OFFICE OF THE CHIEF OF POLICE

ADMINISTRATIVE ORDER NO. 4 February 19, 2015

**SUBJECT:** **COMPUTER-RELATED CRIMES - FIELD NOTEBOOK DIVIDER, FORM 18.52.00 - ACTIVATED**

**PURPOSE:** Important information and evidence are often missed during the preliminary investigation of a computer-related crime. The Computer-Related Crimes - Field Notebook Divider, Form 18.52.00, has been created to assist officers in identifying computer-related crimes and terminology.

**PROCEDURE:** **COMPUTER-RELATED CRIMES - FIELD NOTEBOOK DIVIDER, FORM 18.52.00 - ACTIVATED.** The Computer-Related Crimes - Field Notebook Divider, Form 18.52.00, has been activated and will be used to assist officers in accurately identifying and documenting computer-related crimes.

**FORM AVAILABILITY:** A copy of the Computer-Related Crimes - Field Notebook Divider, Form 18.52.00, is attached for immediate use and duplication, and is available in LAPD E-Forms on the Department's Local Area Network (LAN).

**AUDIT RESPONSIBILITY:** The Commanding Officer, Internal Audits and Inspections Division, will review this directive and determine whether an audit or inspection will be conducted in accordance with Department Manual Section 0/080.30.

CHARLIE BECK
Chief of Police

Attachment

DISTRIBUTION "D"

# COMPUTER-RELATED CRIMES – FIELD NOTEBOOK DIVIDER

This Notebook Divider will assist officers in identifying computer-related crimes and provide a list of terminologies (terms) frequently used with those crimes. For purposes of the Notebook Divider, computer-related crimes apply equally to mobile hand held devices (e.g., mobile phone, tablet).

The Computer Crimes Unit (CCU), Commercial Crimes Division (CCD), primary investigative responsibility is the investigation of unauthorized computer accesses. These crimes are addressed under California Penal Code section 502(c). The CCU will also handle Grand/Petty Theft investigations that involve "phishing," or where the data on the computer is the target of the crime.

## I. CRIMES HANDLED BY THE COMPUTER CRIMES UNIT.

**§ 502 Unauthorized Computer Access.** This is commonly referred to as "hacking." Examples of Unauthorized Computer Access (UCA) are:

* The computer is controlled by an outside source, without permission or knowledge of the owner.
* Data has been removed or altered from the computer without the owner's knowledge or permission.
* Password(s) to the computer and/or webpages/email have been changed, and/or the owner has been locked out or otherwise prevented from accessing his/her own accounts.

A UCA crime may involve additional crimes such as extortion and/or a "denial of service attack". Ask all pertinent questions for an extortion investigation in addition to the UCA.

**§ 487 Grand Theft and § 484 Petty Theft (Via Phishing).** The suspect will "spoof" an email (victim, witness, business client), tricking the victim into buying/selling/shipping goods, money or services. There may be multiple victims involved.

## II. CRIMES HANDLED BY THE AREA.

**§ 422 Criminal Threats (Felony).** Follow the criteria for Criminal Threats. The mere fact that the "threat" was posted on the internet does not change the criteria for Criminal Threats. The threat could be in the form of an email or posting on a social networking site such as Facebook or Twitter.

**§ 646.9 Cyber Stalking (Felony).** (a) Any person who willfully, maliciously, and repeatedly follows or willfully and maliciously harasses another person and who makes a credible threat with the intent to place that person in reasonable fear for his or her safety, or the safety of his or her immediate family; (g) Including that performed through the use of an electronic communication device, or a threat implied by a pattern of conduct or a combination of verbal, written, or electronically communicated statements and conduct, made with the intent to place the person that is the target of the threat in reasonable fear for his or her safety or the safety of his or her family.

**§ 528.5 False Personation (Misdemeanor).** Any person who knowingly and without consent, credibly impersonates another actual person through or on an internet web site or by other electronic means for purposes of harming, intimidating, threatening, or defrauding another person is guilty of a public offense punishable pursuant to subdivision (d). The mere posting of publicly accessible information is not, in itself, a crime.

**§ 487 Grand Theft and § 484 Petty Theft.** Generally, the crime is investigated by the Area if the theft is committed on an auction site such as eBay or Craigslist. Wire transfers (MoneyGram or Western Union) or Green Dot Money Paks are used to facilitate a fraud.

**Exception**: When a file encrypting "ransomware" such as CryptoLocker is installed on a victim's computer. The Computer Crimes Unit will handle.

**§ 653 (m) No Threatening Email Act.** Every person who, with intent to annoy, telephones or makes contact by means of an electronic communication device with another and addresses to or about the other person any obscene language or addresses to the other person any threat to inflict injury to the person or property of the person addressed or any member of his or her family, is guilty of a misdemeanor.

**§ 653.2 Harassing Electronic Communication (Misdemeanor).** (The Penal Code title is Use of Electronic Communication to Instill Fear or to Harass) For brevity, the report may be titled "Har Elec Comm."

"Every person who, with intent to place another person in reasonable fear for his/her safety, or the safety of the other person's immediate family, by means of an electronic communication device, without consent of the other person, for the purpose of imminently causing that other person unwanted physical contact, injury, or harassment, by a third party, electronically distributes, publishes, emails, hyperlinks, or makes available for downloading personal identifying information, including, but not limited to; a digital image of another person, or an electronic message of a harassing nature about another person, which would likely incite or produce that unlawful action"

This section may be used for threats that do not meet the criteria of Criminal Threats, but the victim fears for their safety.

**Cyberbullying.** The State of California does not have a "cyberbullying" law. Interview the victim and determine if the circumstances meet the criteria of any existing criminal code section(s). If not, you may refer the victim to take civil action.

**Jurisdiction.** A computer-related crime may be perpetrated from a suspect's actions outside of the City of Los Angeles. However, if the victim lives or works in the City of Los Angeles, and the crime occurred to the victim while they were at their home or business in Los Angeles, it is a Los Angeles Police Department occurrence. If the suspect lives in the City of Los Angeles, but the crime is committed against a victim outside of the City limits, the victim is to be referred to their local law enforcement agency (LEA). As always, the LAPD may take courtesy reports for those victims and forward the report to the appropriate LEA.

**Internet Crime Complaint Center (IC3) Website IC3.GOV.** This is a clearinghouse for cybercrimes operated by the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). IC3 compiles statistics and provides updated information on current online scams or hoaxes. They take online complaints and make referrals to LEAs if there appears to be a criminal allegation. Law enforcement may refer people to IC3 who observed a scam or hoax on the internet but *are not a victim* of that hoax or scam. For example: Jim receives an email requesting money from Julie, who is out of the country and lost her purse. Jim realized it was a hoax and not Julie sending the email. Jim did not send any money and did not suffer a financial loss. This would be referred to IC3. If Jim had sent money, an Investigative Report (IR) would be taken.

**Reporting/Desk Officer Responsibilities.** Do not immediately refer victims to the CCU or to IC3.gov. Determine if a crime has been committed and take an IR, if applicable. Do not take the victim's computer(s) and/or cell phone(s) and book them as evidence. The investigating officer will determine what evidence is needed and will advise the victim.

**Detective Responsibilities.** Upon being assigned a computer-related crime, detectives must determine if any Internet Protocol (IP) addresses were captured during the commission of the crime. A preservation letter should be sent immediately to the carrier of the IP address to capture any subscriber information, data usage, etc., before the information expires or is deleted. Many carriers maintain subscriber information for as little as 28 days due to the high volume of business. Exemplars may be located on the CCD Divisional page on the Department Local Area Network (LAN) System. The preservation letter is only valid for 90 days, so the detective must follow up with a search warrant within that time period. If an Area detective is assigned a UCA report, the detective must immediately contact CCU and forward the report.

## III. FREQUENTLY USED TERMS.

**Auction Fraud:** Items are offered for sale on an online auction site that either does not exist, or one item is sold to multiple buyers. The most popular sites are Craigslist and eBay. This type of scam is no different than a suspect placing a car for sale in the Auto Trader or in the classified ads of the local newspaper.

**Denial of Service (DOS) Attack:** A website is taken over by a program installed on the computer, either in person or by a disguised link sent to the victim and then opened, and/or by remote access.

**Desktop Computer (Tower):** A stationary computer that has separate components such as a keyboard, mouse, monitor and speakers. They may be large or small.

**Hacking:** The unauthorized access to another's computer. This can be as simple as just figuring out someone's password, or as complex as writing a program to get past another computer's security.

**Internet Protocol (IP) Address:** A code made up of number(s) that identify a particular computer (or any electronic device) on the internet. Every computer requires an IP address to connect to the internet. Internet Protocol addresses consist of four sets of numbers from 0 to 255, separated by three dots. For example "66.72.98.236" or "216.239.115.148".

**Internet Service Provider (ISP) or Service Provider:** The company that provides access to the internet (e.g., Verizon, AT&T, Time Warner).

**Laptop:** Also known as a notebook or tablet, a laptop is a portable computer containing the screen, keyboard and mouse all in one device.

**Phishing:** Requesting confidential information over the internet under false pretenses in order to fraudulently obtain credit card numbers, passwords, or other personal data. For example: a suspect posing as a legitimate business and/or person may ask for funds to be wired, or ask the victim to click on a link and enter confidential information such as bank account/credit card numbers, passwords, social security numbers, etc., feigning that the card or account will be cancelled without receipt of the information.

**Search Engine:** A program that allows the user to search for information on the internet (e.g., Google, Bing, Yahoo).

**Secure/Non-Secure Internet Access:** Secure access requires a password to connect a device to the internet access point. Non-secure access is not password protected and could leave the internet connection vulnerable to hackers.

**Social Network:** A website that allows users to be part of a virtual community. Facebook, Twitter, Google and Instagram are currently the most popular.

**Spoofing:** Fraudulent emails in which the sender's email address and other parts of the email header are altered to appear as though the email originated from a different source.

**Uniform Resource Locator (URL):** The address of a specific website or file on the internet.

**Web Browser:** Often just called a "browser," this is a program used to access the internet. Some common browsers are Internet Explorer, Firefox, Safari, and Chrome.

**Wireless Carrier:** Companies that operate the wireless networks and oversee use of those networks (e.g., Verizon, Metro PCS, AT&T).

**Wireless Connections:** An internet connection without a cable or wire. The two most common are Wi-Fi and Bluetooth.

**Worldwide Web:** Or, the "web," is a globally connected network.

## IV. CHECKLIST FOR INVESTIGATIVE REPORTS.

**Reporting Officer: Document the applicable information in the narrative of your report.**

**For All Computer-Related Crimes.** Write a brief summary of the crime and include the following information, if known:

* Victim's ISP;
* Victim's IP address;
* Suspect's IP address;
* What type of connection (cable/wireless); and,
* Is the internet connection secure (yes/no)?

**Suspect(s):**

* Is the suspect known (include possible suspect information);
* What is the relationship between the suspect(s) and victim(s);
* List possible suspect(s) with all known identifiers in the narrative;
* Why does the victim suspect this particular individual or individuals;
* If the suspect is known, did the suspect ever have access to the victim's device; and,
* If the suspect is known, did the suspect ever have access to the victim's password(s)?

**Prior Court History Between Suspect and Victim.** Answer **all** questions for each court case:

* Type (civil court, family court, criminal court);
* Case number;
* Jurisdiction (city/county);
* Dates/times of court appearances;
* Case disposition (or if pending); and,
* Does the victim have copies of court transcripts?

## V. ADDITIONAL QUESTIONS FOR COMPUTER-RELATED CRIMES.

**If Email is Involved.**

* What is the email address targeted (list all);
* When was the last time the victim was able to access the email accounts(s);
* When did the victim regain access to the email account(s);
* Did the victim report the intrusion to their email provider (e.g., Yahoo, Gmail);
* Did the victim receive any notification from their ISP (e.g., password changes);
* Did the victim download their recent IP activity;
* Who is the ISP (e.g., Time Warner Cable, AT&T);
* If the suspect sent an email to the victim's account, does the victim have a copy of the email and the full header to the email;
* If the suspect sent an email from the victim's account, does the victim know the recipient(s) of the email; and,
* Did the recipient(s) save the suspect's email?

**If Social Media Accounts are Involved.**

* What social media accounts were targeted;
* What is the victim's account log on ID;
* When did the victim last access the social media account;
* When was the victim unable to access his/her social media account;
* Did the victim report the unauthorized access to the social media site (e.g., Facebook); and,
* Did the victim download their IP activity?

**Auction Fraud/Grand or Petty Theft Via a Purchase on the Internet.**

* What site was the ad posted on;
* Is the ad still on the site;
* Does the victim have a copy/screen shot of the ad;
* How did the victim pay for the item(s); and,
* Was the site contacted regarding the fraud?

**Non-business Related – Unauthorized Computer Access (Hack).**

* How many devices are affected ;
* Type of devices affected (e.g., desk top, laptop, tablet, notepad, cellular phone). If other, name device type;
* How many users on each device;
* Are the affected devices at home, work, or both;
* Is the device password protected; and,
* What data was deleted, copied, or altered?

**Business Related – Unauthorized Computer Access (Hack).**

* What data was deleted, copied or altered;
* Was a server involved;
* Does the victim have any server logs;
* Did the victim hire a forensic examiner;
* Does the victim have a copy of the examiner's report; and,
* If the company has an "Information Technology (IT)" person, what is that person's contact information?