Businessweek | The Big Take

The FBI's Star Cooperator May Have Been Running New Scams All Along

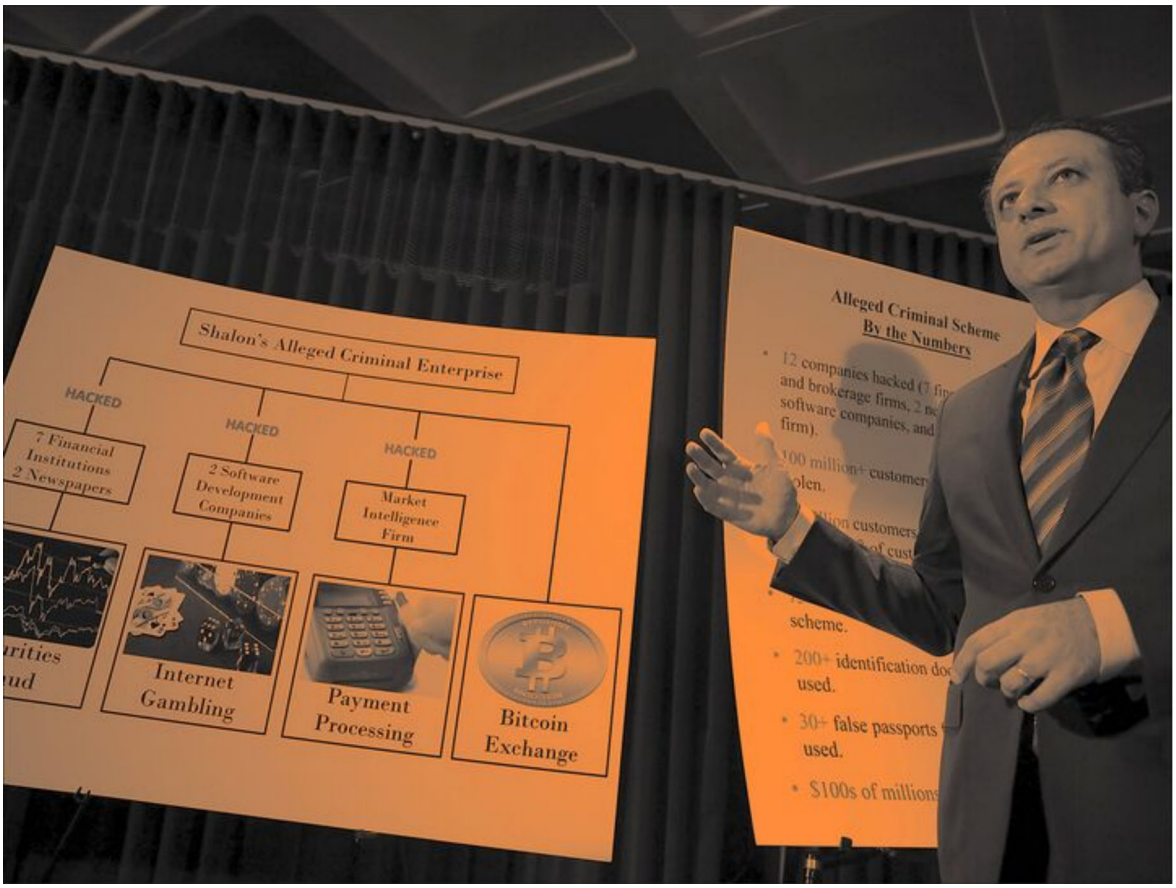
When Gery Shalon, mastermind of the infamous JPMorgan hack, flipped, US law enforcement considered it a triumph. But new evidence suggests that while Shalon was working with the FBI, he built a massive new fraud empire in Europe.

Illustration: Ard Su for Bloomberg Businessweek

By Simona Weinglass, Michael Riley, and Jason Leopold
June 26, 2024 at 11:00 PM GMT+2

On Nov. 10, 2015, Preet Bharara, then the US attorney for the Southern District of New York, stepped behind a podium in the lobby of 1 Saint Andrew's Plaza in Manhattan and made a stunning announcement. Flanked by agents from the FBI and the US Secret Service, he trumpeted the takedown of "one of the largest cyberhacking schemes ever uncovered." JPMorgan Chase & Co., a pillar of the global financial system, had been hacked the year before by a gang that also infiltrated other marquee financial companies, including Dow Jones & Co. and ETrade Financial Corp. After months of patient investigation, Bharara said, agents had connected those breaches to a uniquely sophisticated criminal organization, the leaders of which were now in custody.

As Bharara went on to explain that day, the mastermind of the hacks was a 31-year-old Israeli named Gery Shalon. Shalon, who speaks Hebrew, Russian, Georgian and English, had created a global operation that reached across the world of high-level cybercrime. He ran online gambling websites and an illegal cryptocurrency exchange; he laundered money for hackers and sellers of fake pharmaceuticals.



US Attorney for the Southern District of New York Preet Bharara announces charges against Gery Shalon and two others in the JPMorgan Chase hacking case. *Photo illustration: 731; Photo: Spencer Platt/Getty Images*

The Wall Street hacks were part of an entirely separate scheme to inflate the value of worthless stocks, generating huge profits for Shalon and his gang before prices fell

to support a diversified criminal conglomerate.

Even that may have understated the significance of the case, according to agents who worked it. Shalon was a rare catch—a global thinker adept at connecting figures from the dark web's various fiefdoms with creative schemes that made hundreds of millions of dollars for him and his partners. "This guy was the Don Corleone of cybercrime," says one former FBI agent on the case who asked not to be named in order to speak freely about it.

As Bharara spoke in New York, Shalon was sitting in an Israeli jail, detained at the request of US authorities, and the US attorney predicted the case would change the narrative that foreign hackers can operate with impunity. "The good news is that the FBI and Secret Service have cracked this case—and we aim to prove it in court."

Shalon at the Jerusalem Magistrates' Court. He was detained at the request of US authorities and extradited. *Photo illustration: 731; Photo: Yonatan Sindel/Flash90*

Shalon never saw the inside of a US courtroom, at least not as part of any trial for his crimes. He began cooperating with the Department of Justice, which kept details of the case secret for the next eight years. Shalon still operated from the shadows, this time working for the FBI and US intelligence agencies. But that wasn't all he did, according to police and prosecutors in Europe. They have evidence that during his time as a US cooperator, Shalon continued to run a substantial criminal operation targeting tens of thousands of European victims. The question, they say, is whether the FBI was running Gery Shalon or Shalon was running the FBI.

in Justice Department parlance as a “proactive cooperator,” according to filings regarding his criminal case that were unsealed in December. Eun Young Choi, the assistant US attorney on the case, said at Shalon’s sentencing hearing that Shalon had for years been “acting proactively at the direction of law enforcement in an effort to further various ongoing criminal investigations.” Two former US officials familiar with the details of his cooperation, many of which are being reported for the first time, said that his activities included infiltrating hacking groups and collecting evidence on the US government’s behalf. He even traveled internationally under FBI supervision.

For more than four years, Shalon gave the government details about Russian money laundering, cyber kingpins and global hacking operations, laying the foundation for multiple cases, current and former US officials say. Most important, he delivered something the FBI and US intelligence agencies had made one of their highest priorities: a look inside Russian hacking and cyber operations when concerns over those activities were running at an all-time high.

Shalon was handsomely rewarded for his efforts. Charged with 33 federal counts, including hacking, securities fraud and money laundering, he faced decades in a federal prison. Instead, he spent just 10 months in a New York jail before moving into a seven-bedroom house in Queens, along with his wife and four daughters. He worked from there with an FBI handler until at least January 2021, when he was sentenced to time served. After vacationing with his family in Miami and Las Vegas, Shalon returned to Israel, where he now lives in an exclusive suburb of Tel Aviv.

Shalon’s relatively brief passage through the US justice system isn’t the end of his legal jeopardy, however. And the running of Shalon, one of the most significant cyber cooperators in American history, now has the potential to turn into a debacle for both the FBI and New York’s Southern District, the most powerful US attorney’s office in the country.

Police in Europe have compiled a trove of evidence putting Shalon at the pinnacle of a massive investor scam that stole millions of euros from victims in Sweden, the UK, Germany and Austria. During the course of reporting this article, *Bloomberg Businessweek* interviewed more than 50 people, including crime victims, Shalon’s criminal associates and law enforcement officials in Europe, the US and Israel. Details of his cooperation were described by 12 current and former US officials, who asked for anonymity because aspects of the case remain sealed. Reporters obtained hundreds of pages of confidential police reports detailing the European investigation, including evidence seized from mobile phones, computers and servers in several countries. The US court filings unsealed in December provided additional information for this story.

Businessweek sent the FBI a detailed list of questions about the Shalon case. A spokesperson said the bureau “is unable to accommodate” *Businessweek*’s “request

respond to numerous requests for comment made to his lawyers in the US and Israel or to a letter delivered to his home.

Veteran FBI agents often say that running cooperators and informants is the most important work they do, because it's the only way to pry open the most hardened criminal organizations. It's also high risk, because so much can go wrong.

Although Shalon's business with the US government appears to be over, the officials who oversaw the case now face questions—in particular from European law enforcement agencies as they consider their own case against the now 40-year-old Israeli. The details of the case add fresh fuel to concerns about the way the American system of justice commodifies guilt, exchanging criminal punishment for aid with higher investigative priorities. And thousands of European victims will have questions of their own, about how a mastermind of their woes operated so freely on the US government's watch.

The more value Shalon demonstrated, the more he gained the trust of his handlers—and the more freedom he was given

WHEN, IN THE SUMMER OF 2015, ISRAELI AND AMERICAN AGENTS SHOWED UP AT Shalon's gated house in Savyon—a Tel Aviv suburb known as Israel's Beverly Hills—they found $500,000 in cash, multiple fake passports and a bevy of encrypted computers and digital devices. After his arrest, the Americans demanded that Shalon hand over the device passwords to unlock what they believed would be a trove of valuable evidence linking him to the Wall Street hacks. Shalon calmly declined, and the agents told him they'd see him in New York.

As he sat in an Israeli jail for weeks, the likelihood of decades in prison ahead of him, he made what he later described to agents as a straightforward business calculation. In late 2015 his Israeli lawyer, Yaniv Segev, contacted US officials and signaled that his client was willing to cooperate with US law enforcement to avoid a lengthy prison sentence. It didn't take long for the New York-based team of agents and prosecutors to figure out what they had.

Shalon's quick rise through the world of cybercrime was propelled by built-in advantages. He was born in 1984 in the then-Soviet republic of Georgia, according to Israeli court records, and spent part of his childhood in Russia during the tumultuous years after the collapse of the Soviet Union. It was an era when the Georgian underworld thrived in Russia, and Georgians ran casinos and gaming operations in St. Petersburg just as Vladimir Putin was establishing his base of power in the city.

Shalon's father, Shota Shalelashvili, managed a workers cooperative during Soviet times, but by 1991 he'd become vice president of a Moscow bank called Progressbank, according to a résumé posted online. In 2005, Shalelashvili was convicted by an

Reached by phone, Shalelashvili declined to comment.

Shota Shalelashvili, Shalon's father. *Photo illustration: 731; Source: Creative Commons*

By the time the family emigrated to Israel in the late 1990s, they were rich. As a teenager, Shalon spent much of his time playing tennis, according to acquaintances. He attended elite sports academies in Switzerland and Spain and continued to exercise obsessively long after he stopped dreaming of turning pro. His size and athleticism could be physically intimidating, say people who worked with him later.

In his early 20s, according to court records, Shalon teamed up with notorious Russian spammers who would send millions of emails to promote fake pharmaceuticals and pirated software. With enough email addresses, they were almost guaranteed a certain percentage of conversions, or paying customers—a lucrative business model known in Russian as *partnerka*.

Shalon took what he learned and innovated. He created illegal gambling sites and built massive datasets to target potential customers, in some cases hiring hackers to steal the lists of his competitors, according to the US indictment. He updated old-school money laundering techniques for the cyber age: He created companies to process card payments for gambling sites and malware scams and moved the profits into the legitimate financial system by bribing bank officials in Azerbaijan and elsewhere, according to the indictment and former US officials familiar with the case. Because he sold those services to cybercriminals around the world, Shalon possessed

three days. He included an offer that would turn into a major test of his value.

Joshua Aaron, Shalon's American partner in the JPMorgan hack, had fled to Russia before agents could arrest him. An FBI wanted poster, topped with a photo of a smiling Aaron taken from social media, described the former Florida State University frat brother as the scheme's "front man." Agents believed Shalon had helped Aaron escape to Russia. Now he was offering to get him back, according to three people familiar with the Israel meetings, including Segev, Shalon's lawyer at the time.

A wanted poster for Joshua Aaron, Shalon's American partner in the JPMorgan hacks. Shalon helped the Americans get Aaron out of Russia to be tried in the US. *Photo illustration: 731; Source: FBI*

Russia is a notorious haven for fugitives, including the likes of Edward Snowden, who leaked a trove of US classified secrets, among others. US officials doubted there was much Shalon could do. Yet in May 2016, Moscow police arrested Aaron and charged him with immigration crimes. Seven months later, he was on a commercial flight to the US.

Segev, who represented Shalon during his negotiations with US law enforcement but is no longer his attorney, says the family had orchestrated Aaron's return using its considerable influence in Russia—amplified in this instance by cash. "Shota started an international operation that included bribing some of the officials in Russia," Segev says, referring to Shalon's father.

Depending on the details, that arrangement could violate Justice Department

says. Under most circumstances, “hey can’t commit crimes or violate laws to advance the government’s interests.”

Shalon’s career as an elite US cooperator had begun.

ONE OUTCOME OF THOSE MEETINGS IN ISRAEL WAS THAT SHALON AGREED TO extradition. By June 2016 he was in a New York jail and working actively with the FBI. The information he provided to agents proved to be highly valuable and was shared with US intelligence agencies, four current and former US officials say.

Among the early targets was Peter Levashov, a Russian hacker who ran a global network of zombie computers known as the Kelihos botnet. Botnets are useful in various criminal schemes, and Levashov had been on the FBI’s target list for years. Shalon provided his handlers with deep insight into Levashov and his operations, according to a person familiar with the case, and was also critical in helping authorities track Levashov to Barcelona, where he was arrested in April 2017 by Spanish police.

The more value Shalon demonstrated, the more he gained the trust of his handlers—and the more freedom he was given. Three weeks after Levashov’s arrest, Shalon left jail and moved with his family to a neighborhood of mostly Orthodox former Soviet Jews in Flushing, Queens. His mother, who’s also listed as an owner of some companies associated with her son, paid the $7 million bail.

Shalon wasn’t a particularly talented hacker for an elite cybercriminal—but he didn’t need to be. In 2007 he encountered a Russian named Andrei Tyurin in an online criminal forum and immediately recognized his talent. US officials describe Tyurin as one of the most skilled hackers they’ve ever encountered. It was Tyurin who executed the JPMorgan hack in 2014; he moved through the bank’s heavily protected networks for three months undetected, which led the bank’s security team initially to conclude they were being attacked by a foreign government. The Shalon-Tyurin partnership was particularly nefarious from the point of view of the US consumer—it resulted in the theft of data on nearly a third of all Americans.

Tyurin knew that Shalon had been arrested by the FBI, but Shalon managed to convince his long-time partner that he’d quickly been given his freedom after the US seized $414 million from Shalon in mid-2017. In December of that year, Tyurin agreed to meet Shalon in Georgia to discuss renewing their business relationship. He never made it out of the airport. Tyurin was arrested by Georgian authorities and extradited to the US, where he’s now serving a 12-year sentence for his role in the hacks.

Current and former officials familiar with the case describe Shalon’s level of cooperation with a series of superlatives. Choi called him “an exemplary cooperating witness” in an unsealed court filing; another official says he was one of the

dozen individuals, three people familiar with the situation say.

In February 2018, Shalon's house arrest was lifted, and he was allowed to move freely around New York from 8 a.m. until 8 p.m., court records show. Conditions of his bail restricted his access to the internet without monitoring, but one person familiar with the case says enforcement was largely based "on the honor system."

The family's seven-bedroom faux-stone house had a gym where Shalon worked out. His daughters went to a yeshiva a few blocks away. In 2019 he was even allowed to see a Park Avenue plastic surgeon. The unspecified procedure appears in court files, because it required removal of Shalon's GPS monitoring device while he was under anesthesia.

"He was very nice," says Sonya Suyunov, a neighbor who ran a tailor shop out of her house two doors down from Shalon. "I did alterations for him many times. He had a beautiful wife and four beautiful girls. I did dresses for them, and he'd bring in suits—very expensive suits, Gucci." Suyunov says she had no idea about Shalon's double life or the secrets he kept. She wasn't the only one.

"It's a risk that I'm talking about him, you have to understand"

IN JANUARY 2019 A GERMAN SERIAL SCAMMER NAMED UWE LENHOFF WAS ARRESTED AT a resort in the Tyrolean Alps and charged with running a massive investment fraud in Austria and Germany. According to police, Lenhoff made millions by flooding Facebook with ads touting investments in exotic financial instruments, particularly binary options, and persuading small investors to sign onto fake trading websites, into which they poured their savings. When they tried to get their money back, Lenhoff and his army of "brokers" simply disappeared.

The heart of the scam was an Eastern European call center staffed by young Israelis and Europeans. Police say that the trading websites were a sham—no trades took place—and that the call center employees were the equivalent of actors trying to get naïve investors to transfer money they had no chance of getting back. The 2019 arrests, which, in addition to Lenhoff, included more than a dozen people, stemmed from a massive two-year investigation. German and Austrian police had found call centers running identical scams in Ukraine, Georgia, Bulgaria, Serbia and Bosnia. A common element among many of them was a company called Tradologic, which police came to view as a turnkey solution for investor fraud. For a cut of the profits, Tradologic provided a technology suite, shell companies, offshore bank accounts and a massive marketing apparatus targeting tens of thousands of victims in Austria, Germany, Britain and Scandinavia.

Unlike some of the other detainees, Lenhoff was happy to cooperate, and he told police in Vienna something surprising, according to a transcript seen by *Businessweek*. Obscured beneath layers of partners and frontmen, a controlling force behind

The Europeans were certainly aware of Shalon. He'd been arrested by the FBI. Yet by Lenhoff's account, Shalon was still managing his illicit businesses from a new base in the US. Lenhoff had even flown to New York in 2018 to meet with Shalon, to get to know him better and talk business. "He wanted me to help him get a casino license via Malta," Lenhoff told police. "He also wanted to establish Tradologic in the USA."

Illustration: Ard Su for Bloomberg Businessweek

While American prosecutors portray Shalon as a model cooperator, a completely different picture emerges in hundreds of pages of investigative documents and evidence from Europe. By seizing the phones, computers and servers of Shalon's alleged partners in crime in Europe, investigators tapped into months of texts and digital chats showing the US cooperator feuding with rivals, settling scores and ensuring that he got his rightful share of profits from a massive and ongoing criminal operation.

"Gery knew everything. He controlled everything," said Tal-Jacki Fitelzon, an Israeli who managed sales operations for call centers in Bulgaria and Georgia. Fitelzon spoke in 2023 from a prison in Munich, where he was serving a nearly seven-year sentence for his role in the scam. He recalled taking part in Skype calls when Shalon was in New York, and he said Shalon involved himself in the smallest details of running the business: He used to sift through Tradologic data to figure out how well-off particular investors were and which ones could be bled for more money, then forward the names to managers.

still scared him: “It’s a risk that I’m talking about him, you have to understand.”

As police in Europe learned more about how the call centers functioned, they learned more about Shalon. Tradologic was founded in 2009 by an Israeli named Ilan Tzorya, who took a big infusion of cash from Shalon in 2013. Associates tend to characterize Shalon as ruthlessly ambitious—a businessman who takes over whatever he invests in—and Tzorya was quickly relegated to the role of junior partner.

Illustration: Ard Su for Bloomberg Businessweek

As Shalon sat in jail in Israel and then New York, Tzorya tried to reassert control over the business—or at least that’s what Shalon believed, as seen in text messages and group chats seen by *Businessweek*. Explaining the feud at one point over WhatsApp, Shalon told a potential business partner that “Ilan was not there for me. When I was gone he took my employs he took my ideas he took my money and i had a baby girl born and he didn’t even help my family.” (Except for clarifying punctuation, texts are reproduced here as they were originally written, including spelling and syntax errors.) Once his house arrest was lifted, Shalon appears to have spent a good deal of his time and energy settling the score.

He started by cutting off the payments that Tradologic regularly made to Tzorya as one of the company’s managing partners. “I canceled hes salary ... and I stop dividents,” Shalon wrote to Lenhoff on April 17. “This f---er doing to much fraud on us and using our names to build hes own businesses.”

around the New York area. To business partners, Shalon claimed "to have the FBI wrapped around his little finger," according to one former associate, who asked not to be named out of fear for his safety. The associate says Shalon used his relationship with US law enforcement as a cudgel against both friends and enemies.

Shalon's main worry seemed to be maintaining the flow of millions of euros from the European scams, which the feud made increasingly difficult. After Tzorya resigned from Tradologic in the summer of 2018, Shalon worked furiously to contain the fallout, his communications with associates show: He instructed lieutenants to prevent Tzorya from accessing customer information and ordered a Tradologic executive to transfer the company's remaining cash into Bitcoin "due to Ilan's threats and illegal moves toward the company."

Throughout the rest of 2018, Shalon and Tzorya fought. Tzorya leaked damaging information about the fraud and its underlying operations to a Vienna-based website called FinTelegram News, which publishes leaked information on financial scammers. In return Shalon dispatched a key lieutenant, an Israeli named Gal Barak, to Vienna with a counteroffer for FinTelegram's publisher, Werner Böhm, according to an account Böhm later gave police. In a meeting at Le Méridien Vienna hotel, Barak proposed that the remaining Tradologic partners set up a €3 million ($3.5 million) investment fund over which Böhm would have control, with the idea that he use the money to invest in startups across Europe on behalf of the group. The next day, Böhm, Shalon and Barak got on a WhatsApp chat to confirm the details. "I know Gal would told you, when we are partners and do things we share all problems and help each other no matter what," Shalon told the publisher, according to a copy of the encrypted chat seen by *Businessweek*.

Shalon told Böhm the deal came with no strings attached, but he'd been more transparent with Lenhoff the month before. "I have also budget...big one to kill this bs stories," Shalon told him in a WhatsApp chat captured by police. Shalon wasn't the only one hiding his real motive: Böhm by then was cooperating with the Austrian police, who secretly listened in on both the hotel rendezvous and a later meetup at a beer hall, according to interviews and police documents.

The curtain was about to come down on much of the European operation. In late January 2019, police raided the Bulgarian call center and arrested key managers across Europe, including Barak and Lenhoff. But in the heady days before the raid, Shalon invited Böhm to meet in New York so they could get to know each other in person.

"NY amazing for business," he texted him. Then he added a smile.

OF ALL THE VALUE SHALON PROVIDED TO THE US GOVERNMENT, HIS KNOWLEDGE OF Russia's hacking scene and its cyber operations was his biggest potential payoff as a

administration, even as the probe into Russia's meddling in the 2016 presidential election began to heat up. US officials believed Shalon could fill in some of the gaps. And although the details remain secret, five current and former officials familiar with the case say that in important ways he did.

There's another way to look at it, though: Prosecutors overseeing the case traded away substantial jail time for Shalon in return for something they wanted more.

"You might get something by using an informant that seems valuable, but you are accepting that other crimes might be committed. I would say that is baked into the American system of cooperation," says Alexandra Natapoff, a Harvard law professor, former federal public defender and author of *Snitching: Criminal Informants and the Erosion of American Justice*. "The entire institution is designed to commodify guilt."

> Prosecutors "know that they can't trust their cooperators. The question is why they do it anyway"

Natapoff has studied the use of cooperating witnesses for two decades. Cooperators' cases are so shrouded in secrecy that it's impossible for anyone but a few insiders to evaluate whether justice has been served, she says. The arrangement is often based on a trust relationship between handler and snitch, even though one side is typically a sophisticated criminal adept at lying. Prosecutors "know that they can't trust their cooperators," Natapoff says. "The question is why they do it anyway."

One former veteran FBI agent connected to the case was more blunt: "I'd say the majority of cooperators go sideways. You know that moral imperative isn't there."

The secrecy shrouding the US hacking case puzzled the European investigators as they homed in on Shalon beginning in 2019. Police in Austria and southern Germany spent months combing through evidence seized in the call center raids and interviewing dozens of people involved, and there was a lot to show that Shalon was deeply enmeshed. They knew he was apparently still in New York. But there had yet to be a trial, and just about everything regarding his case remained under seal. Getting a clear understanding of Shalon and his activities was complicated by the fact that, similar to an undercover agent, cooperators in the US are permitted to engage in criminal activity under certain conditions—something known to every federal prosecutor and FBI agent as "otherwise illegal activity," or OIA. Officials say the value of undercover cooperators often depends on their ability to interact convincingly with other criminals, and that sometimes entails committing crimes, although under specific conditions.

Cooperators need warrants and subpoenas to rifle other people's computers, for example, just as an agent does. And law enforcement officials must find ways to mitigate harm to victims. Shalon's handlers would also have needed explicit approval

"Which is worse? To think that our law enforcement is incredibly cynical and willing to let this guy commit these crimes while he's cooperating? Or that they were negligent or naïve and didn't know any of this was going on?" says Bruce Green, a former federal prosecutor and director of the Louis Stein Center for Law and Ethics at Fordham University, after *Businessweek* described the investigation in Europe. "Either is pretty shocking."

It's clear that American officials didn't remain in the dark: In mid-2022, police in Europe informed their counterparts in the FBI of the investigation involving Shalon and asked for information about his status, according to two people with knowledge of the communications. Given their close relationship, that notice normally would have resulted in the two sides working together. In this case, the Americans provided some basic information but said they were unable to share most details about Shalon or his activities.

When he was finally sentenced to time served in New York in January 2021, prosecutors vouched for the extraordinary value of Shalon's cooperation and his honesty in dealing with the government, according to the recently unsealed transcript of the hearing. (Including his detention in Israel, Shalon spent a total of 21 months in jail.)

"You have spent the last several years demonstrating that you now wish to help right wrongs, rather than engage in criminal activity," Chief District Judge Laura Taylor Swain told Shalon at that hearing. "And that is why I am confident that you have moved away from your criminal past and are capable of directing your energies exclusively to lawful, positive behavior that will benefit society for the rest of your life."

> "I trusted him. I thought maybe he'll help me because no one can be so cruel. But he was so cruel"

AT LEAST SOME OF SHALON'S ENERGY ALLEGEDLY WENT INTO VICTIMIZING PEOPLE such as Ute Schramke, a 63-year-old horse trainer who lives near the north German town of Paderborn. She'd worked long hours for years, sometimes flying to other countries for training sessions, and her health had recently begun to suffer. In 2017 she was looking for ways to replace lost income and knew some of her wealthy clients had made money in Bitcoin, so she googled it to find out more. Within a day or two, she got a call out of the blue from a man who referred to himself as James Morra. As Schramke would later find out, Morra's real name was Dimitar Moraliyski, and he was phoning not from an office in London, as he claimed, but from a call center in Belgrade. He was part of Gal Barak's crew.

Looking back, Moraliyski seemed to have a nose for her vulnerabilities, Schramke

supposed trades and stopped taking his calls. Then her mother died, and Moraliyski called again. Schramke was shattered by the loss of her mother and didn't have enough money to buy the house she'd grown up in, with a garden she and her mother had tended for decades. She gave Moraliyski another chance.

Scammers convinced Ute Schramke they were investing her modest savings. Instead, they took it all. *Photo illustration: 731; Photo: Simona Weinglass*

By the time Moraliyski disappeared for good weeks later, Schramke had lost €24,000. She was forced to sell her home and now lives in a small apartment above a shop. She fell into depression, she says, and even contemplated suicide at one point. "I trusted him. I thought maybe he'll help me because no one can be so cruel. But he was so cruel," she says.

The scammers left those kinds of scars all across Europe. About 30,000 people lost money to Lenhoff and his faux brokers through mid-2018, according to a client list obtained by police, and tens of thousands more victims were ripped off through other Tradologic-connected call centers. The nine centers run by Barak alone defrauded victims in Europe of at least €120 million before they were shut down, while criminal organizations using the Tradologic platform stole nearly €1 billion in all, investigators say.

European police believe Shalon's stake in Tradologic and the associated call centers was a big part of his criminal empire, even if their American counterparts largely overlooked it. Prosecutors in Germany and Austria have now obtained convictions

is adjudicated.) Barak got four years. Moraliyski was sentenced to four years and six months.

Lenhoff died under suspicious circumstances while awaiting trial in Germany. He was found lifeless in his cell with multiple toxins in his body, but an investigation didn't find evidence to show a crime had been committed. Of the five leaders of the operation named in a confidential 2020 report by Austrian police, Shalon and his Russian partner, a notorious spammer who now uses the name Vladislav Smirnov, are the only ones who have yet to be formally charged.

Nino Goldbeck, chief public prosecutor at the Central Office for Cybercrime Bavaria, leads Germany's investigation into the call center scams. *Photo illustration: 731; Photo: Ben Kilb/Bloomberg*

That could change soon, however. Two European law enforcement officials, who asked for anonymity to describe internal deliberations, say a decision on whether to charge Shalon will be made by prosecutors in Germany in the next few months. That prosecution would likely use evidence gathered by Austrian police as well. If European authorities do go after the famous hacker, they'll first have to get him out of Israel. German prosecutors have already spent more than two years fighting to extradite several other Israelis charged in similar scams, including Shalon's brother-in-law, David Bar-El.

Shalon now divides his time between an office in Herzliya, where he runs an online gambling business called OX Gaming, and his mansion in Savyon. He acquired a stake in OX Gaming in November 2017, just a few months after getting bail, an Israeli lawsuit

Rudolph, who's suing Shalon over back compensation, says OX Gaming operates "in a gray area," soliciting gamblers in countries that don't recognize the company's Curaçao-based gaming license, for instance. She also got the impression that Shalon is involved in lots of other projects. "Where does Gabi's empire begin, and where does it end?" she says, referring to Shalon by the nickname his family and friends use. "I don't think there is anyone who knows."

As for his time in America, Shalon isn't much the worse for it, says Aharon Chein, a rabbi who was close to Shalon and his family during their time in New York and was among only a handful of people there who knew why Shalon was really in the US. The $400 million the Justice Department managed to seize from him? "That's what they were able to find," Chein says. "He knows how to hide it."

Sitting in the basement of the Georgian Jewish synagogue in Flushing recently, Chein speaks admiringly of the man he knew as generous and devout. Shalon was no friend of the FBI, he says, whatever he told them. He considered his handlers "the enemy."

"Gery Shalon is one of the smartest people I've ever met," the rabbi says. "He's not a real criminal, but he knew how to break the system and make some money." *–With Steven Arons, Helena Bedwell and David Voreacos*