UNITED STATES ATTORNEY'S OFFICE
Southern District of New York

U.S. ATTORNEY PREET BHARARA

FOR IMMEDIATE RELEASE
Tuesday, December 27, 2016
http://www.justice.gov/usao/nys

CONTACT: U.S. ATTORNEY'S OFFICE
James Margolin, Dawn Dearden,
Nicholas Biase
(212) 637-2600

FBI
Martin Feely, Adrienne Senatore,
Kelly Langmesser, Amy Thoreson
(212) 384-2100

MANHATTAN U.S. ATTORNEY ANNOUNCES ARREST OF MACAU RESIDENT AND UNSEALING OF CHARGES AGAINST THREE INDIVIDUALS FOR INSIDER TRADING BASED ON INFORMATION HACKED FROM PROMINENT U.S. LAW FIRMS

Iat Hong Arrested On December 25 In Hong Kong On U.S. Insider Trading and Hacking Charges; In Addition to Successful Cyber Intrusions into Two Law Firms, Defendants Charged with Attempting to Hack into Total of Seven Law Firms

Preet Bharara, the United States Attorney for the Southern District of New York, and William F. Sweeney Jr., the Assistant Director-in-Charge of the New York Field Office of the Federal Bureau of Investigation ("FBI"), announced the arrest of IAT HONG and the unsealing today of a 13-count superseding indictment charging HONG, BO ZHENG, and CHIN HUNG (the "Defendants"). The Defendants are charged with devising and carrying out a scheme to enrich themselves by obtaining and trading on material, nonpublic information ("Inside Information"), exfiltrated from the networks and servers of multiple prominent U.S.-based international law firms with offices in New York, New York (the "Victim Law Firms"), which provided advisory services to companies engaged in corporate mergers and acquisitions ("M&A transactions"). The defendants targeted at least seven law firms as well as other entities in an effort to unlawfully obtain valuable confidential and proprietary information. HONG, a resident of Macau, was arrested on these charges on December 25, 2016, in Hong Kong and is now pending extradition proceedings. HONG was presented for an initial appearance on December 26, 2016, before a Judge in Hong Kong and is expected to have his next court appearance on January 16, 2017.

As alleged, from April 2014 through late 2015, the Defendants successfully obtained Inside Information from at least two of the Victim Law Firms (the "Infiltrated Law Firms") by causing the networks and servers of these firms to be hacked. Once the Defendants obtained access to the law firms' networks, the Defendants targeted email accounts of law firm partners who worked on high-profile M&A transactions. After obtaining emails containing Inside

Information, the Defendants purchased stock in the target companies of certain transactions, which were expected to, and typically did, increase in value once the transactions were announced. The Defendants purchased shares of at least five publicly-traded companies before public announcements that those companies would be acquired, and sold them after the acquisitions were publicly announced, resulting in profits of over $4 million. In each case, one of the two Infiltrated Law Firms represented either the target or a contemplated or actual acquirer in the transaction.

Manhattan U.S. Attorney Preet Bharara said: "As alleged, the defendants – including Iat Hong, who was arrested in Hong Kong on Christmas Day – targeted several major New York law firms, specifically looking for inside information about pending mergers and acquisitions. They allegedly hacked into two prominent law firms, stole the emails of their M&A partners, and made over $4 million in illegal profits. This case of cyber meets securities fraud should serve as a wake-up call for law firms around the world: you are and will be targets of cyber hacking, because you have information valuable to would-be criminals."

FBI Assistant Director-in-Charge William F. Sweeney Jr. said: "The subjects charged in this case allegedly stole nonpublic information through unauthorized access to law firms' computers, and used the information for their own personal gain. The FBI works around the clock to keep these types of alleged securities fraudsters and cyber criminals from trading on stolen information, potentially manipulating the market at the cost of legitimate investors, and harm to corporations."

According to the allegations contained in the superseding indictment (the "Indictment")[1]:

The Law Firm-1 Hack and Insider Trading

At all times relevant to the Indictment, Law Firm-1 was a U.S.-based international law firm with offices in New York, New York, which, among other services, provided advisory services to companies engaged in M&A transactions.

The Contemplated Intermune Transaction

In June 2014, Law Firm-1 was retained by a company not named in the Indictment (the "Company") in connection with a contemplated acquisition of Intermune, a publicly traded U.S.-based drug maker (the "Contemplated Intermune Transaction"). A partner in the M&A group at Law Firm-1 ("Partner-1") was an attorney working on the Contemplated Intermune Transaction.

Beginning on July 21, 2014, the Defendants began exchanging emails concerning, among other things, particular M&A partners at Law Firm-1. In addition, on or about July 29, 2014, HONG emailed HUNG a list of eleven partners at Law Firm-1, including Partner-1.

Also beginning about July 2014, the Defendants, without authorization, caused one of Law Firm-1's web servers (the "Law Firm-1 Web Server") to be accessed by using the unlawfully obtained credentials of a Law Firm-1 employee. The Defendants then caused malware to be installed on the Law Firm-1 Web Server. The access to the Law Firm-1 Web

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

Server allowed unauthorized access to at least one of Law Firm-1's email servers (the "Law Firm-1 Email Server"), which contained the emails of Law Firm-1 employees, including Partner-1.

Between about August 1 and August 15, 2014, Partner-1 was privy to Inside Information about the Contemplated Intermune Transaction. For example, on more than one occasion between August 7 and August 15, 2014, Partner-1 obtained information, including via email, about details of the proposed transaction, including the price per share the Company was considering offering to acquire Intermune.

Between about August 1 and August 9, 2014, the Defendants caused more than 40 gigabytes of confidential data to be exfiltrated from the Law Firm-1 Email Server over the course of at least eight days.

On August 13, 2014, during the time Law Firm-1 was advising the Company on the Contemplated Intermune Transaction and after the Defendants had obtained access to confidential email data maintained at Law Firm-1, HONG used the Inside Information to purchase 7,500 shares of Intermune stock for certain trading accounts (the "Trading Accounts"). Prior to that date, none of the Trading Accounts had purchased any shares of Intermune. Later that day, HONG purchased an additional 1,000 shares of Intermune stock in the Trading Accounts.

On August 16 and 17, 2014, the Defendants exploited their continued unauthorized access to email data belonging to Law Firm-1 by exfiltrating approximately 10 gigabytes of confidential data from the Law Firm-1 Email Server. Between about August 18 and August 21, 2014, HONG and ZHENG used the Inside Information to purchase additional Intermune shares in the Trading Accounts on at least five occasions, totaling an additional 9,500 shares of Intermune stock.

The Contemplated Intermune Transaction was never consummated. Instead, before the market opened on Monday, August 25, 2014, Intermune announced that it had reached an agreement to be acquired by Roche AG, a German company. On that day, Intermune's share price increased by approximately $19 per share, or approximately 40 percent from the closing price on Friday, August 22, 2014, the last prior trading day. That same day, August 25, 2014, the Defendants sold the 18,000 shares that they had begun acquiring twelve days earlier for profits of approximately $380,000.

The Intel-Altera Transaction

In January 2015, Law Firm-1 was retained by Intel Corporation ("Intel"), a publicly traded multinational technology company, in connection with a contemplated acquisition of Altera Corporation ("Altera"), a publicly traded integrated circuit manufacturer (the "Intel-Altera Transaction"). As with the Contemplated Intermune Transaction, Partner-1 was an attorney working on the Intel-Altera Transaction.

Between January and about March 27, 2015, Partner-1 was privy to Inside Information about the Intel-Altera Transaction. On several occasions during this time period, Partner-1 obtained confidential information about the contemplated transaction via email. For example, on

January 29, 2015, Partner-1 received an email with deal terms, including the proposed price per share to purchase Altera.

Between January 13, 2015, in the same month that Law Firm-1 was retained by Intel to advise on the Intel-Altera Transaction, and about February 10, 2015, the Defendants caused approximately 2.8 gigabytes of confidential data to be exfiltrated from the Law Firm-1 Email Server.

Beginning February 17, 2015, during the time Law Firm-1 was advising Intel and after the Defendants had obtained access to confidential email data maintained at Law Firm-1, the Defendants used the Inside Information to purchase shares of Altera stock in the Trading Accounts. Prior to that date, none of the Trading Accounts had purchased any shares of Altera.

To further effectuate their insider trading scheme, between February 17 and March 27, 2015, one or more of the Defendants used the Inside Information to purchase additional shares of Altera stock in the Trading Accounts on at least 26 occasions, ultimately purchasing more than 210,000 shares.

On March 27, 2015, a financial newspaper published an article reporting on confidential merger discussions between Intel and Altera (the "March 27 Newspaper Article"). Following the publication of the article, on March 27, 2015, Altera's share price increased $9 per share, or approximately 26 percent, from Altera's share price on March 27, 2015, just prior to the March 27 Newspaper Article. On April 10 and April 13, 2015, the Defendants sold all of their shares of Altera stock for a profit of approximately $1.4 million.

The Law Firm-2 Hack and Insider Trading

At all times relevant to this Indictment, Law Firm-2 was a U.S.-based international law firm with offices in New York, New York, which, among other services, provided advisory services to companies engaged in M&A transactions.

The Pitney Bowes-Borderfree Transaction

In December 2014, Law Firm-2 was retained by Pitney Bowes Inc., a publicly traded international business services company, in connection with a contemplated acquisition of Borderfree, Inc., a publicly traded e-commerce company headquartered in New York, New York (the "Pitney Bowes-Borderfree Transaction"). A partner in the M&A group at Law Firm-2 ("Partner-2") was an attorney who worked on the Pitney Bowes-Borderfree Transaction.

Beginning about April 7, 2015, after Law Firm-2 had been retained to advise Pitney Bowes, the Defendants, without authorization, caused one of Law Firm-2's web servers (the "Law Firm-2 Web Server"), located in New York, New York, to be accessed by using the unlawfully obtained credentials of a Law Firm-2 employee. The Defendants then caused malware to be installed on the Law Firm-2 Web Server. The malware on the Law Firm-2 Web Server allowed unauthorized access to at least one of Law Firm-2's email servers, also located in New York, New York (the "Law Firm-2 Email Server"), which contained the emails of Law Firm-2 attorneys, including Partner-2.

Between about April 8 and July 31, 2015, the Defendants then caused approximately seven gigabytes of confidential data to be exfiltrated from the Law Firm-2 Email Server over the course of at least six days.

Beginning April 29, 2015, hours after the Defendants had caused data from the Law Firm-2 Email Server to be exfiltrated, HONG and HUNG used the Inside Information to purchase shares of Borderfree stock for the Trading Accounts. Prior to that date, none of the Trading Accounts had purchased any shares of Borderfree stock. To further effectuate their insider trading scheme, between April 29 and May 5, 2015, HONG and HUNG used the Inside Information to purchase additional shares of Borderfree in the Trading Accounts on at least five occasions. In total, HONG and HUNG used the Inside Information to purchase 113,000 shares of Borderfree.

On May 6, 2015, the Pitney Bowes-Borderfree Transaction became public. On that day, Borderfree's stock price increased by approximately $7 per share, or 105 percent, from the previous day's closing price. On May 18, 2015, HONG and HUNG sold their Borderfree shares, earning a profit of approximately $841,000.

Additional Insider Trading and Attempted Insider Trading Based on Inside Information Hacked from the Infiltrated Law Firms

In addition to trading on Inside Information in connection with the Contemplated Intermune Transaction, the Intel-Altera Transaction, and the Pitney Bowes-Borderfree Transaction, detailed above, the Defendants carried out their scheme to enrich themselves by obtaining and trading on the basis of Inside Information exfiltrated from the networks and servers of the Infiltrated Law Firms concerning at least 10 additional M&A transactions, including certain M&A transactions that were contemplated but never consummated. Several of these M&A transactions involved Partner-1 or Partner-2. In total, as a result of trading on Inside Information, the Defendants enriched themselves by at least $4 million.

Attempts to Hack Other Victim Law Firms

In addition to obtaining and trading on Inside Information concerning M&A transactions exfiltrated from the networks and servers of the Infiltrated Law Firms, the Defendants repeatedly attempted to cause unauthorized access to the networks and servers of five other Victim Law Firms using means and methods similar to those used to successfully access the Infiltrated Law Firms. For example, between March and September 2015, the Defendants attempted to cause unauthorized access to the networks and servers of these law firms on more than 100,000 occasions.

The Robotics Company Intrusions

At certain relevant times, the Defendants were also involved in a start-up robotics company (the "Robotics Company"), started by ZHENG, the defendant, which was engaged in the business of developing robot controller chips and providing control system solutions. HONG and HUNG were also involved in running the Robotics Company.

Between April 2014 and late 2015, in addition to their efforts to hack the Victim Law

Firms' networks and servers during this period, the Defendants also caused confidential information to be exfiltrated from the networks and servers of two robotics companies (the "Robotics Company Victims") using substantially similar means and methods of exfiltration as were used to access and attempt to access and exfiltrate information from the Victim Law Firms. Specifically, certain of the same servers that were used to carry out the hacks and attempted hacks of the Victim Law Firms were used to carry out hacks of the Robotics Company Victims. Among other confidential information, the Defendants obtained confidential and proprietary information concerning the technology and design of consumer robotic products, including detailed and confidential proprietary design schematics. Following these exfiltrations from the Robotics Company Victims, the Defendants exchanged emails containing certain of the confidential information they had caused to be exfiltrated from the Robotics Company Victims, including the proprietary schematics.

Defendants and Charges

HONG, 26, and HUNG, 50, are residents of Macau. ZHENG, 30, is a resident of Changsha, China. HONG was arrested on December 25, 2016, in Hong Kong and is now pending extradition proceedings. The defendants are charged with the following offenses, which carry the maximum prison terms listed below. The statutory maximum penalties are prescribed by Congress and are provided here for informational purposes only, as any sentencings of the defendants would be determined by the judge.

Count	Defendants	Charge	Maximum Prison Term
One	HONG, ZHENG, HUNG	Conspiracy to Commit Securities Fraud: Insider Trading	5 years
Two	HONG	Securities Fraud: Insider Trading – Intermune	20 years
Three	ZHENG	Securities Fraud: Insider Trading – Intermune	20 years
Four	HONG	Securities Fraud: Insider Trading – Altera	20 years

Five	HUNG	Securities Fraud: Insider Trading – Altera	20 years
Six	ZHENG	Securities Fraud: Insider Trading - Altera	20 years
Seven	HONG	Securities Fraud: Insider Trading - Borderfree	20 years
Eight	HUNG	Securities Fraud: Insider Trading - Borderfree	20 years
Nine	HONG, ZHENG, HUNG	Conspiracy to Commit Wire Fraud	20 years
Ten	HONG, ZHENG, HUNG	Wire Fraud	20 years
Eleven	HONG, ZHENG, HUNG	Conspiracy to Commit Computer Intrusion	5 years
Twelve	HONG, ZHENG, HUNG	Computer Intrusion – Unlawful Access – Law Firm-2	10 years
Thirteen	HONG, ZHENG, HUNG	Computer Intrusion – Intentional Damage – Law Firm-2	10 years

* * *

Mr. Bharara praised the investigative work of the FBI, and thanked the Securities and Exchange Commission for their assistance. Mr. Bharara also thanked the Office of International

Affairs and Hong Kong law enforcement for their assistance in the arrest and apprehension of HONG. He added that the investigation is continuing.

The charges were brought in connection with the President's Financial Fraud Enforcement Task Force. The task force was established to wage an aggressive, coordinated and proactive effort to investigate and prosecute financial crimes. With more than 20 federal agencies, 94 U.S. attorneys' offices, and state and local partners, it is the broadest coalition of law enforcement, investigatory and regulatory agencies ever assembled to combat fraud. Since its formation, the task force has made great strides in facilitating increased investigation and prosecution of financial crimes; enhancing coordination and cooperation among federal, state and local authorities; addressing discrimination in the lending and financial markets; and conducting outreach to the public, victims, financial institutions and other organizations. Since fiscal year 2009, the Justice Department has filed over 18,000 financial fraud cases against more than 25,000 defendants. For more information on the task force, please visit www.StopFraud.gov.

This case is being handled by the Office's Securities and Commodities Fraud Task Force and the Complex Frauds and Cybercrime Unit. Assistant U.S. Attorneys Andrea M. Griswold, Daniel B. Tehrani, and Kristy J. Greenberg are in charge of the prosecution.

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

16-353 ###