



governmentattic.org

"Rummaging in the government's attic"

Description of documents: **US Department of Homeland Security, US Secret Service (USSS) USSS Intranet Webpages for the Office of Investigation and the Investigation Strategic Plan**

Requested date: 10-August-2004

Released date: 22-August-2007

Posted date: 03-October-2007

Document date: Documents printed 15-February-2007

Source of document: Department Of Homeland Security
United States Secret Service
Freedom of Information and Privacy Acts Branch
245 Murray Drive
Building 410
Washington, D.C. 20223

FOIA Requestor Service Center
Disclosure Officer
Phone: 202-406-6370
Fax: 202-406-5154
Email: FOIA@uss.s.dhs.gov (as of posting date)

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file.



DEPARTMENT OF HOMELAND SECURITY
UNITED STATES SECRET SERVICE
 WASHINGTON, D.C. 20223

Freedom of Information and Privacy Acts Branch
 245 Murray Drive
 Building 410
 Washington, D.C. 20223

AUG 22 2007

File Number: 20040530 - 20040532

Dear Requester:

Reference is made to your Freedom of Information and/or Privacy Acts request originally received by the United States Secret Service on August 10, 2004, for information pertaining to the following files: File No. 20040530 – Copy of the USSS Intranet Webpage for the Office of Investigation; File No. 20040531 – Copy of the Investigation Strategic Plan; and File No. 20040532 – Copy of the Investigation Briefings to the Director during the years 2000 to the present.

Enclosed are copies of documents from Secret Service records. The referenced material was considered under both the Freedom of Information Act, Title 5, United States Code, Section 552 and/or the Privacy Act, Title 5, United States Code, Section 552a. Pursuant to the Acts, exemptions have been applied where deemed appropriate. The exemptions cited are marked below.

In addition, approximately 426 page(s) were withheld in their entirety. An enclosure to this letter explains the exemptions in more detail.

If this boxed is checked, deletions were made pursuant to the exemptions indicated below.

Section 552 (FOIA)

<input type="checkbox"/> (b) (1)	<input checked="" type="checkbox"/> (b) (2)	<input checked="" type="checkbox"/> (b) (3) Statute:	<input type="checkbox"/> (b) (7) (A)	<input type="checkbox"/> (b) (7) (B)
<input type="checkbox"/> (b) (4)	<input checked="" type="checkbox"/> (b) (5)	<input checked="" type="checkbox"/> (b) (6)	<input type="checkbox"/> (b) (7) (F)	<input type="checkbox"/> (b) (8)
<input checked="" type="checkbox"/> (b) (7) (C)	<input checked="" type="checkbox"/> (b) (7) (D)	<input checked="" type="checkbox"/> (b) (7) (E)		

Section 552a (Privacy Act)

(d) (5) (j) (2) (k) (1) (k) (2) (k) (3) (k) (5) (k) (6)

The following checked item(s) also apply to your request:

Some documents originated with another government agency(s). These documents were referred to that agency(s) for review and direct response to you.

page(s) of documents in our files contain information furnished to the Secret Service by another government agency(s). You will be advised directly by the Secret Service regarding the releasability of this information following our consultation with the other agency(s).

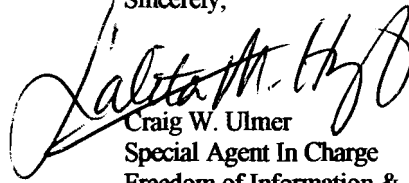
Other: .

Fees: .

If you disagree with our determination, you have the right of administrative appeal within 35 days by writing to Freedom of Information Appeal, Deputy Director, U.S. Secret Service, 245 Murray Drive, Building 410, Washington, DC 20223. If you do decide to file an administrative appeal, please explain the basis of your appeal.

Please use the file number indicated above in all future correspondence with the Secret Service.

Sincerely,

A handwritten signature in black ink, appearing to read "Craig W. Ulmer", written over a horizontal line.

Craig W. Ulmer
Special Agent In Charge
Freedom of Information &
Privacy Acts Officer

Enclosure: FOIA and Privacy Act Exemption List

**FREEDOM OF INFORMATION ACT
SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552**

Provisions of the Freedom of Information Act do not apply to matter that are:

- (b) (1) (A) specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;
- (b) (2) related solely to the internal personnel rules and practices any agency;
- (b) (3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
- (b) (4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (b) (5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
- (b) (6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (b) (7) records or information compiled for law enforcement purposes, but only to the extent that the information: (A) could reasonably be expected to interfere with enforcement proceedings; (B) would deprive a person of a right to a fair trial or an impartial adjudication; (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy; (D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source; (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law; (F) could reasonably be expected to endanger the life or physical safety of any individual;
- (b) (8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for regulation or supervision of financial institutions;
- (b) (9) geological and geophysical information and data, including maps, concerning wells.

**PRIVACY ACT
SUBSECTIONS OF TITLE 5, UNITED STATES CODE, SECTION 552a**

The provisions of the Privacy Act do not apply to:

- (d) (5) material compiled in reasonable anticipation of civil action or proceeding;
- (j) (2) material reporting investigative efforts pertaining to enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;
- (k)(1) material is currently and properly classified pursuant to an Executive Order in the interest of national defense or foreign policy;
- (k) (2) material compiled during investigations for law enforcement purposes;
- (k) (3) material maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of Title 18;
- (k) (5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or for access to classified information, but only to the extent that the disclosure of such material would reveal the identity of the person who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or prior to the September 27, 1975, under an implied promise that the identity of the source would be held in confidence;
- (k) (6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process;

OFFICE OF INVESTIGATIONS

Office of Investigations

- » [Staffing Chart](#)
- » [Investigations Strategic Plan](#)
- » [INV Briefings to the Director](#)

Field Offices

- » [Geographic Jurisdiction](#)
- » Foreign Offices
- » Interpol
- » [International Programs](#)
- » [Miami Field Office](#)
- » [New York Field Office](#)
- » [Oklahoma City Field Office](#)

Administration

- » Budget & Space
- » Awards
- » Vehicles
- » [Manpower Guidelines](#)
- » Special Projects

Vision Statement

Strategy for the Future

- Prioritize investigative cases, focusing our limited resources on those investigations having significant economic and community impact, involve organized criminal groups, are multi-district or transnational in nature, and utilize schemes involving new technologies.

- Maintain a leadership role in the protection of the financial service infrastructure of our nation through aggressive investigation and risk assessment.

- Recommend industry safeguards to prevent fraud based on identification and assessment of systemic weaknesses.

- Expand our overseas presence in support of our investigative and protective missions.

- Increase liaison, training, and other services to foreign financial institutions and law enforcement agencies to stem the flow of foreign manufactured counterfeit U.S. currency and financial crimes that victimize our country's citizens and financial institutions.

- Promote public awareness of Secret Service investigative programs through increased cooperation with the media.

- Develop a criminal information operation to identify and analyze emerging trends in criminal activity in support of our dual mission.

- Strive to recruit, develop, and retain a qualified, diverse workforce that is worthy of the public's trust and confidence.



Operational Divisions

- » [Public Education Seminar Database](#)
- » [Counterfeit Section](#)
- » [Financial Crimes Section](#)
- » [FSD](#)
- » [ISD](#)

Resources

- » [Boys and Girls Club Bulletin Board](#)
- » [CAAP Bulletin Board](#)
- » [Links](#)
- » *Supervisors MUST be consulted before adding names to this form.*
[Registration for CFT/FCD Seminars](#)
- » [Report Templates and Guidelines](#)

This site has been accessed 87074 times since November 28, 2000.
 Content on this site is managed by (b) (6), (b) (7) c, Office of Investigations.
 This page was last modified 1/26/2005.

▶▶ [Investigations](#) | [Counterfeit Section](#)

NavDefault

Page 1 of 1

- [Training Sessions Management](#)
- [Counterfeit International Contacts](#)
- [CFT Tickler](#)
- [CFT Tickler - Calendar View](#)

COUNTERFEIT SECTION

Office of Investigations

About CFT

- » [Counterfeit K-9 Program](#)
 - » [K-9 Calendar](#)
- » [Regions](#)
- » [Research Section](#)
- » [Special Operations Branch](#)
 - » [\(b\) \(2\) High, \(b\) \(7\) e](#)
 - » [Operation Smack-Back](#)
 - » [New Orleans, LA](#)
- » [Staffing Chart](#)
- » [Technology Section](#)

[Cases of Interest Archive](#)
(requires login)

New

[Introduction of the Redesigned Currency Series \\$50](#)

[Sample Images of Redesigned Currency](#)



Frequently Asked Questions

- » [CCS Bulletin Board](#)
- » [General](#)
- » [ICR](#)
- » [Mainframe CCS/CFT](#)

[Introduction of the Redesigned Currency Series \\$20](#)

[Record of Plant Suppression](#)

[Europol CY-2002 Annual Report](#)

[Counterfeit Reference Papers](#)

Educational Materials

- » [Euro Webpage](#)
- » [Booklets and Pamphlets](#)
- » [CD-ROM and Videotapes](#)
- » [Posters and Fliers](#)

[Record of New Counterfeit](#)

[Abandonment Issues Relating to CFT \(per Legal\)](#)

[Policy Directive for New SSF 3115 \(FSD-24/Inv Manual\)](#)

[New Version of SSF 3115 \(Request for Service\)](#)

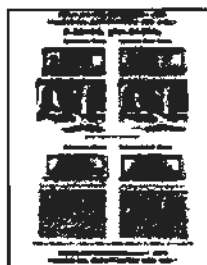
Resources

- » [Certificate of Destruction](#)
- » [CFTUSA Router Messages](#)
- » [Counterfeit Statutes](#)
- » [DocuShare](#)
- » [General Links](#)
- » [Internet Monthly](#)
- » [Morning Reports](#)
- » [Counterfeit Examination Equipment](#)

(b) (2) High, (b) (7) e

[Defects Genuine versus CFT](#)

For a copy of the defect sheet, contact Counterfeit Division.



(b) (2) High, (b) (7) e - Notes are Being Printed on Iraqi Currency Paper

Database Applications

- » [CFT Evidence Tracking DB](#)
- » [CCS Change Form](#)
- » [CCS Change Request Status](#)

(b) (2) High, (b) (7) e Database

(b) (2) High, (b) (7) e Database

- » [RAID Instruction Manual](#)
- » [Public Education Database](#)

Public Education and Training

- » [Case Classification Codes](#)
- » [CFT Reference Sheet](#)
- » [Counterfeit Internet Website](#)
- » [Power Point Presentations](#)
- » [Technology Information Guide](#)
- » [Counterfeit Seminar Interest Form](#)
- » [Counterfeit Seminar Interest](#)

» [Sample Reports](#)

» [Statistics](#)

This site has been accessed 54362 times since June 30, 2000.
Content on this site is managed by (b) (6) Counterfeit Division.
This page was last modified 1/26/2005. (b) (6), (b) (7) c

StarSafe_SiteMap

Page 1 of 1

»» [Investigations | Financial Crimes Section](#)

NavDefault

Page 1 of 1

- [Case Types Application](#)
- [Skimming Application](#)
- [Facility Scheduler](#)
- [Suspicious Activity Reports \(SARs\)](#)
- ⊕ [SAR Administration](#)
- [Electronic Crimes Special Agent Program \(ECSAP\)](#)

FINANCIAL CRIMES SECTION

About FCD

- » [Asset Forfeiture Branch](#)
- » [Electronic Crimes Branch](#)
- » [Financial Fraud Branch](#)

Applications

- » [Case Types](#)
- » [FCD on Docushare](#)

Resource Information

- » [Overseas Initiatives](#)
- » [Federal Rules of Criminal Procedure](#)

News & Announcements

[Counterfeit Document Database Passwords](#)

The format of the [Case Types](#) application has changed. Clicking the link takes you first to a search form. Enter any desired search criteria (or leave blank to view all case types which will take more time to download) then click "Search" to display case types records.

Contact Information

No Current Information

Top links and Information

[ESCAP Program](#) - Electronic Crimes Special Agent Program.

[AFB Quick Reference](#) - Asset Forfeiture Branch Quick Reference.

Content on this site is managed by Criminal Research Specialist (b) (6), (b) (7)(C) Crimes Division.
Last updated on 01/26/2005.

▶▶ [Investigations](#) | [Forensic Services Divison](#)

NavDefault

Page 1 of 1

- [Evidence Tracking Database](#)

Forensic Services Division

Office of Investigations

General Information

- » [Frequently Asked Questions \(FAQ's\)](#)
- » [Division Profile](#)
- » [Research and Development](#)
- » [Roster](#)
(requires login)

New

The [KISS Guide](#) for EVID (paperless SSF1544's) provides an easy approach to utilize the EVID system.

*Revised 10/25/01
pdf format requires [Adobe Acrobat Reader](#)*



Programs

- » [FSD/FCD joint financial crimes database](#)
- » [MEC \(Missing and Exploited Children\)](#)
- » [KIDS System](#)

This Web page was produced to provide information to USSS personnel via the network. Any suggestions would be appreciated.

- [Collection and Preservation of Evidence](#)

Other useful information:

Check the [status](#) of a case?
How to [request](#) forensic services?

[Investigator's Guide to Forensic Services](#)

Many [financial crimes](#) involve counterfeit documents produced with state-of-the-art technologies. [Photographs](#) depicting some of these printing processes are provided here.

Branches

- » [Questioned Document Branch](#)
- » [Identificaton Branch](#)
- » [Polygraph Branch](#)
- » [Visual Information Branch](#)
- » [Branch Photos](#)

Contact Information

- » [Contact List](#)
- » [Employee List with Phone Numbers](#)
(requires login)

b3, 7E

▶▶ Investigative Support Division

NavDefault

- Accident/Tort Claims
- Duty Desk Stats
- ☒ MCI Change Form
- MCI Change Jobs
- TECS Lookout Database
- Victim/Witness Assistance
Monthly Report
- Warrants

INVESTIGATIVE SUPPORT DIVISION

24-Hour Dutydesk: (b) (2) Low or Toll Free (b) (2) Low

Organization

- » [Mission Statement](#)
- » [Organizational Chart](#)
- » [Programs & Services](#)
- » [Operations Desk](#)

Databases

- » [TECS](#)
- » [NCIC](#)
- » [NLETS](#)
- » [MCI](#)
- » [Commercial Databases](#)
- » [Criminal Databases](#)
- » [ADNET](#)

Documents

- » [Original Airport Codes](#)
- » [Latest Airport Codes](#)



Investigative Support Division (ISD) provides advanced investigative analytical support services, through the use of elaborate commercial and criminal computer databases, that assist in the identification of significant criminal activity and in the preparation of evidence for judicial presentations. ISD evaluates the Secret Service information requirements for criminal intelligence, conducts administrative investigations, and locates assets targeted for forfeiture.

Transfer of the CSUR Database and CSUR Call-In Desk to Intelligence Division

As of Monday, September 20, 2004, the CSUR Database and CSUR Call-In Desk will be transferred from ISD to the Intelligence Division. [Click here for more information.](#)

Criminal Research Specialist

- » [Program Description](#)
- » [RAID Database](#)
- » [Locations](#)

Victim & Witness Assistance Program

- » [General Information](#)
- » [Handbook](#)
pdf 227Kb
- » [Victim of Fraud Flyer](#)
pdf 86Kb
- » [Training Presentation](#)
ppt 1Mb

PDF files require [Adobe Acrobat Reader](#)

Links

- » [Informative](#)
- » [Investigative](#)
- » [General](#)

Content on this site is managed by (b) (6) Investigative Support Division.
Last updated on 10/06/2004.

(b) (6) , (b) (7) c

Investigative Strategy for Today and the Future

Case Prioritization and Case Management

Prepared by:
United States Secret Service
Office of Investigations

Contents

Strategy for the Future

Investigative Strategic Goal
(Means and Strategies from our Strategic Plan)

Transnational and Financial Crimes Overview

Case Management
(Foreword from Investigative Manual Chapter INV-35)

Investigative Priorities
(Message to the field from CFT and FCD, Spring 2000)

In Custody Response Reporting

Case Prioritization Guidelines
(Secondary Case Types)

Investigations Main Page

Strategy for the Future

- Prioritize investigative cases, focusing our limited resources on those investigations having significant economic and community impact, involve organized criminal groups, are multi-district or transnational in nature, and utilize schemes involving new technologies.
- Maintain a leadership role in the protection of the financial service infrastructure of our nation through aggressive investigation and risk assessment.
- Recommend industry safeguards to prevent fraud based on identification and assessment of systemic weaknesses.
- Expand our overseas presence in support of our investigative and protective missions.
- Increase liaison, training, and other services to foreign financial institutions and law enforcement agencies to stem the flow of foreign manufactured counterfeit U.S. currency and financial crimes that victimize our country's citizens and financial institutions.
- Promote public awareness of Secret Service investigative programs through increased cooperation with the media.
- Develop a criminal information operation to identify and analyze emerging trends in criminal activity in support of our dual mission.
- Strive to recruit, develop, and retain a qualified, diverse workforce that is worthy of the public's trust and confidence.

[Table of Contents](#) | [Next](#)

INVESTIGATIVE STRATEGIC GOAL REDUCE CRIMES AGAINST OUR NATION'S CURRENCY AND FINANCIAL SYSTEM.

Objective - Reduce losses to the public attributable to counterfeit currency and financial crime under the jurisdiction of the Secret Service.

Means & Strategies

- Prioritize investigative cases, focusing on economic and community impact, involvement of organized criminal groups, multi-district and transnational investigations, and schemes involving new technologies.
- Maintain a leadership role in the protection of the financial service infrastructure through aggressive investigation and risk assessment.
- Recommend industry safeguards to prevent fraud based on identification and assessment of systemic weaknesses.

Objective - Reduce transnational financial crime under the jurisdiction of the Secret Service.

Means & Strategies

- Expand our overseas presence in support of our investigative and protective missions.
- Increase liaison, training, and other services to foreign financial institutions and law enforcement agencies to stem the flow of foreign manufactured counterfeit U.S. currency and financial crimes victimizing U.S. financial institutions.

Objective - Enhance partnerships with foreign and domestic stakeholders.

Means & Strategies

- Increase communication and cooperation with members of the financial services and reprographics industries, law enforcement agencies and prosecutors, and the information technology sector.
- Continue to educate congressional leaders and their staff regarding our investigative mission, foreign and domestic. Suggest statutory changes to more effectively investigate and prosecute crimes under our jurisdiction.
- Promote public awareness of Secret Service investigative programs.

Objective - Aggressively support the protective mission of the Secret Service with field investigative capabilities.

Means & Strategies

- Expand participation in Joint Terrorist Task Forces by lending additional support in tracing terrorists' financial assets and investigating false identification cases.
- Continue to apply computer crime initiatives to protective intelligence cases in the area of Internet threats and investigate groups/individuals that may pose a threat to our protectees.
- Promote field liaison with local law enforcement to assist in preventing targeted violence.
- Enhance a Special Event Staffing and Response Plan to provide for a rapid response team to gather and analyze investigative information on individuals or groups who have threatened our protectees or designated national security events.

[Previous](#) | [Table of Contents](#) | [Next](#)

Transnational and Financial Crimes

[The Globalization of Crime](#) | [The Internet](#) | [High Tech Crime](#) | [Electronic Benefits Transfer Identity Theft](#) | [Foreign Office Expansion Initiative](#) | [The Electronic Crimes Special Agent Program](#)

Introduction

The United States Secret Service mission in the arena of criminal investigations has been historically characterized by its preventive and proactive nature. The focus of this investigative program is the protection of our nation's payment systems and financial infrastructure and is not redundant with the investigative programs of other Federal law enforcement agencies. Our unique core criminal violations concern the counterfeiting of the currency of the United States (and other nations), and fraud perpetrated against the U.S. Government, the citizens of the United States, and American business operations.

The highlights of our comprehensive investigative program include an aggressive public education and awareness campaign and a proactive approach to criminal investigations in general, focusing our resources on investigations of significant economic and community impact. The Secret Service has forged strong alliances with our private industry partners and promotes the "Task Force" approach in our field offices throughout the United States and in our offices abroad. This method allows us to tailor our investigative programs to the local community, thus maximizing favorable public and economic impact.

The Globalization of Crime

As the result of globalization and the information technology revolution, criminals now have the ability to victimize financial institutions or individuals outside their country of origin by:

- Solely electronic means
- Negotiating instruments locally that are of foreign origin or issue
- Working with foreign based co-conspirators
- Taking advantage of differences in legal systems

Traditional concepts of jurisdiction and venue need to be reconsidered--old notions fail to address international criminality. Example: suppose a hacker in Romania breaks into a computer system in New York and copies a database containing credit card account numbers to a computer system in San Jose. A co-conspirator then accesses these accounts, and uses some of the numbers to place an Internet order for \$75,000 of computer equipment from a business in Utah, and has the merchandise shipped to Khazakstan. To complicate matters further, suppose that all of the compromised accounts are from a Bank in Argentina. Where did the crime occur? Who should be the primary investigative agency?

This example demonstrates that open economies, growing interdependence, and the instantaneous nature of financial transactions can all be exploited by criminals. It is clear that law enforcement will be required to adapt its organizational structures, investigative methodologies, and international relationships if these types of new transnational crimes are to be addressed,

because current reporting requirements, legislation, and international partnerships do not sufficiently address these changes.

[Back to Top](#)

The Internet

Computers and the Internet have revolutionized the way that we communicate, entertain, and learn; they have forever changed the way that we conduct business, and socialize:

- Last year there were 3.5 billion financial transactions completed on-line
- It is estimated that over 144 million Americans are plugged into cyberspace
- By 2005, it is predicted that there will be over one billion users worldwide
- The migration to E-Commerce is a forerunner of the arrival of a truly global economy

In the wrong hands, the computers, Internet connections, and wireless communication devices, which have saturated our society, can become weapons capable of wreaking havoc on our financial infrastructure.

[Back to Top](#)

High Tech Crime

Computers and the Internet are an integral part of an ever-increasing amount of the criminal activity investigated by the USSS:

- The proliferation of computer generated and computer assisted fraud is dramatic
- Hardware and software tools developed for the benefit of consumers, small businesses, and corporations are frequently utilized by criminals
- Criminals use the Internet to access public sources of information which can be used to facilitate the commission of financial crimes
- Because of the competitive nature of Internet based financial services, the focus is on speed, "24/7" access, and ease of use, all of which make the job of the cyber criminal a little easier
- The Internet provides the anonymity that criminals desire. In the past most fraud schemes required some "face to face" exchange of information and allowed at least some of the information being provided to be verified relatively easily
- The Internet contains thousands of sites dedicated to all types of

criminal activity

- Hacking sites describe the methods for making intrusions into financial, telecommunications, and government systems, and allow the necessary "tools" to be downloaded; the demand for intrusion investigations is increasing

[Back to Top](#)

Electronic Benefits Transfer

- In June of 1997, the Food Stamp and Government Cash Assistance Program, via the United States Department of Agriculture (USDA), began issuing benefit recipient cards and personal identification numbers (PINs), to be used at retail locations such as supermarkets participating in the new Electronic Benefits Transfer (EBT) system.
- The EBT system handles transactions for the USDA, Food Stamp Benefits, Food and Consumer Services, Aid to Families with Dependant Children, and other government delivered cash assistance programs, by tracking allocations electronically.
- Under the EBT system, food stamp consumers apply for their benefits in the usual way, and once eligibility and the level of benefits have been determined, an account is established in the participant's name, and food stamp benefits are deposited electronically into the account each month.
- When paying for groceries, the food stamp customer's card is "swiped" through a point of sale terminal, and the client enters their designated PIN. The PIN and the account balance are verified electronically, the client's account is then debited for the amount of the purchase, and the retailer's account is credited. No money or actual food stamps change hands.
- Fraud associated with EBT programs is a violation of 18 USC 1029, access device fraud, a violation for which the Secret Service has primary investigative jurisdiction. Some cases may also involve money laundering and/or computer fraud violations, which the Secret Service also has the authority to investigate.
- As with any recurring payment system, EBT is open to a wide variety of fraud to include multiple false applications for benefits, counterfeiting of the EBT card and trafficking of non-cash benefits for cash or contraband.
- Organized criminal groups have increasingly manipulated the EBT system to reap high rewards. The EBT cards are used to conduct illegal transactions where cards are purchased by street level offenders for fifty cents on the dollar. These offenders then present the cards to cooperating merchants who in turn redeem the cards for their full credited value.

[Back to Top](#)

Identity Theft

Identity theft is the use of another person's identity to commit fraudulent activity. It is not typically a "stand alone" crime; it is almost always a component of one or more crimes, such as bank fraud, credit card or access device fraud, or the utterance of counterfeit financial instruments. In many instances, an identity theft case encompasses several different types of fraud. According to the statistics compiled through the Federal Trade Commission's Identity Theft Hotline:

- 54% of complaints involved credit card fraud - i.e. someone either opened up a credit card account in the victim's name or "took over" their existing credit card account
- 26% of complaints involved the activation of telephone, cellular, or other utility service in the victim's name
- 16% of complaints involved bank accounts that had been opened in their name, and/or fraudulent checks had been negotiated in the victim's name
- 11% of complaints involved consumer loans or mortgages that were obtained in the victim's name.

Unfortunately, consumers have little control over who has access to their personal identifiers. Social Security Numbers, in conjunction with other personal identifiers, are used for the granting of credit (auto loans, home mortgages, small business loans, apartment leases, activating service for utilities, etc), and when obtaining banking and investing services. They are requested by government agencies on applications for licenses, permits, and benefits, and are required by most health care providers for the maintenance of medical records.

- It is not realistic to expect that through the passage of new legislation or by modifying or adding regulations, the government can prevent consumers' personal identifiers from being used for a wide variety of record keeping and credit related applications. What can be done, however, is to establish information security standards and procedures to try to minimize the number of inadvertent disclosures that occur, as well as to reduce vulnerabilities to computer intrusions.
- Currently, it is a relatively simple matter for criminals to obtain personal information on a variety of individuals through public sources, particularly the Internet. Many government and private sector web sites have promotion lists, financial disclosure forms, and biographies of executives posted on them.
- Cyber criminals have also hacked into Internet merchant sites and made copies of the customer lists, which contain personal information and credit card account numbers. These account numbers are then used in conjunction with other personal identifiers to order

merchandise, which they have sent, throughout the world. Most account holders are not aware that their credit card account has been compromised until they receive their billing statement.

- In many cases, the hacking attempts are successful not due to the expertise of the cyber criminals, whose attempts are often quite technologically crude, but because of the failure of some business and government entities to take basic computer security precautions. It is not reasonable for consumers to expect that they will not have to provide personal identifiers when obtaining credit or services, but it is reasonable for them to expect that basic security measures will be taken to prevent these identifiers from being compromised and/or misused.
- It is the responsibility of government regulators, law enforcement agencies, financial institutions, and other private sector entities to work together to reduce the risk of such information falling into the wrong hands, and to identify, investigate, and prosecute those individuals responsible for the use of such information in identity theft schemes.

Some positive steps have already been taken. The Identity Theft and Assumption Deterrence Act, which was signed into law in October of 1998, provides increased protection for the victims of identity theft through enhancements to Title 18 United States Code, Section 1028:

- People whose credit has been compromised are now identified as true victims--historically with financial crimes such as bank fraud or credit card fraud, the victim identified by statute was the person, business or financial institution that lost the money.
- The Federal Trade Commission (FTC) was established as the one central point of contact for these victims to report all instances of identity theft. This collection of all ID theft cases allows for the identification of systemic weaknesses and the ability of law enforcement to retrieve investigative data at one central location. It further allows the FTC to provide people with the information and assistance they need in order to take the steps necessary to correct their credit records.
- Sentencing potential and asset forfeiture provisions were enhanced to help to reach prosecutorial thresholds and allow for the repatriation of funds to victims.
- A loophole was eliminated by making it illegal to steal another person's personal identification information with the intent to commit a violation. Previously, only the production or possession of false identity documents was prohibited. With advances in technology such as E-commerce and the Internet, criminals today do not need actual documents to assume an identity.

The Secret Service continues to attack identity theft by aggressively pursuing our core violations. It is by the successful investigation of criminals involved in financial and computer fraud that we are able to identify and suppress identity theft.

- The Secret Service emphasizes the investigation of counterfeit instruments--counterfeit currency, counterfeit checks, counterfeit credit cards, counterfeit stocks or bonds, etc--many of these schemes would not be possible without the compromise of innocent victims' financial identities.
- The Secret Service targets organized criminal groups, which are engaged in financial crimes on both a national and international scale. Many of these groups are prolific in their use of stolen financial and personal information to further their financial crime activity.
- The Secret Service works in concert with the state, county, and local police departments to ensure our resources are being targeted to those criminal areas that are of a high concern to local communities, and we work very closely with both federal and local prosecutors to ensure our investigations are relevant, topical, and prosecutable under existing guidelines.

This partnership approach to law enforcement is exemplified by our financial crimes task forces located throughout the country. Each of these task forces pools the personnel and technical resources needed to maximize the expertise of each participating law enforcement agency.

[Back to Top](#)

Foreign Office Expansion Initiative

- The U.S. Secret Service currently has seventeen (17) offices in foreign countries and a permanent assignment at Interpol, as well as overseas initiatives in the United Kingdom and Germany.
- Recently, new offices have been opened in Moscow, Pretoria, Lagos, and Frankfurt. The request to open a new office in New Dehli is pending approval, and Mexico City should be opened within the next six months.
- This expansion will increase our ability to become involved in foreign investigations that are of significant strategic interest.

[Back to Top](#)

The Electronic Crimes Special Agent Program

- ECSAP agents are highly trained and are qualified as experts in the preservation and analysis of electronic evidence to include computers, telecommunications devices, electronic organizers, scanners, and other electronic paraphernalia.
- They can also provide expertise in the investigation of network intrusions and database thefts.
- The current program has 140 trained SAs, of whom 114 are in the field and are available to conduct examinations. Another forty (40) SAs will receive ECSAP

training in FY 01.

[Previous](#) | [Table of Contents](#) | [Next](#)

CASE MANAGEMENT (INV-35)

An investigation dealing with the manufacture of fictitious financial instruments, false identification, or the counterfeiting of currency or corporate bank checks, usually reveals they were most likely produced using a computer and desktop publishing software. Experience indicates the majority of Secret Service investigations involve the computer, whether as the target of the crime, a tool used to commit the crime, or as a repository of evidence.

In recognition of these developments, the Office of Investigations has initiated a "one program" philosophy. Headquarters operational divisions can no longer afford to be viewed as individual entities, but must become fully integrated into one mutually supportive unit who's primary mission is to support the field. The Secret Service is confronting a technological transformation in criminal methodology and must adapt our methods of investigation to meet this new challenge. The Office of Investigations has introduced the "one program" philosophy to meet the challenges presented by emerging technologies. The first line of defense in this effort is the Electronic Crimes Special Agent Program (ECSAP).

In the furtherance of the International Crime Control Act and a number of Presidential Directives, the Service has developed an ambitious overseas initiative to address the growing threat of transnational crime. International criminal groups operating both within and outside the borders of the United States have targeted American citizens and our financial infrastructure. The "one program" philosophy will be the cornerstone on which we build our investigative agenda for the future. Discretionary and non-discretionary criteria will no longer be used in the prioritization of cases.

Investigative priority should be based upon a variety of factors to include, but not limited to: potential seizures, economic impact, criminal activity in a particular district, and organized group activity. Protective intelligence remains in a position of top priority. SAICs must allocate resources to the most significant investigations and manage all other cases as resources allow. In order to accomplish this, priority should be given to core violation investigations involving the following:

1. Transnational or multi-district investigations.
2. Schemes involving multiple defendants participating in organized groups.
3. Newly evolving schemes utilizing computers and/or exploiting emerging technologies.
4. High actual dollar loss with the potential for seizure and asset forfeiture.
5. Impact on the local community.

The use of these criteria in case selection and initiation will serve to enhance the investigative effectiveness of each office while allowing for the maximum utilization of available resources.

[Previous](#) | [Table of Contents](#) | [Next](#)

OFFICE OF INVESTIGATIONS

INVESTIGATIVE PRIORITIES

January 1 – December 31, 2004

As the Secret Service moves from the Department of the Treasury to the Department of Homeland Security, change is inevitable. However, the Office of Investigations remains committed to quality investigative cases involving our core violations. The Department of Homeland Security recognizes the importance of our investigative mission to homeland security, specifically with regard to maintaining economic security. In the department's strategic plan, the Protection goal clearly addresses this importance. It reads, "Safeguard our people and their freedoms, critical infrastructure, property, and the economy of our Nation from acts of terrorism, natural disasters, or other emergencies." Your daily investigative activities will support the Department in achieving this goal.

Though investigations have changed and become more complex over the last twenty years, our core mission has remained the same: protection of the country's payment and financial systems. The Secret Service has a rich history in this arena and we must maintain that leadership role. Increasingly, industry leaders look to the Secret Service for guidance on safeguards that can be put into place to prevent fraud and to assess systemic weaknesses.

Proper case prioritization will enable field offices to focus our resources on investigations that have significant economic and community impact. As we move into the 21st Century, so must our investigations. Our investigations must continuously shift to keep pace with new technology and the criminal element that will always try to exploit the weaknesses in those new technologies.

Having stated the above, the Office of Investigations realizes that this year will be extremely busy for the field with the inordinate amount of protection that a campaign year brings. This makes it even more important that supervisors prioritize investigations that will have the biggest community impact. Offices need to come up with creative case management plans to ensure we do not lose the investigative momentum gained over the last several years. Stay engaged investigatively. If you develop significant cases during a period of time when your manpower is stretched to its limits, the Office of Investigations is committed to getting you the assistance you need.

Finally, Protection and Protective Intelligence investigations will always remain our number one priority because of their time sensitive nature and the importance of the key leaders we protect. However, looking back over our storied history, our original mandate was to protect this nation's financial infrastructure: our currency. Even though our financial infrastructure has evolved and changed over the years, our mandate has not.

Brian K. Nagel
AD – Investigations