United States Department of Justice

THE UNITED STATES ATTORNEY'S OFFICE
SOUTHERN DISTRICT of NEW YORK

U.S. Attorneys » Southern District of New York » News » Press Releases

Department of Justice

U.S. Attorney's Office

Southern District of New York

FOR IMMEDIATE RELEASE Tuesday, November 10, 2015

Attorney General And Manhattan U.S. Attorney Announce Charges Stemming From Massive Network Intrusions At U.S. Financial Institutions, U.S. Brokerage Firms, A Major News Publication, And Other Companies

Loretta E. Lynch, the Attorney General of the United States, Preet Bharara, the United States Attorney for the Southern District of New York, Diego Rodriguez, Assistant Director-in-Charge of the New York Field Office of the Federal Bureau of Investigation ("FBI"), and Robert J. Sica, Special Agent in Charge of the US Secret Service New York Field Office ("USSS") announced today the unsealing of a superseding indictment charging GERY SHALON, a/k/a "Garri Shalelashvili," a/k/a "Gabriel," a/k/a "Gabi," a/k/a "Phillipe Mousset," a/k/a "Christopher Engeham," with orchestrating massive computer hacking crimes against U.S. financial institutions, brokerage firms, and financial news publishers, including the largest theft of customer data from a U.S. financial institution in history (the "U.S. Financial Sector Hacks"). SHALON is charged with committing these crimes with JOSHUA SAMUEL AARON, a/k/a "Mike Shields," in furtherance of securities market manipulation schemes that SHALON and AARON perpetrated with defendant ZIV ORENSTEIN, a/k/a "Aviv Stein," a/k/a "John Avery" in the United States. As alleged, SHALON also orchestrated computer network hacks and cyberattacks in furtherance of other major criminal schemes, including unlawful internet casinos and illicit payment processors which SHALON operated with ORENSTEIN. SHALON also owned and controlled an illegal U.S.-based Bitcoin exchange known as Coin.mx. SHALON and ORENSTEIN were arrested in July 2015 by the Israel Police on an indictment that charged the underlying securities fraud, and they remain in custody in Israel pending extradition on those charges. The United States Attorney's Office will seek their extradition to stand trial in the United States on the additional charges announced today. AARON remains at large. Also announced today is the unsealing of a separate indictment charging ANTHONY R. MURGIO with operating Coin.mx in the United States, and related crimes. MURGIO, who was arrested on a Complaint in July 2015, will be arraigned before the Honorable Alison J. Nathan.

Attorney General Loretta E. Lynch said: "As set forth in the indictment, these three defendants perpetrated one of the largest thefts of financial-related data in history –

making off with the sensitive information of literally thousands of hard-working Americans. These charges were made possible in large part because those victims came forward and worked with the Department of Justice to hold the perpetrators accountable. In an age when enormous quantities of vital information are stored in digital format on potentially vulnerable Internet-connected devices, public-private partnerships and information-sharing are more critical than ever. The Department of Justice is committed to protecting the financial data of all our citizens and the financial integrity of our institutions. I'd like to thank the prosecutors and law enforcement professionals who worked tirelessly on this case, and the victims who offered their full cooperation with law enforcement to make these criminal charges possible."

Manhattan U.S. Attorney Preet Bharara said: "Today, we have exposed a cybercriminal enterprise that for years successfully and secretly hacked into the networks of a dozen companies, allegedly stealing personal information of over 100 million people, including over 80 million customers from one financial institution alone. The charged crimes showcase a brave new world of hacking for profit. It is no longer hacking merely for a quick payout, but hacking to support a diversified criminal conglomerate. This was hacking as a business model. The alleged conduct also signals the next frontier in securities fraud – sophisticated hacking to steal nonpublic information, something the defendants discussed for the next stage of their sprawling enterprise. Fueled by their hacking, the defendants' criminal schemes allegedly generated hundreds of millions of dollars in illicit proceeds. Even the most sophisticated companies – like those victimized by the hacks in this case – have to appreciate the limits of their ability to uncover the full scope of any cyber-intrusion and to stop the perpetrators before they strike again. If they have been hacked, most likely others have been as well, and even more will be. The best bet to identify, stop and punish cybercriminals is to work closely, and early, with law enforcement. That happened here, and today's charges are proof of that."

FBI Assistant Director-in-Charge Diego Rodriguez said: "Shalon, Aaron, and their co-conspirators allegedly robbed victim companies, often for months at a time, stealing the contact information of tens of millions of customers. They cloaked themselves in secrecy, but their methods rivaled those of the traditional masked robber. Today's indictment sheds light on an increasingly complex threat. But just as criminals continue to develop relationships with one another in order to advance their objectives, the law enforcement community has developed a collaborative approach to fighting these types of crimes."

USSS Special Agent in Charge Robert J. Sica said: "This investigation is indicative of the sophistication and complexity of cybercrime and the transnational criminal organizations that are responsible for it. Transnational cybercriminal organizations operate with impunity regardless of national borders as these criminal organizations seek to profit from information stolen through the unauthorized access to victims' networks. Through the U.S. Secret Service global network of Electronic Crimes Task Forces, our field offices located overseas, and the close cooperation of our foreign law enforcement partners, no cybercriminal is beyond our reach. We will remain relentless in pursuing these criminals wherever they may reside."

According to the allegations contained in the superseding indictment[1]:

From approximately 2012 to mid-2015, SHALON, working with AARON and others, orchestrated the U.S. Financial Sector Hacks, stealing personal information of over 100 million customers of the victim companies. Among these, their network intrusion at one bank ("Victim-1") resulted in the theft of personal information of over 80 million Victim-1

customers, making it the largest theft of customer data from a U.S. financial institution in history. SHALON, AARON, and their co-conspirators engaged in these crimes in furtherance of other criminal schemes. In particular, in an effort to artificially manipulate the price of certain stocks publicly traded in the United States, SHALON and his co-conspirators sought to market the stocks, in a deceptive and misleading manner, to customers of the victim companies whose contact information they had stolen in the intrusions.

In addition to directing the U.S. Financial Sector Hacks, SHALON directed computer network hacks and cyberattacks against numerous companies outside of the financial sector. SHALON and his co-conspirators engaged in these crimes in furtherance of large-scale criminal businesses that SHALON and ORENSTEIN operated in the United States and other countries. In particular, between approximately 2007 and July 2015, SHALON owned and operated unlawful internet gambling businesses in the United States and abroad; owned and operated multinational payment processors for illegal pharmaceutical suppliers, counterfeit and malicious software ("malware") distributors, and unlawful internet casinos; and owned and controlled Coin.mx, an illegal United States-based Bitcoin exchange that operated in violation of federal anti-money laundering laws. Nearly all of these schemes, like SHALON's securities market manipulation schemes, relied for their success on computer hacking and other cybercrimes committed by SHALON and his co-conspirators.

Through their criminal schemes, between in or about 2007 and in or about July 2015, SHALON and his co-conspirators earned hundreds of millions of dollars in illicit proceeds, of which SHALON concealed at least $100 million in Swiss and other bank accounts.

SHALON, AARON, ORENSTEIN, and their co-conspirators operated their criminal schemes, and laundered their criminal proceeds, through at least 75 shell companies and bank and brokerage accounts around the world. The defendants controlled these companies and accounts using aliases, and by fraudulently using approximately 200 purported identification documents, including over 30 false passports that purported to be issued by the United States and at least 16 other countries.

The U.S. Financial Sector Hacks

Between approximately 2012 and August 2014, SHALON and a co-conspirator ("CC-1"), working at times with AARON, executed the hacks of the computer networks of Victims 1-9. Among other things, in foreign-language electronic communications, during these hacks, SHALON bragged about the size and scope of his securities market manipulation schemes, and described to CC-1 his use of the stolen data in furtherance of those schemes. SHALON and CC-1 also discussed expanding their network intrusions to encompass thefts of material non-public information from the financial institutions and other firms they were hacking.

The Securities Market Manipulation Schemes

Since 2011, SHALON, AARON, ORENSTEIN, and their co-conspirators orchestrated multimillion-dollar stock manipulation – or "pump and dump" – schemes to manipulate the price and trading volume of dozens of publicly traded microcap stocks ("penny stocks") in order to enable members of the conspiracy to sell their holdings in those stocks at artificially inflated prices. In some instances, SHALON and AARON caused the companies to become publicly traded in furtherance of the scheme. To do so, SHALON caused privately held companies to engage in "reverse mergers" with publicly traded

shell corporations SHALON controlled. ORENSTEIN managed bank and brokerage accounts used in furtherance of the schemes under aliases that ORENSTEIN supported with false passports and other false personal identification information.

To artificially manipulate the trading volume and prices of dozens of stocks, among other things, at pre-arranged times, SHALON and AARON disseminated materially misleading, unsolicited messages by various means – including by email ("spam") to up to millions of recipients per day – that falsely touted the stock in order to trick others into buying it. SHALON and AARON engaged in the U.S. Financial Sector Hacks in part to acquire email and mailing addresses, phone numbers, and other contact information for potential victims to whom they could send such deceptive communications. SHALON and his co-conspirators generated tens of millions of dollars in unlawful proceeds from the securities market manipulation schemes.

The Unlawful Internet Gambling Schemes, Hacks and Cyberattacks

From at least in or about 2007 up to and including in or about July 2015, SHALON, ORENSTEIN and their co-conspirators operated unlawful internet casinos in the United States and elsewhere through hundreds of employees in multiple countries. In the United States, the defendants knowingly operated at least 12 unlawful internet casinos (the "Casino Companies") which, through their websites, offered real-money casino gambling in violation of federal law and the laws of numerous states, including New York State. Through the Casino Companies, SHALON, ORENSTEIN, and their co-conspirators generated hundreds of millions of dollars in unlawful income.

In furtherance of his unlawful internet gambling schemes, SHALON and his co-conspirators engaged in massive hacks and cyberattacks against other internet gambling businesses to steal customer information, secretly review executives' emails, and cripple rival businesses. For example, SHALON orchestrated network intrusions of Victims-10 and -11, companies that provided operating software to SHALON's internet casinos. In doing so, SHALON sought to, and did, secretly obtain access to the email accounts of senior executives at both companies to ensure that the companies' work with SHALON's competitors did not compromise the success of SHALON's unlawful internet gambling businesses.

The Illicit Payment Processing Scheme and Hack

From at least in or about 2011 until in or about July 2015, SHALON, ORENSTEIN, and their co-conspirators operated IDPay and Todur, multinational payment processors for criminals who sought to receive payments by credit and debit card in furtherance of their unlawful schemes. Through these payment processors, SHALON, ORENSTEIN, and their co-conspirators knowingly processed credit and debit card payments for, at a minimum, unlawful pharmaceutical distributors, purveyors of counterfeit and malicious purported "anti-virus" computer software, their own unlawful internet casinos, and Coin.mx, an illegal United States-based Bitcoin exchange owned by SHALON. In doing so, SHALON, ORENSTEIN, and their co-conspirators knowingly processed hundreds of millions of dollars in transactions for criminal schemes, for which they earned a percentage of every transaction.

Beginning in or about 2012, SHALON and his co-conspirators hacked into the computer networks of Victim-12, a U.S. company which assessed merchant risk and compliance for credit card issuers and others, including by detecting merchants that accepted credit card payments for unlawful goods or services. Thereafter, on an ongoing basis, SHALON

and his co-conspirators monitored Victim-12's detection efforts, including by reading emails of Victim-12 employees, so they could take steps to evade detection by Victim-12 of their unlawful payment processing scheme.

The Unlawful Bitcoin Exchange

From in or about 2013 to in or about July 2015, SHALON knowingly owned Coin.mx, a Bitcoin exchange service, which was operated by MURGIO in the United States at SHALON's direction in violation of federal anti-money laundering ("AML") registration and reporting laws and regulations. Through Coin.mx, SHALON, MURGIO, and their co-conspirators enabled their customers to exchange cash for Bitcoins, charging a fee for their service. In total, between approximately October 2013 and July 2015, Coin.mx exchanged millions of dollars for Bitcoins on behalf of its customers.

* * *

SHALON, 31, of Savyon, Israel, AARON, 31, a U.S. citizen who resides in Moscow, Russia, and Tel Aviv, Israel, and ORENSTEIN, 40, of Bat Hefer, Israel, are charged with the following offenses, which carry the maximum prison terms listed below:

Count	**Defendants**	**Charge**	**Maximum Prison Term**
One	SHALON and AARON	Conspiracy to Commit Computer Hacking	5 years
Two	SHALON and AARON	Computer Hacking	5 years
Three	SHALON and AARON	Computer Hacking	5 years
Four	SHALON, AARON, and ORENSTEIN	Conspiracy to Commit Securities Fraud	20 years
Five	SHALON, AARON, and ORENSTEIN	Conspiracy to Commit Wire Fraud: Securities Market Manipulation Scheme	20 years
Six to Twelve	SHALON, AARON, and ORENSTEIN	Securities Fraud	20 years
Thirteen	SHALON, AARON, and ORENSTEIN	Wire Fraud	20 years

Fourteen	SHALON, AARON, and ORENSTEIN	Identification Document Fraud Conspiracy	20 years
Fifteen	SHALON, AARON, and ORENSTEIN	Aggravated Identity Theft	Mandatory 2 years
Sixteen	SHALON and ORENSTEIN	Unlawful Internet Gambling Enforcement Act Conspiracy	5 years
Seventeen	SHALON and ORENSTEIN	Unlawful Internet Gambling Enforcement Act	5 years
Eighteen	SHALON and ORENSTEIN	Operation of Illegal Gambling Business	5 years
Nineteen	SHALON and ORENSTEIN	Conspiracy to Commit Wire Fraud: Unlawful Payment Processing	20 years
Twenty	SHALON	Conspiracy to Operate an Unlicensed Money Transmitting Business	5 years
Twenty One	SHALON	Operation of an Unlicensed Money Transmitting Business	5 years
Twenty Two	SHALON, AARON, and ORENSTEIN	Money Laundering Conspiracy: Securities Market Manipulation Scheme	20 years
Twenty-Three	SHALON, AARON, and ORENSTEIN	Money Laundering Conspiracy: Internet Gambling and Payment Processing Schemes	20 years

For his alleged conduct, MURGIO, 31, of Tampa, Florida, is charged with the following offenses: (1) conspiracy to operate an unlicensed money transmitting business, which carries a maximum prison term of 5 years; (2) operation of an unlicensed money transmitting business, which carries a maximum prison term of 5 years; (3) conspiracy to make corrupt payments with intent to influence an officer of a financial institution, which carries a maximum prison term of 5 years; (4) making corrupt payments with intent to influence an officer of a financial institution, which carries a maximum prison term of 30 years; (5) conspiracy to commit wire fraud, which carries a maximum prison term of 20 years; (6) wire fraud, which carries a maximum prison term of 20 years; and (7) money laundering, which carries a maximum prison term of 20 years.

The maximum potential sentences in this case are prescribed by Congress and are provided here for informational purposes only, as any sentencing of the defendant will be determined by the judge.

Mr. Bharara praised the investigative work of the FBI and the United States Secret Service, and expressed his sincere gratitude to the Office of the State Attorney of the Israel Ministry of Justice's Department of International Affairs and the Israel National Police, Cyber Unit - Lahav 433, for their support and assistance with the investigation and the ongoing extradition proceedings. He also thanked the SEC, Immigration and Customs Enforcement - Homeland Security Investigations, the Financial Industry Regulatory Authority, the National Credit Union Administration, the Office of International Affairs of the U.S. Department of Justice, and the Financial Services Information Sharing and Analysis Center, which significantly aided the investigation by facilitating information-sharing among the victim institutions.

The prosecution of this case is being overseen by the Office's Complex Frauds and Cybercrime Unit.Assistant U.S. Attorneys Nicole Friedlander, Eun Young Choi, and Sarah Lai are in charge of the prosecution.Assistant U.S. Attorney Edward Diskant of the Office's Money Laundering and Asset Forfeiture Unit is in charge of the forfeiture aspects of the case.

The charges contained in the indictment are merely accusations, and the defendants are presumed innocent unless and until proven guilty.

---

[1] As the introductory phrase signifies, the entirety of the text of the superseding indictment and the description of the indictment set forth herein constitute only allegations, and every fact described should be treated as an allegation.

15-287 USAO - New York, Southern

Download u.s._v_shalon_et_al_indictment_s1.pdf (2.49 MB)
Download u.s._v_anthony_murgio_indictment_s1.pdf (1.74 MB)

Updated November 10, 2015