United States v. Gholamreza Rafatnejad

- Good afternoon. My name is Geoffrey Berman, and I am the United States Attorney for the Southern District of New York.
- Today, in one of the largest state-sponsored cyber-attacks ever prosecuted by the Department of Justice, we have unmasked criminals that normally work in total anonymity, hiding behind the ones and zeros of computer code.
- This massive and brazen cyber-assault on the computer systems of 144 U.S. universities, 176 foreign universities in 21 countries, and dozens of governmental organizations and private sector companies as alleged; this assault was conducted on behalf of the government of Iran's Islamic Revolutionary Guard, also known as the "IRGC."

- As the Indictment alleges, the defendants were the leaders and operators of the Mabna Institute, an Iranian company that conducted this attack at the behest of the IRGC and then sold the illegal fruits of its hacking. The company was set up in 2013 by two of the defendants – Gholamreza Rafatnejad and Ehsan Mohammadi. And while the company's name may sound legitimate, this so-called "*Institute*" was set up for one reason only--to *steal* scientific resources from other countries around the world.
- The defendants' global campaign of cyber attacks operated in three parts: a university campaign, private company hacks, and government and non-governmental entity hacks.

  <u>University Campaign</u>

  - With respect to the University Campaign, from 2013 through 2017, the defendants targeted more than 100,000 accounts of university professors

around the world. And by tricking professors to click on fake links, compromised 8,000 accounts.

- Once they gained access to these accounts, the defendants stole massive amounts of academic data and intellectual property. The universities, combined, had to pay $3.4 billion to access this information – the defendants got it for free.
- They targeted data and research from all fields, including science and technology, engineering, social sciences, medical and other professional fields. In total, they stole at least 31.5 **terabytes** of data – that's about 35 billion pages -- and sent that data back to computers they controlled outside of the United States. And to be clear—this is not just raw data. It is the innovations and intellectual property from our country's greatest minds.

Private Sector

- The second part of the campaign targeted at least 36 private sector companies in the United States and at least 11 companies based in foreign countries, including Germany, Italy, Switzerland, Sweden, and the United Kingdom.
- The hackers targeted firms and companies across sectors – law firms, technology companies, consulting companies, financial services firms, health care companies, biotechnology companies, and others.
- Once they gained access, the defendants, among other things, stole entire email mailboxes from the victims. They even set up rules in the stolen accounts to secretly forward all new emails to the defendants.

U.S. Government and NGO Victims

- The third, and perhaps the most troubling, part of the hacking campaign targeted U.S. government and non-governmental organizations.
- Among their victims: the U.S. Department of Labor, the United Nations, and even the Federal Energy Regulatory Commission, which is the agency that regulates the interstate transmission of electricity, natural gas, and oil. That agency has the details of some of the most sensitive infrastructure in the United States.

- We believe that all nine defendants are currently in Iran. And I have a message for them, and for others that attempt to harm our country through cyber assaults - We have worked tirelessly to identify you, and you cannot hide behind a keyboard half a world away and expect not to be

held to account. Together with our law enforcement partners, we will work relentlessly and creatively to apply the legal tools at our disposal to unmask and charge you. We will do all we can to bring you to justice.

- While these defendants remain at large, they are now fugitives from the American judicial system. These defendants are no longer free to travel outside Iran without risk of being arrested. They cannot leave Iran to conduct business. The only way they will see the rest of the world is through their computer screen, but stripped of their greatest asset – anonymity. And the memory of American law enforcement is long – we will not forget, and we will do all we can to bring you to justice.
- Do not forget—at the crux of this case is the fact that the *government of Iran* systematically and methodically hacked into the cyber-systems of our country, with the intent to

steal as much information as possible. But as clever as these alleged criminals thought they were, they were ultimately detected and identified by the most sophisticated, capable, and advanced law enforcement in the world. In that regard, I want to thank the FBI, represented here by Bill Sweeny, Assistant Director in Charge of the New York Field Office. Their work in this case has been extraordinary and we are very lucky to have them as partners.

- I also would like to thank the prosecutors in my Office who investigated and prosecuted this case: our Criminal Division Chief, Lisa Zornberg, for her leadership and expertise; the Co-Head of our Complex Frauds and Cybercrime Unit, Timothy Howard, AUSAs Jonathan Cohen and Richard Cooper as well as the other Co-Head of

our Complex Frauds and Cybercrime Unit, Michael Ferrara.