



**U.S. Department of Justice**

*United States Attorney  
Eastern District of New York*

AB: CMP/MBM  
F. #2010R02203

*271 Cadman Plaza East  
Brooklyn, New York 11201*

November 18, 2010

VIA FAX

The Honorable Dora L. Irizarry  
United States District Judge  
Eastern District of New York  
225 Cadman Plaza East  
Brooklyn, New York 11201

Re: United States v. Lin Mun Poo  
Criminal Docket No. 10-891 (DLI) (ALC)

Dear Judge Irizarry:

The government respectfully submits this letter in support of its motion for a permanent order of detention of the defendant Lin Mun Poo. On November 18, 2010, a Grand Jury in the Eastern District of New York returned the attached four-count indictment charging the defendant with access device fraud and aggravated identity theft (Counts One and Two), as well as two counts involving computer "hacking" - specifically, unauthorized computer access and transmission of malicious code involving a computer network of the Federal Reserve Bank (Counts Three and Four). As explained below, the government has also obtained extensive evidence of the defendant's criminal hacking activity targeting the national security, military and financial sectors of the United States.

The defendant, a Malaysian citizen, was arrested on a complaint in Brooklyn, New York on October 21, 2010, shortly after his arrival at John F. Kennedy International Airport ("JFK") from Europe. At the defendant's arraignment on October 22, 2010, United States Magistrate Judge Viktor V. Pohorelsky entered a permanent order of detention with leave to make an application for bail. Should the defendant apply for pretrial release when he is arraigned on the indictment or at his initial appearance before the Court, the government respectfully submits that the defendant poses a serious risk of flight and should remain in pretrial detention.

## Factual Proffer

The government proffers the following facts concerning the charges at issue and pretrial detention. See United States v. LaFontaine, 210 F.3d 125, 130-31 (2d Cir. 2000) (the government is entitled to proceed by proffer in a detention hearing); United States v. Ferranti, 66 F.3d 540, 542 (2d Cir. 1995) (same); United States v. Martir, 782 F.2d 1141, 1145 (2d Cir. 1986) (same). These facts are relevant to three of the factors to be considered in the detention analysis under the Bail Reform Act: (1) the nature and circumstances of the crimes charged, (2) the history and characteristics of the defendant, including his risk of flight, and (3) the evidence of the defendant's guilt. See 18 U.S.C. § 3142(g).

### I. Nature and Circumstances of Crimes Charged and the Evidence of the Defendant's Guilt

The government's evidence of the defendant's guilt of the charged crimes, as well as uncharged criminal activity, demonstrates his position as an extremely sophisticated and dangerous computer hacker. At the time of the defendant's arrest, Secret Service agents seized a heavily encrypted laptop computer that was in his possession. This computer contained a massive quantity of stolen financial account data and personal identifying information, including more than 400,000 credit card, debit card and bank account numbers, in violation of 18 U.S.C. §§ 1029 and 1028A (Counts One and Two).

In his post-arrest statement, the defendant admitted compromising the computer servers of a number of major financial institutions and companies. For example, the defendant admitted that he compromised a computer network of the Federal Reserve Bank ("FRB") by exploiting a vulnerability he found within their secure system. The FRB in Cleveland, Ohio has confirmed that an FRB computer network was hacked in approximately June 2010, resulting in thousands of dollars in damages, affecting ten or more FRB computers, and forming the basis for Counts Three and Four.

The defendant's seized computer also contains evidence of additional and very significant hacking activity. For example, the defendant possessed data illegally obtained from the computer network of FedComp, a data processor for various credit unions in the United States. By hacking into the FedComp system, the defendant had unauthorized access to the data of the Firemen's Association of the State of New York Federal Credit Union and the Mercer County New Jersey Teachers' Federal Credit

Union, among other victims. The defendant also admitted to compromising the computer networks of several major international banks and companies, and admitted earning money by finding and exploiting network vulnerabilities or trading and selling the information contained therein.

The defendant has not limited his criminal conduct to compromising financial institutions. The government has obtained evidence that his cybercrime activities extend to the national security sector. For example, in approximately August 2010, the defendant hacked into the secure computer system of a major Department of Defense contractor, which provides systems management for military transport and other highly sensitive military operations. These are but a few examples of the government's evidence of the defendant's criminal hacking activity targeting the United States' financial and national security sectors.

## II. History and Characteristics of the Defendant and Risk of Flight

The defendant is a resident and citizen of Malaysia. He traveled to the United States from Malaysia via Europe on a round-trip ticket, with a planned return date to Malaysia of November 22, 2010. The government is not aware of any family or professional ties to the United States or New York. Indeed, the defendant appears to have traveled to the United States for the sole purpose of engaging in criminal activity; within hours of his arrival at JFK on October 21, 2010, United States Secret Service agents observed the defendant selling stolen credit card numbers for \$1,000 at a diner in Brooklyn and arrested him shortly thereafter. In his post-arrest statement, the defendant admitted that the primary purpose of his journey to the United States was to meet with an individual who the defendant believed was capable of regularly providing the defendant with a large volume of stolen card numbers and personal identification numbers, which the defendant said he planned to use to withdraw cash from automated teller machines.

The defendant's lack of any non-criminal ties to the United States and his return plane ticket to Malaysia are sufficient to demonstrate his severe flight risk. Moreover, the defendant has seemingly limitless unauthorized access to financial accounts and identity information from around the world, which would enable him to easily obtain financial resources and a new identity to facilitate his flight. Finally, the defendant faces a lengthy term of incarceration, which would increase his motive to flee the United States if he were released

from custody. Under United States Sentencing Guideline § 2B1.1, which assigns a minimum loss amount of \$500 per unauthorized access device (resulting in a total loss amount of at least \$20 million), the defendant's estimated Guidelines range for Count One alone is 78 to 97 months. The defendant is also charged with aggravated identity theft in violation of 18 U.S.C. § 1028A, which carries a mandatory, consecutive sentence of two years. These factors unequivocally demonstrate risk of flight by a preponderance of the evidence. United States v. Chimurenga, 760 F.2d 400, 405 (2d Cir. 1985).

Conclusion

For these reasons, the government respectfully requests that the Court maintain the permanent order of detention issued on October 22, 2010 with respect to the defendant Lin Mun Poo.

Respectfully submitted,

LORETTA E. LYNCH  
United States Attorney

By: /s/ Cristina M. Posa  
Cristina M. Posa  
Melissa B. Marrus  
Assistant U.S. Attorneys  
(718) 254-6668/6790

cc: Kannan Sundaram, Esq. (via fax)

Attachment