Russian effort to disrupt the American political process, released by members of the House Intelligence Committee last November. PHOTO: JON ELSWICK/ASSOCIATED PRESS

"Russian intelligence services...can sit back and collect from thousands of miles away," said Leo Taddeo, chief information security officer of Cyxtera Technologies and the former special agent in charge of the Federal Bureau of Investigation's New York Cyber Division. "The more they know about us, and what we care about, the better they can sharpen their influence campaigns."

Black4Black and its partner account BlackMattersUS, which had hundreds of thousands of followers on social media, asked the American entrepreneurs to answer detailed questions so it could write articles promoting their companies. More than a dozen entrepreneurs contacted by the Journal said they turned over data to participate in the directory, yet none reported gaining any new customers. None had been contacted by Facebook or government investigators; only one had heard about the accounts' ties to Russia.

Efforts to reach representatives of Black4Black or BlackMattersUS weren't successful.

Multiple Russian accounts reached out to Orlando, Fla., fitness instructor Maurice Bright in early 2017 with enticing offers: work with them to build his fledgling business.

While Black4Black offered Mr. Bright free promotion in its business directory, a group claiming to be an activist organization, using the Instagram account BlackFist, paid Mr. Bright to teach self-defense lessons in his community. In exchange, it wanted information about the people who showed up for classes, including phone numbers, email addresses and even videos.

“They were really adamant about getting names,” Mr. Bright said.

He gave BlackFist videos and photos but said he stopped short of sending attendees’ contact information. He quit working with the group after it asked him to provide more “aggressive” lessons, including training in offensive combat.

In all, he said he made roughly $700 teaching 12 classes in a local park. BlackFist paid him using a PayPal account connected to the Russia-backed BlackMattersUS, the Journal found. The same account, which PayPal has shut down, is listed as fraudulent in the special counsel’s indictment.

Trainers across the country were contacted by BlackFist with a similar offer, according to interviews, Instagram posts and event listings.

Another Russian group, “Don’t Shoot,” identified as Russia-linked in congressional hearings last fall, appeared to collect information by asking followers to sign petitions and report police misconduct on its website, DoNotShoot.us.

The website, which was still active this month, has 12 petitions purporting to have hundreds of signatures each, as well as more than 400 reports of misconduct.

San Antonio resident Lysa Reyes said Don’t Shoot helped her create a petition calling for an end to “police violence against pit bulls” after her family dog, Mr. Brown, was shot and killed by a Bexar County Sheriff’s Office deputy. Her family promoted the petition on social media, and according to Don’t Shoot’s website, it amassed 370 signatures.

Don’t Shoot’s website says it ensures “direct delivery to decision makers,” but a representative for the sheriff’s department said he found no record of having received the petition.

For many Americans targeted by the apparent collection effort, concerns linger about the fact that sensitive information could be in the hands of Russian operatives.

“We’re all just trying to make an honest living here,” said Ms. Hales, the business owner from Cleveland. “I would feel comfortable knowing that whoever’s behind this and whatever information they were pursuing has been shut down.”

Write to Rob Barry at rob.barry@wsj.com