



DEPARTMENT OF THE ARMY  
UNITED STATES ARMY CRIMINAL INVESTIGATION COMMAND

## CRIMINAL INTELLIGENCE SUMMARY

---

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

CRIMINTSUM 035-02

30 Aug 2002

CIOP-ACE (195)

230001R – 292400R Aug 2002

### WARNING

1. The Criminal Intelligence Summary (CRIMINTSUM) provides a periodic update of police intelligence information for law enforcement and security personnel, military commanders, intelligence analysts, and others with force protection duties. It does not include classified information.
2. Because the CRIMINTSUM is For Official Use Only and because it contains information protected by the Privacy Act, further distribution of these summaries is restricted to Department of Defense (DoD) and law enforcement agencies only, unless approval from Headquarters, US Army Criminal Investigation Command (USACIDC) has been obtained beforehand. Violations of the Privacy Act make both the releasing organization **and the person involved in the unauthorized release** liable in civil suits. Do not release information to the media or others without a valid need to know.
3. Information should not be released to the media, or other agencies within or outside DoD who have no valid need to know. This report contains privileged information, which must be protected. Further dissemination should be limited to a minimum, consistent with the purpose of supporting effective law enforcement and public safety. Persons or organizations violating distribution restrictions will be banned from receiving future USACIDC summary reports.

---

FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE

DISTRIBUTION: This document is provided for your information and use. It is intended for law enforcement and security personnel, military commanders, intelligence analysts, and other officials with a need to know. Further dissemination should be limited to a minimum, consistent with the purpose of supporting effective law enforcement and public safety. Copies of this document, enclosures thereto, and information therefrom will not be further released outside your agency without prior approval. Additional release requires prior approval from the USACIDC Deputy Chief of Staff for Operations, phone (703) 806-0300.

**FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE**

CIOP-ACE (195)

SUBJECT: Criminal Intelligence Summary 035-02

**A. DRUG RELATED**

**1. Methamphetamine Information:** The drug methamphetamine attacks the central nervous system and produces chemical changes in the regions of the brain that control emotions and such basic drives as hunger. The drug artificially stimulates the so-called "pleasure" areas, essentially cutting off the brain's normal chemical reactions. During their high, users typically show increased activity and a general feeling of well-being. As the drug wears off, the positive feeling fades and the user typically demands more of the drug. The pleasure/tension cycle can lead to addiction. The following website provides additional information: [www.valleymeth.com](http://www.valleymeth.com). Included links are a methlab locator focusing on California, [www.methvalley.com/graphics/locator.html](http://www.methvalley.com/graphics/locator.html); and a link to the worldwide meth website, [www.valleymeth.com/graphics/worldwide.html](http://www.valleymeth.com/graphics/worldwide.html) (McClatchy Company Newspapers).

**B. HOAXES / SCAMS**

**1. Identity Theft:** Identity theft or identity fraud is the taking of the victim's identity to obtain credit, credit cards from banks and retailers, steal money from the victim's existing accounts, apply for loans, establish accounts with utility companies, rent an apartment, file bankruptcy or obtain a job using the victim's name. Attachment 1 is an article written by the CID Intelligence Division concerning identity theft.

**2. Coca-Cola Urban Legend:** The "Coke" threat is an Urban Legend. Per <http://Snopes.com> and <http://urbanlegends.about.com>, e-mail messages continue to be forwarded with details about helpful terrorists or people of supposed Middle Eastern background warning kindly Americans to stay away from Coca-Cola. The versions cited above are simply re-workings of the "grateful stranger rewarding a helpful citizen with a warning about impending attack" type of tales that were circulating within a month of the September 11 terrorist attacks. These were applied to IRA terrorists (among others) years earlier and told in various forms, particularly in connection with wars, for several decades now. Nonetheless, this rumor continues to circulate in newer and newer versions that push the target date farther into the future to keep it current, saddling authorities with the task of debunking the same rumor over and over.

Examples of the alleged incidents are provided below for information purposes. An almost identical scenario was reported to authorities at Ft Leonard Wood, MO on 30 Aug 02 and is currently being investigated by CID.

Urban legend example #1: "On 18 Aug 02, a Middle Eastern man in line at a cash register in a Tomlinson's Dept Store in Myrtle Beach, SC, was \$1 or \$2 short and a woman in line made up the difference for him. The Middle Eastern man waited by the store door and

---

---

**FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE**

DISTRIBUTION: This document is provided for your information and use. It is intended for law enforcement and security personnel, military commanders, intelligence analysts, and other officials with a need to know. Further dissemination should be limited to a minimum, consistent with the purpose of supporting effective law enforcement and public safety. Copies of this document, enclosures thereto, and information therefrom will not be further released outside your agency without prior approval. Additional release requires prior approval from the USACIDC Deputy Chief of Staff for Operations, phone (703) 806-0300.

**FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE**

CIOP-ACE (195)

SUBJECT: Criminal Intelligence Summary 035-02

thanked the woman profusely. He then told her not to drink Coca Cola after 26 Aug 02, and that "they had found a way to get all Americans."

Urban legend example #2: "On 3 Aug 02, the FBI Communications Center received a telephone call from a male resident of Louisville, Kentucky. The caller advised that his girlfriend works as a cashier at WalMart in Louisville, and on Saturday an Arab man in her check out lane did not have enough money to cover his purchases. The female cashier gave him \$3.00 to cover the purchases. When the cashier was departing WalMart after completing her shift, the Arab man approached the cashier in the parking lot to thank her for the money. He told her he wanted to give her a hint, "to not drink coke after August 5."

**C. LAW ENFORCEMENT EFFORTS / SAFETY**

**1. Pepper Spray Pen:** The pen (see photo) resembles a normal writing instrument until the cap is removed. A spray button releases Pepper Spray when pushed. Law Enforcement and Security personnel should be cautious of these items as they can disable an Officer and may pass undetected through a security checkpoint (USCG).



**2. Marker Concealment Device:** This concealment device (see photo) was a standard "Marks a Lot" permanent marker. The top when removed reveals a standard felt tip for writing. The ink mechanism for the pen was removed and conceals a fully functional marijuana pipe. The hollowed out portion of the pen could also be used to conceal small knives, blades or handcuff keys. Law enforcement officers should be aware of this device and are also reminded to conduct thorough searches of persons arrested prior to transporting. An officer conducting a routine search located this device (Cincinnati Intelligence, Disseminated through O.C.T.A.G.O.N.).

---

---

**FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE**

DISTRIBUTION: This document is provided for your information and use. It is intended for law enforcement and security personnel, military commanders, intelligence analysts, and other officials with a need to know. Further dissemination should be limited to a minimum, consistent with the purpose of supporting effective law enforcement and public safety. Copies of this document, enclosures thereto, and information therefrom will not be further released outside your agency without prior approval. Additional release requires prior approval from the USACIDC Deputy Chief of Staff for Operations, phone (703) 806-0300.

**FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE**

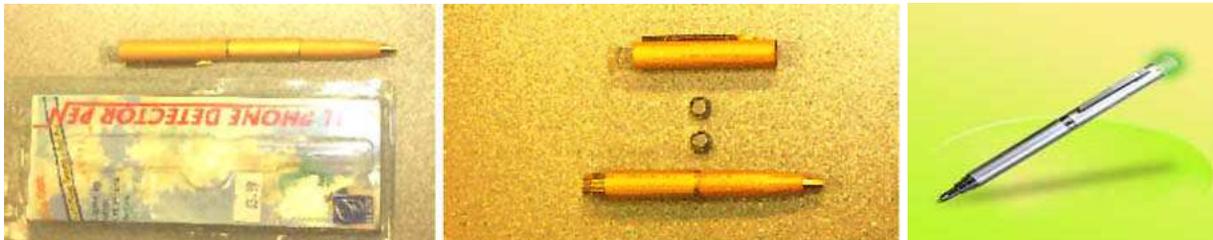
CIOP-ACE (195)

SUBJECT: Criminal Intelligence Summary 035-02



Concealment Device

**3. Cell Phone Detector Pen:** Special ink pens designed to signal incoming cell phone calls may also detect police body wires, cell phone wires, video transmitters, and other undercover police equipment. The pens are marketed to alert owners of incoming cell phone calls when the phone ringer is off. They will receive transmissions between the 800MHz to 2.4GHz range. The device is a working pen – gold or silver in color. The upper portion contains two small watch batteries which power the receiver. On the top of the device is a clear push top. When the receiver is activated, it will flash a red LED signal indicating a device is present. The receiver will activate between 5 – 10 feet of the radio signal. Law enforcement officers need to be aware of this device, particularly officers operating in undercover or covert operations. If you encounter this type of device, you should immediately cease transmission from covert police equipment. The devices are marketed on the Intranet through various websites including [www.globalsources.com](http://www.globalsources.com) and [www.geekpens.com](http://www.geekpens.com) (Cincinnati Intelligence, Disseminated through O.C.T.A.G.O.N.).



**4. Production/Sale of M-4 Replica Paintball Gun:** An M-4 Real Action Marker (RAM) paintball gun is being manufactured and sold by Asia Paintball Supply Company, Unit B, 22/F, 77 Wang Lung Street, Richwealth Industrial Bldg, Tsuen Wan, Hong Kong, Tel (852) 2409-4466, Fax (852) 2409-9632, [www.asiapaintball.com](http://www.asiapaintball.com), [aps@asiapaintball.com](mailto:aps@asiapaintball.com). The M-4 RAM is an exact replica of the US Army issued M-4 rifle to include ejecting spent cartridges and feeding a new paintball cartridge through a magazine feed system (CID, Redstone Resident Agency, 0120-02).

**5. Hidden, Hand-Held Weapon:** The weapon depicted (see photo) was found on an individual after he was ordered removed in the Honolulu district court. Subject was in the

---

**FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE**

DISTRIBUTION: This document is provided for your information and use. It is intended for law enforcement and security personnel, military commanders, intelligence analysts, and other officials with a need to know. Further dissemination should be limited to a minimum, consistent with the purpose of supporting effective law enforcement and public safety. Copies of this document, enclosures thereto, and information therefrom will not be further released outside your agency without prior approval. Additional release requires prior approval from the USACIDC Deputy Chief of Staff for Operations, phone (703) 806-0300.

**FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE**

CIOP-ACE (195)

SUBJECT: Criminal Intelligence Summary 035-02

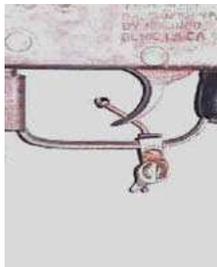
Immigration Court, located in the Federal building, (**having already gone through one security inspection**). When the subject was ordered removed, the Detention Enforcement Officer took him into custody and conducted a more thorough search. **Reminder, even though someone was screened and is in a secure area doesn't mean that he is unarmed.** The referenced weapon is 5" long with two 2" prongs set about an inch apart (DOJ).



**6. High Rate-of-Fire Trigger Modifier:** A weapon was recovered on 30 Jul 02 by members of the Cincinnati Police during execution of a drug related search warrant. An MAK-90, (AK-47 variant) rifle recovered was equipped with a "Hell-Fire Trigger System" (also marketed under the name of "Hell-Storm 2000"). This trigger attachment interferes with normal operation of a semi-automatic firearm by causing a "static" condition and allowing the bolt to repeatedly slam against the firing pin to simulate fully automatic gunfire. Depending on the type of firearm on which it is installed, it can produce a firing rate of approximately 10 to 15 rounds per second. The devices are marketed on the Internet through various websites including [www.perfectgiftgetter.com](http://www.perfectgiftgetter.com) (Cincinnati Police Intelligence Unit, (513) 564-2200).



Rifle with device



Trigger-guard



Close-up of device

---

**FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE**

DISTRIBUTION: This document is provided for your information and use. It is intended for law enforcement and security personnel, military commanders, intelligence analysts, and other officials with a need to know. Further dissemination should be limited to a minimum, consistent with the purpose of supporting effective law enforcement and public safety. Copies of this document, enclosures thereto, and information therefrom will not be further released outside your agency without prior approval. Additional release requires prior approval from the USACIDC Deputy Chief of Staff for Operations, phone (703) 806-0300.

**FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE**

CIOP-ACE (195)

SUBJECT: Criminal Intelligence Summary 035-02

**D. LARCENY METHODS OF OPERATION**

**1. Larceny of Government Funds:** Between Jan 00 and Jul 01, an employee systematically stole \$17,392.55 in cash payments from a Child Development Center (CDC). The payments were voided or changed on the DA Forms 1992 (Non-Appropriated Fund Receipt Vouchers) and marked paid on the patron's payment card. The money collected on the DA Form 1992 was not recorded on a cash register system, but on hand written receipts only. These changes were manually made to the DA Form 1992 by either voiding the payment entirely or by changing certain numbers to show less cash. The actual amount paid by the patron was marked on their payment card and then the cash was stolen from the facility. The payment cards and a copy of the DA Form 1992 were retained locally, while another copy of the DA Form 1992 was forwarded to the Central Accounting Office (CAO). Neither the first line supervisor, nor the auditor at the CAO ever questioned the numerous voids and manual changes to the DA Form 1992, thereby allowing the theft to go undetected. A command audit of the CDC comparing the payment cards, DA Forms 1992, and the daily activity reports revealed the systematic larceny by an employee (CID, Ft. Drum, 0218-02).

**E. INTERNATIONAL INVESTIGATIVE EFFORTS**

**1. Tanzania - USA Sign Accord to Combat Illegal Money Transfers:** The US and the government of Tanzania have signed an agreement to assist the Tanzanian government officials in building their capacity to combat crimes relating to illegal money transfers. The agreement will assist Tanzania to combat crimes relating to money transfers carried out illegally. According to the finance minister, Hon Basil Mramba, the agreement will enable Tanzania to investigate and prosecute those engaged in criminal activities. According to the US ambassador to Tanzania, Robert Royall, the US decided to sign this agreement after Tanzania expressed interest in combating illegal money transfers. The agreement is part of the US's efforts to combat international terrorism (FBIS, Radio Tanzania).

**2. Driver's Licenses from Province of Quebec, Canada:** Beginning 3 Sep 02, licenses bearing photographs (probationary or first-time licenses) will no longer be handed out at the Societe's service outlets. Instead, they will be sent directly to license holders by mail within a few days following the procedure. Intended to issue official documents in a more secure manner, this new step is in keeping with the major ongoing endeavors that have been implemented since the fall of 2001 to ensure optimal service and more intensive checks on applicants' identities (NLETS).

---

---

**FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE**

DISTRIBUTION: This document is provided for your information and use. It is intended for law enforcement and security personnel, military commanders, intelligence analysts, and other officials with a need to know. Further dissemination should be limited to a minimum, consistent with the purpose of supporting effective law enforcement and public safety. Copies of this document, enclosures thereto, and information therefrom will not be further released outside your agency without prior approval. Additional release requires prior approval from the USACIDC Deputy Chief of Staff for Operations, phone (703) 806-0300.

**FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE**

CIOP-ACE (195)

SUBJECT: Criminal Intelligence Summary 035-02

**F. OTHER POLICE INTELLIGENCE**

**1. BOLO Missing Taiwanese Fishing Vessel Hsing Lung:** The US Coast Guard is currently investigating the possible conversion (hijacking) of the Taiwanese fishing vessel 'Hsing Lung' (see photo). On 15 Aug 02, the USCG received a report from the vessel's owner that nine People's Republic of China (PRC) crewmen took over the vessel, and it was headed east. 'Hsing Lung' was last known to be operating 1,200 nautical miles Northeast of Guam as of 11 Aug 02. The owner of the 'Hsing Lung' believes the vessel may attempt to reach Southern California. The vessel normally operates up to four months at sea without logistics support and would be capable of making the voyage. The USCG projects the vessel would arrive off Southern California between September 3 and 15 with the most likely arrival window 7 through 10 Sep. There have been two confirmed conversion events that offloaded to Southern California beaches: (1) 21 May 01 to Black's Beach in San Diego County; (2) 23 May 02 to Crystal Cove State Park in Orange County. Vessel sightings or personnel landings should be reported to the USCG and the Immigration and Naturalization Service (INS).

**Cautionary Note:** In April 01, PRC crewmen converted the Taiwanese fishing vessel Chun Fu Yu No. 17. The crew carried Improvised Explosive Devices (IEDs) for use against law enforcement. A Bureau of Alcohol, Tobacco, and Firearms (BATF) laboratory analysis of the IEDs indicated they were capable of causing significant property damage, injury or death. The IEDs were described as round softball size objects containing a gray substance with a short fuse. The crew claimed the IEDs were made for use against law enforcement, military, or coast guard who might attempt to stop and board the vessel prior to its final destination of Guam. There have been growing numbers of converted fishing vessels used to smuggle "crewmembers" into Guam, Hawaii, and the North America mainland since Jun 00. While there is reason to suspect most masters are complicit, there have been documented cases of violence against Taiwanese masters. Explosives are not uncommon on Asian fishing vessels and may be used for fishing; however, the intent of the crewmen on the Chun Fu Yu No. 17 and the capability of their IEDs pose a severe threat to law enforcement personnel. Crews involved in smuggling ventures are likely to be prosecuted here in the US and/or Taiwan, which increases the potential for resisting arrest (USCG).



---

---

**FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE**

DISTRIBUTION: This document is provided for your information and use. It is intended for law enforcement and security personnel, military commanders, intelligence analysts, and other officials with a need to know. Further dissemination should be limited to a minimum, consistent with the purpose of supporting effective law enforcement and public safety. Copies of this document, enclosures thereto, and information therefrom will not be further released outside your agency without prior approval. Additional release requires prior approval from the USACIDC Deputy Chief of Staff for Operations, phone (703) 806-0300.

**FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE**

CIOP-ACE (195)

SUBJECT: Criminal Intelligence Summary 035-02

Point of contact for this report is SA Mary Ann Wolfe or SA Joe Garrett (703) 806-4902 / 4910, e-mail [Mary A Wolfe@Belvoir.army.mil](mailto:Mary_A_Wolfe@Belvoir.army.mil) or [Joe.Garrett@us.army.mil](mailto:Joe.Garrett@us.army.mil). Criminal Intelligence Summaries may also be viewed at the FBI's Law Enforcement OnLine (LEO) intranet (<http://www.fbi.gov/hq/cjisd/leo.htm>) in the Law Enforcement Sensitive Communications section and the Military Law Enforcement Special Interest Group.

---

---

**FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE**

DISTRIBUTION: This document is provided for your information and use. It is intended for law enforcement and security personnel, military commanders, intelligence analysts, and other officials with a need to know. Further dissemination should be limited to a minimum, consistent with the purpose of supporting effective law enforcement and public safety. Copies of this document, enclosures thereto, and information therefrom will not be further released outside your agency without prior approval. Additional release requires prior approval from the USACIDC Deputy Chief of Staff for Operations, phone (703) 806-0300.

**FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE**

CIOP-ACE (195)

SUBJECT: Criminal Intelligence Summary 035-02

**ATTACHMENT 1**

**Identity Theft**

Identity theft or identity fraud (true name fraud) is the taking of the victim's identity to obtain credit, credit cards from banks and retailers, steal money from the victim's existing accounts, apply for loans, establish accounts with utility companies, rent an apartment, file bankruptcy or obtain a job using the victim's name. Impersonators may steal thousands of dollars in a victim's name without the victim knowing about it for months or years<sup>1</sup>. According to the Federal Bureau of Investigation, identity theft is one of the fastest growing white-collar crimes in the nation<sup>2</sup>. More than 500,000 consumers are victimized each year by identity theft<sup>3</sup>; and the Army community experiences the same criminal losses as the communities surrounding bases.

Perpetrators spend countless hours retrieving personal and financial data from compromised computer systems, the Internet, unattended offices, unlocked mailboxes and unshredded trash, with the intention of using the information or selling it to other thieves. Information such as complete names, addresses, financial account numbers, identifying numbers such as Social Security numbers, dates of birth, tax records, canceled checks, credit card statements, and places of birth, are the most collected items (HQ, USACIDC).

Law enforcement guidance<sup>4</sup> to prevent identity theft includes the following tips:

- Order and closely review biannual copies of your credit report from each national credit reporting agency.
- Remove your name from mailing lists for pre-approved credit lines.
- Remove your name from marketers' unsolicited mailing lists.
- Only release your personal data (Social Security number, date of birth, bank account or credit account numbers, etc.), to agencies that require it for action you have initiated. Never give this information to unsolicited telephone callers or over the Internet.
- Request that the Department of Motor Vehicles assign an alternate driver's license number if it currently features your Social Security number.
- Shred all documents containing personal information.
- Ensure that your PIN numbers cannot be observed by anyone while you're utilizing an ATM or public telephone.

---

---

**FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE**

DISTRIBUTION: This document is provided for your information and use. It is intended for law enforcement and security personnel, military commanders, intelligence analysts, and other officials with a need to know. Further dissemination should be limited to a minimum, consistent with the purpose of supporting effective law enforcement and public safety. Copies of this document, enclosures thereto, and information therefrom will not be further released outside your agency without prior approval. Additional release requires prior approval from the USACIDC Deputy Chief of Staff for Operations, phone (703) 806-0300.

**FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE**

CIOP-ACE (195)

SUBJECT: Criminal Intelligence Summary 035-02

- Close all unused credit card or bank accounts.
- Contact your creditor or service provider if expected bills don't arrive.

For information concerning resolving credit problems caused by identity theft, see Fair Credit Billing and Avoiding Credit and Charge Card Fraud:

<http://www.consumer.gov/idtheft>.

<sup>1</sup> SSG Marcia Triggs, Army Link News, "Scams Target Veterans for Identity Theft," 22 JAN 02.  
William Stakes, Stuttgart online community news, "Identity Thieves Target Military Members," 9 APR 02. Sandy Goss, Soldiers online, "Beware the Identity Thieves," SEP 00.

<sup>2</sup> M.J. Frank and Associates, [www.IdentityTheft.org](http://www.IdentityTheft.org).

<sup>3</sup> Testimony of the United States Secret Service to the House Committee on Banking and Financial Services, September 13, 2000.

<sup>4</sup> "Protecting Yourself Against Fraud," FBI, 9 SEP 1997.

---

---

**FOR OFFICIAL USE ONLY - LAW ENFORCEMENT SENSITIVE**

DISTRIBUTION: This document is provided for your information and use. It is intended for law enforcement and security personnel, military commanders, intelligence analysts, and other officials with a need to know. Further dissemination should be limited to a minimum, consistent with the purpose of supporting effective law enforcement and public safety. Copies of this document, enclosures thereto, and information therefrom will not be further released outside your agency without prior approval. Additional release requires prior approval from the USACIDC Deputy Chief of Staff for Operations, phone (703) 806-0300.