

Court File No. 081217556X1
Affidavit of Darren Hafner
Date Sworn: _____

**IN THE COURT OF QUEEN'S BENCH OF ALBERTA
JUDICIAL DISTRICT OF CALGARY**

**IN THE MATTER OF AN APPLICATION PURSUANT TO SECTION 13 OF THE
EXTRADITION ACT FOR A WARRANT FOR THE ARREST OF EHUD
TENENBAUM**

BETWEEN:

THE UNITED STATES OF AMERICA

Extradition Partner

- and -

EHUD TENENBAUM

Person Sought

AFFIDAVIT

I, Darren Hafner, Peace Officer, of the City of Calgary, Province of Alberta,
MAKE OATH AND SAY AS FOLLOWS:

1. I am a member of the Calgary Police Service currently assigned to the Commercial Crime unit. As such, I have personal knowledge of the matters deposed to in this Affidavit, except where stated to be based on information and belief and where so stated I verily believe them to be true.
2. Pursuant to a Provisional Arrest Request (the "Request") made by the Government of the United States of America ("USA") to the Government of Canada, I swear this Affidavit in support of an application for a warrant for the provisional arrest of Ehud Tenenbaum pursuant to the provisions of the

Extradition Act and the Treaty on Extradition between the Government of Canada and of the United States of America.

3. Pursuant to section 13 of the *Extradition Act*, the Minister of Justice, through his authorized official has authorized the Attorney General of Canada to apply for a warrant for the provisional arrest of Ehud Tenenbaum. A true copy of the Minister's Authorization dated September 22, 2008 is attached as Exhibit "A" to this Affidavit.

4. Based on my reading of the facts set out in the Request, I have reasonable grounds to believe and do believe the following to be true:

(a) The particulars of the person who is sought to be provisionally arrested are as follows:

Name:	Ehud Tenenbaum
Date of Birth:	August 29, 1979
Place of Birth:	Israel
Citizenship:	Israel
Height:	6'0
Weight:	215 lbs
Eye Colour:	Brown
Hair Colour:	Brown
Ethnicity/Race:	_____

(b) On August 20, 2008, United States Magistrate Judge Ramon E. Reyes of the United States District Court, Eastern District of New York issued a Warrant for the arrest of Ehud Tenenbaum to stand trial on a charge of Fraudulent use of unauthorized access devices, in violation of Title 18, United States Code, Section 1029(b)(2). A true copy of the Warrant is attached as Exhibit "B" to this Affidavit.

(c) The "PIN" Cashout Conspiracy:

Since approximately October 2007, the United States Secret Service ("USSS") has been investigating an international conspiracy to hack into the computer systems of financial institutions and other businesses in the United States for the purpose of stealing confidential financial account information, which the hackers in turn sell to individuals in the United States and other countries over the Internet. The hackers and their associates generally transmit this information via instant messenger services, such as Microsoft Instant Messenger, or via electronic mail. The purchasers of the stolen financial information use the account numbers to encode plastic credit cards, which they then use to withdraw currency from automated teller machines ("ATMs") located at banks in the United States and elsewhere in a scheme known as a "PIN cashout." As detailed below, Ehud Tenenbaum's participation in this conspiracy began at least in January 2008. The most recent evidence of his participation in the conspiracy is from May 2008, although his participation is likely continuing to the present date.

In January and February 2008, the USSS investigated the network intrusion of two financial institutions, OmniAmerican Credit Union, based in Fort Worth, Texas, and Global Cash Card based in Irvine, California. As a result of these network intrusions, credit card and debit card numbers were stolen and subsequently used worldwide to withdraw money. The victim banks determined that their card numbers had been obtained through a breach of their computer network initiated via "SQL injection." SQL is a database software code similar to Oracle, and SQL injection is a form of attack on a database-driven website, in which the attacker executes unauthorized SQL commands by taking advantage of insecure code on a system connected to the Internet, bypassing the firewall. The approximate actual loss due to these two breaches is over \$1 million;

however, the potential loss could have exceeded \$10 million to \$15 million. In April and May 2008, the USSS became aware of two other large-scale financial institutions network intrusions, at Symmetrex, a financial transaction processor based in Florida, and at 1st Soruce Bank in Indiana. These institutions and their associated banks (MetaBank, a United States bank based in Iowa and South Dakota, held the funds backing Symmetrex's debit cards) suffered a loss of over \$3 million, and each victim indicated that their networks had been compromised via SQL injection.

The USSS determined that the suspected hackers were using several servers in Virginia, located at HopOne Internet Corp. ("HopOne") in McLean, Virginia. Based on data obtained pursuant to court-ordered pen registers and trap and trace devices, it became apparent that much of the traffic going through the HopOne servers was originating from the Dutch company LeaseWeb.

As a result of the involvement of the LeaseWeb servers, on April 7, 2008, the United States requested the assistance of law enforcement authorities in the Netherlands in tracking all computer traffic pertaining to three servers hosted by LeaseWeb, and intercepting the content of that traffic. The Netherlands acceded to this request and authorized interception of the LeaseWeb servers for a 30-day period, which was renewed on May 9, 2008. Through the investigation, the prosecutor has determined that EHUD Tenenbaum, using the online nickname Analyzer22@hotmail.com (see Section E below for identification of Tenenbaum as Analyzer22@hotmail.com), has discussed with other known hackers and PIN Cashers information about hacking into the above-referenced four banks, as well as many other U.S. and foreign financial institutions.

- (d) The Role of EHUD Tenenbaum in the PIN Cashout Conspiracy:

In an MSN Instant Messenger ("IM") conversation, or "chat" on April 18, 2008, Tenenbaum revealed that he was responsible for hacking into the network of Global Cash Card; the compromise of this network resulted in a February 2008 PIN cashout operation. In the same chat, Tenenbaum said he was attempting to hack into the same system again. In his IM, Tenenbaum wrote, "yesterday I rechecked [Global Cash Card] they are still blocking everything. so we cant hack them again."

On April 18, 2008, Tenenbaum further discussed the intrusion of Symmetrex and exchanged syntax (computer commands) used to carry out this attack with a co-conspirator. He also exchanged over 150 compromised credit/debit card numbers obtained via this intrusion. Tenenbaum further discussed his access into servers used to attack a large number of U.S. financial institutions.

In an April 20, 2008 chat, Tenenbaum provided account information taken from Symmetrex's network to be shared with cashing crews. Tenenbaum said he expected to receive 10 to 20 percent of the proceeds from this PIN cashout. Throughout the night of April 20, 2008, Tenenbaum received updates on the global operation, noting that the cards were functioning successfully in Russia and, for a time, in Turkey, but were not working in Pakistan or Italy. This PIN cashout operation continued into April 21, 2008, with Tenenbaum reporting they had success in the United States, Canada, Sweden, Bulgaria and Germany. By 3:00 p.m. on April 21, 2008, Tenenbaum stated that after paying his cashers, he earned approximately "350 - 400," which, based on this investigation, most likely refers to 350,000 to 400,000 dollars or euros. Tenenbaum's co-conspirator estimated that he had earned 150,000 to 200,000 dollars or euros and asked Tenenbaum how much he wanted for his share, writing, "i think 150 like possible if poser finish all will be 200k maybe total how much u want me to send you?"

In a chat on April 20, 2008, Tenenbaum instructed his co-conspirator to prepare a team for another ATM cashout scheme. Tenenbaum said that he had 25 account numbers, each with a balance of \$1,500.00, writing, "i am making a small operation, u have cashier? i been trying to get a hold of u i saved for u 25 cards each one 1500\$ limit, get cashier as soon as possible, ok, i will load them."

In another chat on April 28, 2008, Tenenbaum commented on the size of the network of 1st Source Bank, stating that he had already hacked into the bank's system, obtained administer privileges, and had found many credit card numbers and ATM output. Tenenbaum wrote, "is HUGE i saw, atm outputs, tons of cards, i am admin there, and i already cracked some of the domain." Tenenbaum's co-conspirator replied that s/he already had people inside the network, and asked Tenenbaum to stop accessing that particular network. Tenenbaum responded, "dude like i told ya its windows network i am happy i could help u to get shell there now its ur guys job."

In a chat on May 19, 2008, Tenenbaum told his co-conspirator that he hacked into the largest bank network in Greece, and that he has friends working at this bank. In his IM, Tenenbaum wrote, "i hacked this huge bank network really huge. what u think? good hack? Btw linked server AXEDB is even better. alpha.gr is the biggest bank in Greece."

(e) Identification of Ehud Tenenbaum as Analyzer22@hotmail.com:

Subscriber information obtained from Hotmail identified the registered first and last name for "Analyzer22@hotmail.com" as "Ehud Tenenbaum." In addition, the registered birth date for "Analyzer22@hotmail.com" is listed as August 29, 1979, the birth date of Ehud Tenenbaum.

Additionally, Hotmail's login records show that "Analyzer22@hotmail.com" connected to the Microsoft IM service on at least one occasion from the Internet Protocol ("IP") address 69.70.122.98. USSS agents conducted an RWhois search of Videotron, the Internet service provider in Montreal, Quebec, Canada that owns and operates the IP address 69.70.122.98. (RWhois is an extension of the Whois protocol, which is a tool used to look up information about domain names and IP addresses.) The results of this search showed that this IP address registered to a business customer called "Internet Lab Secure," located at [REDACTED], Montreal, QC, H2R 1W7, Canada.

On July 30, 2008, Canadian law enforcement authorities obtained a warrant to search for the subscriber information of the IP address 69.70.122.98, which established that the subscriber for IP address 69.70.122.98 is Internet Labs Secure Inc. of [REDACTED] [REDACTED] Montreal, QC, H2R 1W7, Canada. In addition, Canadian law enforcement authorities have determined that Tenenbaum is listed as a director of Internet Labs Secure Inc. On July 25, 2008, the *Service de police de la ville de Montreal* confirmed that Tenenbaum resides at this address.

Furthermore, forensic analysis of the network of Global Cash Card indicated that this same IP address, 69.70.122.98, was used to check balances of compromised accounts and attempted to increase balance limits on these compromised accounts. This IP address also was used to obtain compromised usernames and passwords in this attempt. System logs from Global Cash Card indicate that between February 14, 2008, and February 18, 2008, a user connected to the compromised bank network from this IP address, and on February 15, 2008, another IP address

associated with Tenenbaum was used to download a file containing all of that compromised computer's data.

To date, the investigation has attributed at least \$10 million in losses associated with these network intrusions and PIN cashout activities.

The USSS is aware of a current investigation being conducted by multiple Canadian law enforcement agencies, in which Tenenbaum is accused of committing similar crimes, including introducing into the network of a Canadian financial institution for the purposes of withdrawing funds using compromised account numbers.

5. On August 28, 2008, I was present at the time of Ehud Tenenbaum's arrest on a Canada-wide warrant in Montreal, Quebec. Mr. Tenenbaum's arrest was based on fraud charges instituted by the Calgary Police Service. I believe that he has been in custody at the Calgary Remand Centre since his return to Calgary following his arrest in Montreal. A bail hearing relative to his outstanding Calgary Police Service charges is scheduled to take place at 2:00 p.m. on Monday, September 22, 2008 in the Provincial Court of Alberta (Courtroom 306).
6. At the time of his arrest, Tenenbaum was in possession of an Israeli passport. This passport is now in my custody. I have reviewed the photograph of Tenenbaum that was included in the Provisional Arrest Request submitted by the United States of America with the photograph in the passport seized from Tenenbaum, as well as my own personal observations, and believe that the individual currently in custody at the Calgary Remand Centre and the persons depicted in the passport photograph and the photograph contained in the Provisional Arrest Request is the same person, Ehud Tenenbaum. A true copy of the photograph included in the Provision Arrest Request submitted by the United States of America is attached as "Exhibit C" to this my affidavit.

7. I am advised by Craig Bell of the Canadian Border Service Agency (CPSA) and do verily believe that Tenenbaum was admitted to Canada on March 11, 2008 at Toronto, Ontario. As a citizen of Israel, Tenenbaum would not have required a Visa but, rather, would have enjoyed visitor status for a period of 6 months from the date of entry into Canada. As such, Tenenbaum's lawful status in Canada as a visitor expired on September 11, 2008.
8. Having reviewed the contents of the Provision Arrest Request prepared by authorities in the United States of America, I believe that the Government of the United States of America has evidence available to lead at trial which is capable of proving the above allegations and that this evidence derives from reliable and credible sources.

A Provisional Arrest Warrant is Necessary in the Public Interest

6. I believe that it is necessary in the public interest that the Court order the arrest of Ehud Tenenbaum on a provisional arrest warrant to ensure that he remains within this jurisdiction and to prevent him from committing further criminal offences. I believe that there is a risk that if Ehud Tenenbaum is not arrested on a provisional arrest warrant but merely summonsed, he would not attend his extradition proceedings. I base my beliefs on the following:


(a) Ehud Tenenbaum is a resident of Israel and, as such, has no known links to the City of Calgary or the Province of Alberta.

(b) If directed to attend his extradition proceedings by means of a summons only the Court would have no ability to specify any conditions that would govern his behaviour while at large awaiting the conclusion of proceedings under the *Extradition Act*.

7. I believe the facts set out in this Affidavit are true and request that a Warrant for the Provisional Arrest of Ehud Tenenbaum be issued pursuant to the *Extradition Act*.

Sworn before me in the City of Calgary,)
in the Province of Alberta this 22)
day of September, 2008.)
)
)
)
)
)

ATwell 3444)
A Commissioner for Oaths in and for the)
Province of Alberta)

 2874
DARREN HAFNER