CR 12 (Rev. 5/03)

WARRANT FOR ARREST

United States District Court	DISTRICT: SOUTHERN DISTRICT OF NEW YORK
UNITED STATES OF AMERICA v. LEE JASON JUESHENG, a/k/a " iAlert," a/k/a "Jason Kato"	DOCKET NO.: 12 MAG MAGISTRATE'S CASE NO.: 1605 NAME AND ADDRESS OF INDIVIDUAL TO BE ARRESTED: LEE JASON JUESHENG, a/k/a " iAlert," a/k/a "Jason Kato"
WARRANT ISSUED ON THE BASIS OF: ☐ Order of Court ☐ Indictment ☐ Information X Complaint	DISTRICT OF ARREST: Southern District of New York
TO: UNITED STATES MARSHAL OR ANY OTHER AUTHORIZED OFFICER	CITY

YOU ARE HEREBY COMMANDED to arrest the above-named person and bring that person before the United States District Court to answer to the charge(s) listed below.

DESCRIPTION OF CHARGES

Access Device Fraud

IN VIOLATION OF	UNITED STATES CODE TITLE: 18	SECTION: § 1029(a)

BAIL	OTHER CONDITIONS OF RELEASE	
ORDERED BY: HENRY PITMAN United States Magistrate Judge Southern District of New York	SIGNATURE (~~FEDERAL JUDGE~~/U.S. MAGISTRATE): S/ JUN 15 2012	DATE ORDERED
CLERK OF COURT	(BY) DEPUTY CLERK	DATE ISSUED

RETURN

This warrant was received and executed with the arrest of the above-named person.

DATE RECEIVED	NAME AND TITLE OF ARRESTING OFFICER	SIGNATURE OF ARRESTING OFFICER
DATE EXECUTED		

Note: The arresting officer is directed to serve the attached copy of the charge on the defendant at the time this warrant is executed.

Approved: _____
Alexander Wilson
Assistant United States Attorney

12 MAG 1605

Before: HONORABLE HENRY B. PITMAN
United States Magistrate Judge
Southern District of New York

UNITED STATES OF AMERICA	:	SEALED COMPLAINT
- v. -	:	Violation of 18 U.S.C. §§ 1029(a)(2)
LEE JASON JUESHENG, a/k/a "iAlert," a/k/a "Jason Kato,"	:	COUNTY OF OFFENSE: New York
Defendant.	:	

SOUTHERN DISTRICT OF NEW YORK, ss.:

JOHN LEO, JR., being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI") and charges as follows:

COUNT ONE
(Access Device Fraud)

1. From on or about February 6, 2012, up to and including on or about February 21, 2012, in the Southern District of New York and elsewhere, LEE JASON JUESHENG, a/k/a "iAlert," a/k/a "Jason Kato," the defendant, knowingly and with intent to defraud, and affecting interstate and foreign commerce, trafficked in and used one and more unauthorized access devices, and by such conduct obtained something of value aggregating $1,000 and more, to wit, KATO sold approximately 119 stolen credit card numbers for property with a value of approximately $2,055.

(Title 18, United States Code, Sections 1029(a)(2).)

The bases for my knowledge and for the foregoing charge are, in part, as follows:

2. I have been personally involved in the investigation of this matter. This affidavit is based upon my investigation, my conversations with other law enforcement agents, and my examination of reports and records. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

3. I have been a Special Agent with the FBI for approximately six years. For the past five years, I have been assigned to the computer intrusion squad in the FBI's New York Field Office. I have received training regarding computer technology, computer fraud, and white collar crimes.

4. Based on my training and experience, I have learned the following:

a. Carding: "Carding" refers to various criminal activities associated with stealing personal identification information and financial information belonging to other individuals - including the account information associated with credit cards, bank cards, debit cards, or other access devices - and using that information to obtain money, goods, or services without the victims' authorization or consent. For example, a criminal might gain unauthorized access to (or "hack") a database maintained on a computer server and steal credit card numbers and other personal information stored in that database. The criminal can then use the stolen information to, among other things: (1) buy goods or services online; (2) manufacture counterfeit credit cards by encoding them with the stolen account information; (3) manufacture false identification documents (which can be used in turn to facilitate fraudulent purchases); or (4) sell the stolen information to others who intend to use it for criminal purposes. "Carding" refers to the foregoing criminal activity generally and encompasses a variety of federal offenses, including, but not limited to, identification document fraud, aggravated identity theft, access device fraud, computer hacking, wire fraud, and bank fraud.

b. Carding Forums: "Carding forums" are websites used by criminals engaged in carding ("carders") to facilitate their criminal activity. Carders use carding forums to, among other things: (1) exchange information related to carding, such as information concerning hacking methods or computer-security

vulnerabilities that could be used to obtain personal identification information; and (2) buy and sell goods and services related to carding, for example, stolen credit card or debit card account numbers, hardware for creating counterfeit credit cards or debit cards, or goods bought with compromised credit card and debit card accounts. Carding forums often permit users to post public messages (postings that can be viewed by all users of the site), sometimes referred to as "threads." For example, a user who has stolen credit card numbers may post a public "thread" offering to sell the numbers. Carding forums also often permit users to communicate one-to-one through so-called "private messages." Because carding forums are, in essence, marketplaces for illegal activities, access is typically restricted to avoid law enforcement surveillance. Typically, a prospective user seeking to join a carding forum can only do so if other, already established users "vouch" for the prospective user, or if the prospective user pays a sum of money to the operators of the carding forum. User accounts are typically identified by a username and access is restricted by password. Users of carding forums typically identify themselves on such forums using aliases or online nicknames ("nics").

Background on the Investigation

5. Based on my participation in the investigation of this matter, I know the following:

a. In or about June 2010, the FBI established an undercover carding forum (the "UC Site"), enabling users to discuss various topics related to carding and to communicate offers to buy, sell, and exchange goods and services related to carding, among other things.

b. The FBI established the UC Site as an online meeting place where the FBI could locate cybercriminals, investigate and identify them, and disrupt their activities.[1] The UC Site was configured to allow the FBI to monitor and to record the discussion threads posted to the site, as well as private messages sent through the site between registered users. The UC Site also allowed the FBI to record the Internet protocol

[1] The registration process for the UC Site required users to agree to terms and conditions, including that their activities on the UC Site were subject to monitoring for any purpose.

("IP") addresses of users' computers when they accessed the site.[2]

c. Access to the UC Site was limited to registered members and required a username and password to gain entry. Various membership requirements were imposed from time to time to restrict site membership to individuals with established knowledge of carding techniques or interest in criminal activity. For example, at times new users were prevented from joining the site unless they were recommended by two existing users who had registered with the site, or unless they paid a registration fee.

d. New users registering with the UC Site were required to provide a valid e-mail address as part of the registration process. An e-mail message was sent to that email address containing registration instructions. In order to complete the registration process, the new user was required to open the e-mail, click on a link in it, and then enter an activation code specified in the e-mail message. The e-mail addresses entered by registered members of the site were collected by the FBI.

e. In the course of the undercover operation, the FBI contacted multiple affected institutions and/or individuals to advise them of discovered breaches in order to enable them to take appropriate responsive and protective measures. Based on information obtained through the site, the FBI estimates that it helped financial institutions prevent many millions of dollars in losses from credit card fraud and other criminal activity, and has alerted specific individuals regarding breaches of their personal email or other accounts.

f. At all times relevant to this Complaint, the server for the UC Site, through which all public and private messages on the UC Site were transmitted, was located in New York, New York.

Access Device Fraud by the Defendant

6. As set forth in detail below, LEE JASON JUESHENG, a/k/a "iAlert," a/k/a "Jason Kato," the defendant, sold 119 stolen credit card numbers to a user of the UC Site in exchange for three iPad 2 electronic devices (the "iPads") with a value

[2] Every computer on the Internet is identified by a unique number called an Internet protocol ("IP") address, which is used to route information properly between computers.

of $2,055.29. Unbeknownst to JUESHENG, the individual to whom he sold the 119 stolen credit cards was in fact a Special Agent of the FBI, using an undercover online identity ("UC-1").

7. Based on my involvement in monitoring the UC Site and my review of files and logs maintained by the FBI concerning the UC Site, I know the following:

a. On or about October 7, 2010, a new user registered on the UC Site with the nickname "iAlert." As set forth in paragraphs 11 through 14 below, "iAlert" has subsequently been identified as LEE JASON JUESHENG, a/k/a "iAlert," a/k/a "Jason Kato," the defendant. When registering on the UC Site, JUESHENG listed interests including "carding," "dumps," and "skimming." "Carding" has been described above in paragraph 4(c). Based on my training and experience and knowledge of this investigation, I also know that:

(1) "dumps" is a term often used by carders to refer to credit card data in the form in which such data is stored on the magnetic strips on the backs of credit cards; and

(2) "skimming" is an illegal activity that involves the installation of devices, known as "skimmers," on Automated Teller Machines ("ATMs"), that surreptitiously record the user's bank account numbers, along with the corresponding Personal Identification Numbers, enabling criminals to use that information to steal money from customers' accounts.

b. I have reviewed JUESHENG's postings and private messages on the UC Site, and messages he exchanged with undercover law enforcement agents and a confidential source via various instant-messaging, or "chat," services, on the Internet. In these communications, JUESHENG repeatedly offered to sell or purchase credit card, bank account and other financial information, carding-related technology such as skimmers, and malware-related services and products. JUESHENG also indicated that he had started and run his own alternate carding forum website.

c. On or about February 3, 2012, UC-1 started a discussion thread on the UC Site stating, in substance and in

part, that UC-1 was using stolen credit card numbers to purchase items at stores in Manhattan, New York.

d. On or about February 5, 2012, JUESHENG, using the nickname "iAlert," posted a response in that discussion thread started by UC-1, stating, in substance and in part, that if UC-1 could get items for JUESHENG, JUESHENG could provide UC-1 with "unlimited dumps."

e. On or about February 6, 2012, JUESHENG and UC-1 exchanged a series of private messages via the UC Site including the following, in substance and in part:

(1) UC-1 referred to JUESHENG's response described in paragraph 7(c) above, and asked if JUESHENG needed something.

(2) JUESHENG responded that he needed two iPhones and three iPads.

(3) UC-1 asked what he would receive in return, and asked if JUESHENG had "cards."

(4) JUESHENG responded that he had "unlimited dumps."

f. On or about February 12, 2012, JUESHENG and UC-1 exchanged a series of private messages via the UC Site, during which, in substance and in part, UC-1 asked for a phone number to include in the shipping instructions for the iPads, and in response JUESHENG provided a Japanese phone number (the "KATO PHONE NUMBER").

8. From reviewing records relating to the account used by UC-1 on ICQ, an instant-messaging, or "chat," service, on the Internet, I know the following:

a. On or about February 6, 2012, LEE JASON JUESHENG, a/k/a "iAlert," a/k/a "Jason Kato," the defendant, and UC-1 exchanged a series of ICQ messages. During the exchanges, they stated the following, in substance and in part:

(1) JUESHENG asked UC-1 where UC-1 was located. UC-1 stated that he was in New York City near Times Square.

(2) JUESHENG offered "200 dumps" for three iPads and two iPhones. UC-1 stated that he could only get iPads at that time.

(3) JUESHENG and UC-1 agreed that JUESHENG would provide UC-1 with "120 dumps" in exchange for UC-1 sending him three "ipad 2[s]."

b. On or about February 10, 2012, JUESHENG and UC-1 exchanged another series of ICQ messages. During this exchange, JUESHENG stated, in substance and in part, that UC-1 should ship the iPads to "Kato Jason" at an address in Tokyo, Japan (the "KATO ADDRESS").

c. On or about February 21, 2012, JUESHENG and UC-1 exchanged another series of ICQ messages. During this exchange, JUESHENG provided UC-1 with a link to a file containing what appears to be credit card data for 120 credit cards. I have reviewed records provided by a credit card issuer ("Issuer-1"), which show that this file included data for 119 actual credit cards.

9. From conversations with other FBI agents and review of FBI records, I know that in or around February 2012, FBI personnel purchased the iPads for $2,055.29 and shipped them to the KATO ADDRESS.

10. From my review of United States Postal Service records, I know the iPads were delivered to the KATO ADDRESS on or about February 18, 2012.

Identification of the Defendant

11. Using an undercover online identity, I have communicated with "iAlert" via MSN Messenger, a popular instant-messaging, or "chat," service, on the Internet. When communicating with me, "iAlert" has used an account in the name "kato.jason@hotmail.co.jp."

12. Based on my involvement in monitoring the UC Site and my review of files and logs maintained by the FBI concerning the UC Site, I know that on or about January 1, 2011, "iAlert" informed another user of the UC Site that his account on Skype, an Internet communications service, was in the name "kato.jason."

13. As noted above in paragraphs 7(f) and 8(b), "iAlert" instructed UC-1 to ship the iPads to "Kato Jason" at the KATO

ADDRESS, using the KATO PHONE NUMBER in the shipping instructions.[3]

14. From my review of records provided by Interpol Japan, I know the following:

a. The listed subscriber for the KATO PHONE NUMBER is "Jason Kato," residing at the KATO ADDRESS.

b. LEE JASON JUESHENG and his wife, whose last name is Kato, are residents of the KATO ADDRESS.

c. Lee Jason Juesheng has used the alias "Jason Kato."

15. Accordingly, I believe that the individual who has used the UC Site under the name "iAlert" is LEE JASON JUESHENG, a/k/a "iAlert," a/k/a "Jason Kato," the defendant.

WHEREFORE, I respectfully request that an arrest warrant be issued for LEE JASON JUESHENG, a/k/a "iAlert," a/k/a "Jason Kato," the defendant, and that he be arrested and imprisoned or bailed, as the case may be.

JOHN LEO, JR.
Special Agent
Federal Bureau of Investigation

Sworn to before me this
15th day of June 2012

S/ Henry Pitman
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK

HENRY PITMAN
United States Magistrate Judge
Southern District of New York

[3] In his communications with UC-1, "iAlert" indicated that the KATO ADDRESS was a "drop address" and that his "drop" would send the iPads to him after they arrived. Based on the investigation of this matter and the facts as set forth in this Complaint, however, I believe that there is no "drop" and "iAlert" is a resident of the KATO ADDRESS.