QUESTIONNAIRE ON FRAUD AND THE CRIMINAL MISUSE AND FALSIFICATION OF IDENTITY (IDENTITY FRAUD)

RESPONSE OF THE UNITED STATES DELEGATION TO THE INTERGOVERNMENTAL EXPERT GROUP

MAY 2006

PART I: FRAUD

1. Please provide short descriptions or information, where available, on the following:

(a) Your country's commercial law framework, including contract laws, consumer protection laws and tort laws. Please provide the specific law or regulation.

The United States has a federal system of government. This means that many of the laws governing commercial transactions – including contract, consumer protection, and tort laws – are enacted and enforced at the state level. Some commercial-transactions laws with nationwide significance – such as statutes governing securities and commodities transactions and certain business activities affecting interstate or foreign commerce – are enacted at the federal level. An exhaustive listing of these statutes would be prohibitively long. Some examples of these statutes are the 1933 and 1934 securities laws, the Commodity Exchange Act, and the Federal Trade Commission (FTC) Act. The latter Act, among other things, prohibits unfair or deceptive acts or practices in or affecting commerce. States typically have closely analogous consumer-fraud statutes that contain similar prohibitions within their borders.

(b) What percentage of your country's commercial customs and infrastructure, including means of conducting large (commercial) and small individual (consumer) transactions, are conducted with debit cards? What percentage are conducted with credit cards? What percentage are conducted electronically? What percentage are conducted by barter? What percentage are conducted with other means?

According to the Statistical Abstract of the United States,[1] the Nilson Report contains the following data on consumer-payment systems for 2000, 2003, and 2008 (projected):

Method of Payment	***Transactions - Number (Billions)***	***Transactions - Percent Distribution***	***Volume - Amount (Billions of Dollars)***	***Volume - Percent Distribution***
Total	2000: 112.3 2003: 123.7 2008: 146.9	2000: 100.0 2008: 100.0	2000: 5,291 2003: 6,030 2008: 7,357	2000: 100.0 2008: 100.0
Paper	2000: 80.4 2003: 79.0 2008: 73.1	2000: 71.6 2008: 49.8	2000: 3,482 2003: 3,475 2008: 2,718	2000: 65.8 2008: 36.9
- *Direct check payments*	2000: 28.8 2003: 26.8 2008: 23.5	2000: 25.6 2008: 16.0	2000: 2,271 2003: 2,093 2008: 1,459	2000: 42.9 2008: 19.8
- *Cash*	2000: 50.3 2003: 51.1 2008: 48.7	2000: 44.8 2008: 33.1	2000: 1,092 2003: 1,263 2008: 1,152	2000: 20.6 2008: 15.7
- *Money orders*	2000: 0.9 2003: 0.8 2008: 0.7	2000: 0.8 2008: 0.5	2000: 82 2003: 82 2008: 74	2000: 1.5 2008: 1.0
- *Travelers checks*	2000: 0.2 2003: 0.2 2008: 0.1	2000: 0.2 2008: 0.05	2000: 13 2003: 11 2008: 6	2000: 0.2 2008: 0.1
- *Food stamps*	2000: 0.2 2003: 0.1 2008: --	2000: 0.1 2008: --	2000: 4 2003: 2 2008: --	2000: 0.1 2008: --
- *Official checks*	2000: 0.1 2003: 0.1 2008: 0.2	2000: 0.1 2008: 0.1	2000: 22 2003: 24 2008: 27	2000: 0.4 2008: 0.4
Cards	2000: 28.8 2003: 40.7 2008: 64.5	2000: 26.6 2008: 43.9	2000: 1,589 2003: 2,110 2008: 3,594	2000: 30.4 2008: 48.9
- *Credit cards*	2000: 19.9 2003: 21.4 2008: 27.3	2000: 17.7 2008: 18.6	2000: 1,238 2003: 1,438 2008: 2,178	2000: 23.4 2008: 29.6
- *Debit cards*	2000: 8.2 2003: 16.1 2008: 30.5	2000: 7.3 2008: 20.8	2000: 309 2003: 583 2008: 1,213	2000: 5.8 2008: 16.5
- *Prepaid cards*	2000: 1.3 2003: 2.5 2008: 5.6	2000: 1.1 2008: 3.8	2000: 31 2003: 69 2008: 171	2000: 0.6 2008: 2.3

Method of Payment	*Transactions - Number (Billions)*	*Transactions - Percent Distribution*	*Volume - Amount (Billions of Dollars)*	*Volume - Percent Distribution*
- *Electronic benefits transfer cards*	2000: 0.5 2003: 0.8 2008: 1.2	2000: 0.4 2008: 0.8	2000: 11 2003: 20 2008: 32	2000: 0.2 2008: 0.4
Electronic	2000: 2.1 2003: 4.0 2008: 9.3	2000: 1.8 2008: 6.3	2000: 219 2003: 445 2008: 1,045	2000: 4.1 2008: 14.2
- *Preauthor-ized payments*	2000: 1.5 2003: 2.4 2008: 4.7	2000: 1.4 2008: 3.2	2000: 166 2003: 276 2008: 567	2000: 3.1 2008: 7.7
- *Remote payments*	2000: 0.5 2003: 1.5 2008: 4.5	2000: 0.5 2008: 3.1	2000: 53 2003: 169 2008: 478	2000: 1.0 2008: 6.5

Note: -- represents zero. "Official checks" include cashier's, teller's, and certified checks.

The Nilson Report also contains the following data on debit-card holders and use for 2003 and 2008 (projected):

Type of Debit Card	*Cardholders (Millions)*	*Number of Cards (Millions)*	*Number of Transactions (Millions)*	*Volume (Billions of Dollars)*
Total	2003: 170 2008: 188	2003: 268 2008: 293	2003: 18,442 2008: 33,936	2003: 820 2008: 1,630
- Bank	2003: 166 2008:146	2003: 199 2008: 234	2003: 12,010 2008: 20,619	2003: 577 2008: 1,044
- EFT	2003: 169 2008: 178	2003: 256 2008: 283	2003: 6,414 2008: 13,298	2003: 242 2008: 586
- Other	2003: 11 2008: 10	2003: 11 2008: 10	2003: 19 2008: 19	2003: 1 2008: 1

Note: Cardholders may hold more than one type of card. EFT - electronic funds transfer.

The Nilson Report also contains the following data on credit-card holders and use for 2003 and 2008 (projected):

Type of Credit Card	*Cardholders (Millions)*	*Number of Cards (Millions)*	*Credit Card Spending (Billions of Dollars)*	*Credit-Card Debt Outstanding (Billions of Dollars)*
Total	2003: 164 2008: 176	2003: 1,460 2008: 1,513	2003: 1,735 2008: 2,604	2003: 786 2008: 965
- Bank	2003: 117 2008: 129	2003: 556 2008: 653	2003: 1,164 2008: 1,744	2003: 581 2008: 711
- Phone	2003: 122 2008: 112	2003: 175 2008: 151	2003: 19 2008: 16	2003: 2 2008: 2
- Store	2003: 115 2008: 114	2003: 542 2008: 510	2003: 133 2008: 146	2003: 89 2008: 98
- Oil company	2003: 73 2008: 69	2003: 86 2008: 80	2003: 48 2008: 64	2003: 6 2008: 7
- Other	2003: 7 2008: 6	2003: 101 2008: 119	2003: 371 2008: 634	2003: 108 2008: 148

Note: Cardholders may hold more than one type of card. "Other" includes auto rental and miscellaneous cards; and (except for data on cardholders) includes Discover, American Express, and Diners Club.

With respect to barter, the International Reciprocal Trade Association (IRTA) estimated that about half a million business firms would use the services of commercial barter companies in 2005.[2] The IRTA also estimated that $1 billion is bartered each year through barter exchanges, and that commercial barter accounts for an additional $6 billion or more per year.[3]

(c) The extent to which information and communication technologies (including wireline telephones, wireless or cellular telephones, fax machines, electronic mail and the Internet) are available in urban and rural areas, and the extent to which they are used for commercial activities.

All of these technologies are widely available in both urban and rural areas throughout the United States, and all are heavily used in commercial activities. For example, the Statistical Abstract of the United States reported that in 2003, 95.5 percent of U.S. households had telephone service, 61.8 percent had computers, 54.6 percent had Internet connections, and 19.9 percent had broadband Internet.[4]

2. Is fraud dealt with in your country's legal system:

(a) Only as a criminal matter?

( ) Yes (x) No

(b) Also in civil, administrative or other laws?

(x) Yes ( ) No

3. How is fraud defined in your country's legal framework? Please provide relevant definitions, the specific law or regulation, and a description of the constituent elements of the offences in use in your national criminal laws (see also questions 7 and 8).

Federal criminal law in the United States does not contain a definition of the term "fraud," although that term is frequently used in various federal criminal offenses directed at fraud. The typical approach in federal law is to refer to a "scheme or artifice" to defraud, with reference to a particular type of payment mechanism (e.g., credit cards) or organization (e.g., federally regulated financial institutions, insurance companies) involved in the fraud. State fraud statutes may not refer to a "scheme or artifice" to defraud, but may address either general or specific types of fraud.

The most frequently used federal offenses against fraud are:

- Mail fraud (18 U.S.C. § 1341). This offense, in essence, criminalizes any use of the United States mail in furtherance of a scheme or artifice to defraud.
- Wire fraud (18 U.S.C. § 1343). This offense, in essence, criminalizes any wire, radio, or television communication in interstate or foreign commerce in furtherance of a scheme or artifice to defraud.
- Financial institution fraud (18 U.S.C. § 1344). This offense criminalizes any execution, or attempt to execute, a scheme or artifice to defraud a federally insured financial institution, or to obtain any money under the control or custody of a federally insured financial institution by using false or fraudulent pretenses, representations, or promises.
- Access device fraud (18 U.S.C. § 1029). This statute contains a number of separate offenses criminalizing different aspects of fraud that involves "access devices" (i.e., cards, plates, numbers, or other data that, by themselves in with other access devices, allow access to bank or financial accounts). For example, subsection 1029(a)(1) criminalizes knowingly and with fraudulent intent producing, using, or trafficking in one or more counterfeit access devices; subsection 1029(a)(2) criminalizes knowingly and with fraudulent intent trafficking in or using one or more unauthorized access devices during any one-year period, and by such conduct obtaining anything of value aggregating $1,000 or more during that period; and subsection 1029(a)(3) criminalizes knowingly and with fraudulent intent possessing 15 or more counterfeit or unauthorized access devices.

Passport fraud is often committed in the United States and at U.S. posts abroad, for the purpose of adopting another identity to facilitate further criminal activity ranging from financial crimes to terrorism. While it might be argued that the identity theft is incidental to the individual not wanting to be who s/he really is (be that a citizen or alien) as that identity is already associated with criminal activity, the effect is the same: victimizing of a person whose identity is stolen. It is also falsely claiming a benefit to which the person may not be entitled.

Visa fraud, on the other hand, is committed by aliens attempting to enter the United States. They may do so in their genuine identity; attempting to qualify when they know they are ineligible; or with a document in a stolen false identity from the country of origin, or from another country that is seen as less threatening. The object is sometimes relatively benign; simply the ability to enter the United States to benefit from its freedoms. But there is also a wide range of serious criminal behavior that has been associated with it; not least of which is widespread benefits and entitlements fraud that becomes a serious drain on the public treasury.

The principal offenses relating to passport and visa fraud include:

- False statement in application and use of passport (18 U.S.C. § 1542). This offense criminalizes any false application for a passport either for the perpetrator's own use or the use of another; and it criminalizes the use or provision to another of a falsely obtained passport.
- Forgery or false use of passport (18 U.S.C. § 1543). This offense states that it is a crime to falsely make, forge, counterfeit, mutilate or alter any passport or instrument purporting to be a passport with the intent to use it; or to use, attempt to use or to furnishes to another any passport or any such document.
- Misuse of passport (18 U.S.C. §1544). This offense states that it is a crime to use or attempt to use any passport issued or designed for the use of another; or use or attempt to use any passport in violation of the conditions or restrictions or rules prescribed pursuant to the laws regulating issuance of passports; or furnishes, disposes of or delivers a passport to any person for use by another than the person for whose use it was originally intended.
- Fraud and misuse of visas, permits and other documents (18 U.S.C. § 1546). This statute contains a number of separate offenses criminalizing different aspects of fraud that involves immigrant and non-immigrant visas, permits, border crossing cards, alien registration cards, or other documents prescribed by statute or regulation for entry into or as evidence of authorized stay or employment. Subsection 1546(a) prohibits the forgery, counterfeiting, alteration or making of the above documents or the uttering, use, attempt to use, possession, acceptance or receipt; or who falsely applies for such a document. Subsection 1546(b) makes it an offense to use an identification document knowing that the document was not issued lawfully, knowing that the document is false, or making a false attestation for the purpose of satisfying a requirement of Section 274A(b) of the Immigration and Nationality Act.

4. Please indicate the types of fraud most commonly encountered in your country and their typical characteristics.

There is no single government agency or private-sector entity that compiles statistical data on the principal types of fraud that occur within or affect the United States. Some of the more frequently reported types of fraud include:

- Accounting fraud, in which officers of publicly traded companies seek to manipulate accounting data and corporate reports to make the financial soundness of their companies appear better than it is;

- Advance-fee fraud, which can encompass any type of fraud scheme in which victims are induced to pay money to criminals for nonexistent "taxes," "fees," or "customs duties" before the criminals are expected to provide whatever goods or services (e.g., offshore tax shelters) they have promised to victims;
- Credit-card and debit-card fraud, which can be found in many types of traditional and online consumer transactions;
- Financial institution fraud, which can include check-kiting schemes, fraudulent loan applications, negotiation of counterfeit checks, and fraudulent withdrawal of customers' funds by check or Automated Teller Machine (ATM) transactions;
- Identity document fraud, passport fraud and visa fraud, which is often a precursor to other criminal activities;
- Insurance fraud;
- Internet fraud, which can include other types of fraud listed above and below where the Internet is used;
- Securities and other investment fraud, which can involve both market-manipulation schemes, fraudulent offers of stock in nonexistent or bankrupt companies, fraudulent foreign-currency transactions, "prime bank"schemes, offshore trusts and investments, and insider trading; and
- Telemarketing fraud, which can encompass the use of the telephone to further any of the types of fraud schemes listed above.

5. Which of the following criteria are in principle used in the legal system of your country for purposes of classification of types of fraud:

(a) Type of commercial structure attacked or exploited by offenders; [1]

(x) Yes ( ) No

and / or

(b) Characteristics of methods used by the offenders; [2]

(x) Yes ( ) No

and / or

(c) Identification by the type of victim; [3]

(x) Yes ( ) No

and / or

[1] Criterium used for the description of certain types of fraud, such as credit-card, bank and financial instrument frauds.

[2] Criterium used for the description of certain types of fraud, such as pyramid scheme and advance-fee frauds.

[3] Ranging from private individuals to private commercial interests and States funds.

(d) Identification by the type of offenders; [4]

( ) Yes (x) No

and/or

(e) Specific infrastructures used for the commission of frauds; [5]

(x) Yes ( ) No

and / or

(f) Other?

(x) Yes ( ) No

Please provide examples and the specific law or regulation for each example.

(a) Some federal fraud offenses involve commercial (and governmental) structures attacked or exploited. These include mail fraud (18 U.S.C. § 1341), which protects the U.S. mail system; computer fraud (18 U.S.C. § 1030(a)(4)), which protects "protected computers" (i.e., computers for the exclusive use of a financial institution or the U.S. Government and computers used in interstate or foreign commerce); major fraud against the United States (18 U.S.C. § 1031); fraud in connection with email (18 U.S.C. § 1037); financial institution fraud (18 U.S.C. § 1344), which protects federally insured and chartered financial institutions; 18 U.S.C. § 510, which addresses forged endorsements on U.S. Treasury checks and bonds or securities of the United States; and 18 U.S.C. § 514, which prohibits the making or passing of fictitious financial instruments appearing to be instruments issued under the authority of the United States, a foreign government, a state or other political subdivision of the United States, or an organization.

(b) Only a few specialized federal fraud statutes can be said to address the methods that offenders use. These include the access device fraud offenses (18 U.S.C. § 1029), such as those described above in the response to question 3.

(c) Only one federal fraud statute, the telemarketing fraud sentencing enhancement (18 U.S.C. § 2326), addresses a particular category. This section provides for additional periods of imprisonment in instances where certain frauds victimized 10 or more persons over age 55, or targeted persons over age 55.

(d) Federal fraud offenses do not address specific types of offenders. Some other federal offenses that may be used in conjunction with federal fraud offenses, however, do refer to specific types of offenders. These include the bank bribery offense (18 U.S.C. § 215), which, among other things, prohibits financial institution "insiders" (i.e., officers, directors, employees, agents, and attorneys of a financial institution) corruptly soliciting or demanding for the benefit of any person aything of

---

[4] For example, some typologies of fraud distinguish the perpetrators between insiders and outsiders

[5] Including, for example, stamp, money-circulation and immigration frauds.

value, where they intend to be influenced or rewarded in connection with any business or transaction of the financial institution; and the RICO statute (18 U.S.C. § 1961 et seq.), which, among other things, prohibits any person, through a pattern of racketeering activity, from acquiring or maintaining any interest in or control of any enterprise that is engaged in or the activities of which affect interstate or foreign commerce.

(e) Some fraud offenses can be said to involve specific infrastructures. These include wire fraud (18 U.S.C. § 1343), which refers to the use of wire, radio, and television communications in interstate or foreign commerce, and the "CAN-SPAM" Act (18 U.S.C. § 1037), which addresses fraud involving email.

(f) Several statutes provide for penalties for crimes involving identity theft have a sliding scale of punishments that tie to the purpose of the crime to the crime, with narcotics smuggling being penalized at an enhanced level, and terrorism being penalized at the maximum level (18 U.S.C. §§ 1542, 1543, 1544). State fraud offenses involving securities law violations are generally based on provisions in the Uniform Securities Act and state criminal statutes, and track federal fraud offenses including actions for theft, deception, misrepresentation, and conspiracy.

6. Has your country encountered one or more of the following types of fraud:

(a) Frauds in which the scheme entailed the payment of funds in advance for goods or services that were not fully delivered if at all (for example, goods promised through on-line auctions or protection for credit and debit losses);
(x) Frequently ( ) Occasionally ( ) Rarely ( ) Never

(b) Frauds in which victims were charged fraudulently excessive prices compared to the value of goods or services actually delivered;
(x) Frequently ( ) Occasionally ( ) Rarely ( ) Never

(c) Frauds in which victims were induced to deliver goods or services that were never paid for;
(x) Frequently ( ) Occasionally ( ) Rarely ( ) Never

(d) Frauds in which victims were induced to pay for influence or opportunities (including corruption) that were never fully delivered if at all;
( ) Frequently ( ) Occasionally (x) Rarely ( ) Never

(e) Frauds involving purported charities or charitable donations;
(x) Frequently ( ) Occasionally ( ) Rarely ( ) Never

(f) Frauds involving commercial financial structures, such as financial instruments, stocks and similar structures, including asset protection schemes, off-shore investment schemes and other investments, as well as insolvency, bankruptcy and similar structures, where these exist;
(x) Frequently ( ) Occasionally ( ) Rarely ( ) Never

(g) Frauds involving private commercial structures, including credit and debit card systems, cheques, zahlscheine and similar structures, where these exist;
(x) Frequently ( ) Occasionally ( ) Rarely ( ) Never

(h) Frauds involving loans;
(x) Frequently ( ) Occasionally ( ) Rarely( ) Never

(i) Frauds involving lottery or prize winnings;
(x) Frequently ( ) Occasionally ( ) Rarely( ) Never

(j) Frauds against public or private procurement systems;
(x) Frequently ( ) Occasionally ( ) Rarely( ) Never

(k) Frauds involving insurance;
(x) Frequently ( ) Occasionally ( ) Rarely( ) Never

(l) Transport frauds, including maritime frauds;
( ) Frequently ( ) Occasionally (x) Rarely( ) Never

(m) Other types of fraud?

(X) Frequently ( ) Occasionally ( ) Rarely( ) Never

Please specify or provide examples[6]:

(a) Advance-fee fraud schemes are one of the oldest general types of fraud schemes in the United States. With the growth of the Internet, fraud schemes that involve exploitation of online auctions or fraudulent online retail sales have become quite common. In 2005, for example, the U.S. Federal Trade Commission (FTC) found that consumer complaints involving online auctions were the largest single category of consumer complaints (other than identity theft) filed with the FTC – approximately 12 percent of 686,683 complaints.[5] Similarly, the Internet Crime Complaint Center (IC3) -- a joint venture of the Federal Bureau of Investigation and a private-sector nonprofit organization, the National White Collar Crime Center – found that in 2005, Internet auction fraud was "by far the most reported offense," comprising 62.7 percent of the 97,076 complaints that it referred to law enforcement.[6] Some of the many varieties of advance-fee schemes that U.S. law enforcement and regulatory agencies encounter include bogus offers of loans or credit cards; prize or lottery winnings; fraudulent solicitations for help in transferring funds from various African countries; offshore nonexistent "prime bank" investment schemes; foreign currency scams; and offshore tax shelters and international affinity fraud based on religious, cultural, or ethnic representations.

(b) Telemarketing-fraud schemes often involve inducing people to pay for goods or services vastly lower in price and quality than the victims are led to believe. Over the past years, for example, telemarketing-fraud schemes have included fraudulent offers of prizes and lottery or sweepstakes winnings; magazine subscriptions; and charitable donations.

(c) Certain Internet fraud schemes, such as those involving online auctions or online retail sales, as well as credit-card fraud schemes often involve inducing people

[6] Replies and information to be provided may also include comments on the extent to which the basic typology contained in question 6 is valid for each country national law and practice, as well as suggestions on any additions or refinements deemed appropriate.

to provide goods or services that were never paid for. These often involve high-value merchandise, such as expensive electronics equipment, cameras, and watches.

(e) At any point in time, there are always some fraud schemes involving solicitations for ostensibly charitable purposes. These typically include solicitations that purport to be for the benefit of police officers or firefighters. When natural disasters strike, the incidence of such schemes can rise dramatically. After the terrorist attacks of September 11, 2001, and Hurricanes Katrina and Rita in 2005, for example, law enforcement authorities saw a significant number of schemes that purported to be collecting money for survivors of the disasters.

(I) A number of transnational telemarketing-fraud schemes engage in fraudulent offers or "guarantees" of substantial prizes or lottery winnings. These schemes have received substantial attention in recent years from both Canadian and U.S. law enforcement agencies.

(j) Procurement fraud schemes occur with some frequency in defense-procurement contracts and in contracts for procurement of services after large-scale natural disasters, when contracts are let for debris removal and infrastructure rebuilding. The U.S. Department of Justice's Hurricane Katrina Fraud Task Force, for example, is actively investigating procurement contracts stemming from the damage caused by Hurricanes Katrina, Rita, and Wilma along the Gulf Coast of the United States in 2005.[7]

(k) Insurance fraud covers a wide range of criminal conduct relating to fraudulent claims for property damage or loss or for physical injury. Some typical types of insurance fraud include disability or workers' compensation fraud, theft or conversion of customer funds, false claims for renovations due to hurricane damage, sales of false motor vehicle insurance cards, and staged-auto-accident rings.[8]

(m) Passport and visa fraud is often a precursor to other criminal activity. This includes identity fraud/theft and/or claiming a benefit to which one is not entitled, such as an alien who commits passport fraud is making a false claim to U.S. citizenship (18 U.S.C. § 911).

7. Are types of fraudulent conduct covered in your country's legislation by offences other than criminal or non-criminal offences directed specifically at fraud? (see also question 2b)

(x) Yes ( ) No

8. If the answer to question 7 is yes please specify such offences and how they are seen to be related to fraud. Please also provide the specific law or regulation for such offences.

At the federal level, the Federal Trade Commission Act (see 15 U.S.C. § 45(a)(1)) declares unfair methods of competition, and unfair and deceptive acts and practices in or affecting commerce, to be unlawful. The FTC can use this authority to initiate civil actions to enforce the Act. Similarly, in the area of investments, the Securities and Exchange Commission and the Commodity Futures Trading Commission can bring civil actions under their respective statutory authorities to regulate securities and commodities markets. At the state level, state Attorney

Generals and state regulators (banking, insurance, securities) and District Attorneys using analogous consumer-protection and securities laws, can also file civil and criminal actions to protect consumers from fraudulent and deceptive practices, including investment schemes.

9. Please indicate and describe the types of fraud that represent a particular concern for the authorities of your country in view of:

(a) Possible links to domestic or transnational organized crime, including the involvement of organized criminal groups[7] in any element of the offences, including laundering of the proceeds;

(b) Possible links to terrorism, including the commission of frauds by individuals or groups suspected of involvement in terrorism and the use or suspected use of proceeds of fraud to fund activities related to terrorism;

(c) Elements of transnationality, including:

(I) Offenders in one country targeting victims in another country;

(ii) Offenders in more than one country;

(iii) Victims in more than one country;

(iv) Use of third countries for other purposes, including concealment of offenders, deception of victims, or laundering or concealment of proceeds;

(v) Large number of offenders or victims;

(vi) Large amounts of proceeds of crime.

(a) One type of crime that is associated with a variety of current fraud schemes is the creation and use of counterfeit business and personal checks and postal money orders. The large-scale manufacture and dissemination of these counterfeit checks and postal money orders is typically associated with West African criminal groups, whether operating in the United States or abroad. These counterfeit checks and postal money orders have been seen in telemarketing-fraud schemes, in which victims are led to believe that they are receiving checks constituting lottery or prize winnings; and Internet fraud sales schemes, in which victims who offer real merchandise for sale online (e.g., motor vehicles) accept the counterfeit checks as payment for the goods they are selling, or victims are induced by criminals to receive fraudulently ordered merchandise and reship it to other U.S. or foreign destinations, and then to accept the counterfeit checks or money orders as payment for their services. In all cases, the checks and money orders are made out for amounts larger

[7] Article 2, subparagraph (a) of the United Nations Convention against Transnational Organized Crime defines organized criminal group as follows: organized criminal group shall mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit (see A/RES/55/25 of 15 November 2000, annex I, art. 2(a)).

than the debt owed or commission to be paid to the victim, so that the victim is induced to deposit the check or money order in his or her bank account and to wire the balance of the funds to a foreign bank account before he or she is notified by the banks that the check or money order is counterfeit.

Another type of crime that has been increasingly associated with organized crime in recent years is telemarketing fraud. A joint U.S.-Canada working group reported in 2003 that traditional organized crime groups, as well as motorcycle gangs and other ethnically-based organized criminal groups, have sought greater influence over and profit from some transnationally operating telemarketing-fraud operations, because these schemes can be highly lucrative but far less risky than drug-trafficking or other violent criminal activities.[9]

Schemes involving large-scale credit-card and debit-card fraud have also involved organized criminal groups. In some cases, these groups operate across many states and even countries, arranging for the theft of credit or debit cards in one or more areas, shipping the cards to another area where identification matching the names on the cards can be counterfeited, and soliciting individuals to use the stolen cards and fraudulent identification to purchase valuable goods that are provided to the ringleaders of the schemes.

It should be noted that the United States has recently seen a number of fraud schemes that operate from the United States, but that target substantial number of residents of other countries. In 2004, for example, a federal indictment charged 10 individuals - including an alleged capo, a soldier and associates in the Gambino crime family - for their role in a telephone "cramming" scheme that allegedly generated approximately $500 million in gross revenues, and an Internet fraud scheme that generated more than $200 million more in fraudulent charges to consumers in three continents. The telephone scheme involved placing of unauthorized charges on the local telephone bills of millions of consumers. As a result of increasing consumer complaints, several defendants and others allegedly created a call center, in which the operators were directed initially to attempt to "sustain" the bogus charges by persuading customers that the charges on their phone bills were authorized.[10] Other U.S.-based schemes have offered fraudulent investments to large numbers of foreign and U.S. investors. In a recent federal case, a Connecticut man was charged with fraud- and money laundering-related offenses relating to his alleged operation of a company that operated a "Ponzi" scheme that defrauded more than 13,000 foreign investors and 10,000 U.S. investors and took in more than $6 million.[11]

(b) There have been some public reports of fraud schemes that involve a demonstrable connection to terrorist organizations. In 2004, the U.S. Court of Appeals affirmed the conviction of an individual connected with a cigarette-smuggling operation that generated proceeds in part to provide funding to the terrorist organization Hizballah.[12] The operation smuggled cigarettes from one state that levied very low taxes on cigarette sales ($0.50 per carton) to another state that levied much higher taxes ($7.50 per carton) and sold the cigarettes in the latter state without paying the cigarette-sales taxes there.[13]

In addition, in 2002 an FBI official testified in a Congressional committee about an Al-Qaeda cell in Spain that used stolen credit cards in fictitious sales schemes and for other purchases for the cell. The cell members reportedly "kept purchases below amounts where identification would be needed," and used stolen telephone and credit cards for communications back to Pakistan, Afghanistan, and Lebanon.[14]

(c) One of the most significant fraud trends in recent years has been the growing transnational dimensions of large-scale mass-marketing fraud schemes (i.e., schemes that exploit mass-communications techniques, such as telemarketing, the Internet, and mass-mailing, to reach large numbers of potential victims in multiple jurisdictions). It is not uncommon for criminal organizations based in various in Europe and Africa to conduct their contacts with victims in North America and other continents from those countries, and to use multiple channels, including electronic-funds-transfer systems, to receive funds from victims and to launder those funds in still other jurisdictions. In March 2006, for example, a federal grand jury in the Eastern District of New York indicted four individuals of Nigerian citizenship on federal charges of running an "advance-fee" scheme that targeted U.S. victims with promises of millions of dollars. All four individuals allegedly operated their scheme from Amsterdam. The scheme allegedly included sending millions of "spam" emails to thousands of potential victims in multiple locations.[15]

Another fraud scheme that reflects multiple aspects of transnationality involved several individuals of Canadian nationality who operated the Tri-West Investment Club, a transnational Internet-based investment scheme, from Mexico and Costa Rica. The scheme purported to offer "prime-bank"-related investments, but defrauded approximately 15,000 investors in 60 countries of $58 million between 1999 and September 2001.[16]

10. Does your country consider ordinary fraud to include non-economic offences, such as frauds involving travel or identity documents?

(x) Yes ( ) No

If the answer is yes please specify:

In federal criminal law, the identification-document statute (18 U.S.C. § 1028) includes a number of offenses associated with the production of false or fraudulent identification documents, and 18 U.S.C. § 1546 prohibits a number of actions associated with fraud and misuse of visas, permits, and other immigration-related documents. In addition, proof of the existence of a scheme to defraud may include proof that the defendants engaged in the misuse of other people's identifying information or identification documents as part of the scheme.

11. How are fraud and related offences punished in the legal system of your country? Are the penalty requirements compatible with the definition of serious crime in article 2, subparagraph (b) of the United Nations Convention against Transnational Organized

Crime (2000)[8]? Please specify the punishment or penalty and the specific law or regulation for each.

In federal criminal law, nearly every fraud-related offense meets the Convention's definition of "serious crime." For example, financial institution fraud (18 U.S.C. § 1344) has a maximum term of 30 years imprisonment; mail fraud (18 U.S.C. § 1341) and wire fraud (18 U.S.C. § 1343) each have a maximum term of 20 years imprisonment (30 years imprisonment if the offense affects a financial institution); access-device fraud offenses have maximum terms of 10, 15, and 20 years imprisonment, depending on the specific offense involved; and computer fraud (18 U.S.C. § 1030(a)(4)) has a maximum term of 5 years imprisonment for a first offense under section 1030. Many states' fraud offenses also meet the Convention's definition of "serious crime" with similar terms of imprisonment.

12. In your country's legislation, are the offences relating to fraud and similar conduct considered as predicate offences for the purposes of measures against money-laundering?

(x) Yes ( ) No

If the answer is yes please specify the offence and specific law or regulation.

Under the two main federal money-laundering offenses, 18 U.S.C. §§ 1956 and 1957, the "specified unlawful activities" that constitute predicate offenses include, among other fraud-related offenses, identification-document fraud (18 U.S.C. § 1028), access-device fraud (18 U.S.C. § 1029), computer fraud (18 U.S.C. § 1030(a)(4)), mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), and financial-institution fraud (18 U.S.C. § 1344).[17]

13. How is the liability of legal persons for participation in frauds or other related offences established in your country legal system?

In general, federal fraud offenses and judicial constructions of those offenses have permitted the charging of corporate entities as well as natural persons for fraud. The essential elements of these offenses are the same for corporate entities and natural persons.

14. Please provide information on your country's legal framework enabling confiscation of proceeds of fraud or other related offences, as well as of property, equipment or other instrumentalities used in or destined for use in such offences and proceeds of fraud transformed or converted into other property or intermingled with legitimately obtained property. Please also provide the specific law or regulation for such offences.

Under the criminal forfeiture section of the United States Code (18 U.S.C. § 982), federal courts, in imposing sentence on a person convicted of a federal offense, can impose criminal forfeiture in a variety of circumstances that involve fraud. These include:

---

[8] "Serious crime shall mean conduct constituting an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty" (see A/RES/55/25 of 15 November 2000, annex I, art. 2(b)).

- When the person is convicted of a violation of, or a conspiracy to violate, mail, wire, or financial institution fraud affecting a financial institution, or of the identification-document, access-device, or computer-fraud offenses, the court may order that the person forfeit any property constituting, or derived from, proceeds the person obtained directly or indirectly as the result of the violation (18 U.S.C. § 982(2));
- When the person is convicted of a violation of, or a conspiracy to violate, the major fraud offense (18 U.S.C. § 1031) or mail or wire fraud involving the sale of assets acquired or held by conservators of a financial institution, the court may order that the person forfeit any property, real or personal, which represents or is traceable to the gross receipts obtained, directly or indirectly, as a result of the violation (18 U.S.C. § 982(3));
- When the person is convicted of an offense under 18 U.S.C. § 1028, 1029, 1341, 1342, 1343, or 1344 (or a conspiracy to commit that offense) if the offense involved telemarketing, the court shall order that the defendant forfeit any real or personal property used or intended to be used to commit, facilitate, or promote the commission of the offense, or constituting, derived from, or traceable to the gross proceeds that the defendant obtained directly or indirectly as a result of the offense (18 U.S.C. § 982(a)(8)).

State courts have similar provisions for forfeiture, restitution, and rescission in many instances.

15. Does the legal system of your country provide for any remedies (e.g., civil compensation or restitution) available to victims of fraud or other related offences? Please specify.

Yes. The sentencing authority of federal courts in criminal cases includes the authority to order restitution for victims of the offense or offenses of conviction. In addition, in enforcing the Federal Trade Commission Act, the FTC can seek consumer redress to provide civil compensation to victims of the fraudulent or deceptive practices.

16. Please indicate whether problems resulting from under-reporting of fraud victimization exist in your country. If fraud is believed to be under-reported, what, in your opinion, are the reasons for this, and how could accurate data about occurrence rates be obtained?

It has been apparent for a number of years that there is substantial underreporting of fraud victimization in the United States. For example, in a 2005 survey of U.S. adults, the National White Collar Crime Center found that while 36 percent of individuals and 46.5 percent of households reported experiencing at least one form of fraud within the previous year, only 30.1 of those households who told the survey that they had been victimized also reported the victimization to law enforcement or another crime control agency.[18] There are several reasons for underreporting, but not all of these pertain to each type of fraud.

- In the Center's survey, 67 percent of the households that were victimized reported the victimization to at least one source (e.g., a credit-card company, the business or person involved, law enforcement, a consumer-protection agency, or an attorney). While the reports to entities other than law

enforcement may have helped to resolve the problem from the victim's standpoint, those reports may not make their way to a common repository for tracking and analyzing fraud complaints.

- In some types of fraud, such as telemarketing fraud or investment fraud, victims who lose large amounts of money may be so embarrassed by being duped and losing their money that they refrain from reporting the loss to anyone, even family members or friends.
- In some cases, consumers or investors may not know which government agency is willing to receive and use their fraud complaints.

Because fraud complaints filed with government agencies are likely to underreport the incidence and prevalence of the fraud, the most promising way of obtaining more accurate data for a large population may be random-digit dialing surveys. This method was used in the National White Collar Crime Center's 2005 white-collar crime survey, and in various identity-theft surveys by the FTC, the Better Business Bureau, and the U.S. Department of Justice's Bureau of Justice Statistics.[19] Techniques involving face-to-face contact, such as focus groups or individual interviews, have sometimes been helpful in developing anecdotal evidence about certain types of fraud, but these are impractical for obtaining random samples of data across the population.

17. What is the impact of commercial systems or technologies, such as banking and credit-card systems, on the commission of fraud or other related offences in your country (including transnational offences which involve your country)?

Banking and credit-card systems, as well as computer-based technologies such as the Internet, can be both targets and instrumentalities for fraud. For many types of fraud, criminals must make use of banking and credit-card systems to obtain cash or transfer funds to other accounts after receiving funds from their victims. Informal, unregulated systems of funds transfers may be more useful for other types of crime (e.g., terrorist funding), but criminals engaging in fraud need the security that banking and credit-card systems can provide to be sure that they can access and transfer their criminal proceeds whenever they wish.

18. In your opinion, how could public and private commercial entities collaborate most effectively in the prevention and control of such offences?

Several approaches in the United States to public-private collaborations in preventing and controlling fraud have proved highly fruitful:

- *Collaboration in Receiving and Analyzing Complaints*. In developing its principal consumer complaint database for fraud and deceptive practices, Consumer Sentinel, over a number of years, the Federal Trade Commission (FTC) has encouraged private-sector organizations, such as consumer groups, and other governmental organizations, such as state Attorneys General and other law enforcement and regulatory agencies, to send consumer complaints to Consumer Sentinel. In addition, since 2000, a nonprofit organization, the National White Collar Crime Center, has joined forces with the FBI to operate the Internet Crime Complaint Center. In both instances, private- and public-sector entities have seen substantial benefits in gathering complaints from

disparate sources into a central location where they can be reviewed and analyzed for trends and recurring patterns of behavior and, where appropriate, identified as a basis for regulatory or law-enforcement investigation.

- *Collaboration in Analyzing Other Evidence of Possible Fraud*. In some cases, such as Internet fraud, both private companies and law-enforcement agencies may come across evidence that would be relevant to a criminal investigation. Because the company may not be a victim of fraud, but may see the potential for significant fraud developing (e.g., where the company has gathered evidence indicating that a particular website or set of emails may be fraudulent), it may be more appropriate for the company to pass this information expeditiously to law enforcement, and where appropriate, to work with law enforcement agents in analyzing the electronic evidence relating to the fraud. Both the FBI and the U.S. Secret Service have developed successful collaborations with various private companies, which often prefer to work with law enforcement without seeking any publicity for their efforts.

- *Collaboration in Public Education and Prevention Activities*. In some cases, public- and private-sector entities have successfully collaborated in developing public-education and prevention campaigns to reduce fraud and encourage reporting of fraud.

19. Please specify whether your country has enacted any laws or regulations designed to encourage or provide a legal incentive to the party of a commercial transaction to implement procedures designed to detect, deter and address fraud.

One statute that provides strong incentives for companies to implement fraud-detection and fraud-deterrence measures is the Sarbanes-Oxley Act. Section 302 of that Act, for example, provides that the chief executive officer and chief financial officer of a company shall prepare a statement to accompany the audit report to certify the appropriateness of the financial statements and disclosures contained in the periodic report, and that the financial statements and disclosures fairly present, in all material respects, the operations and financial condition of the issuer. Compliance with this requirement, by implication, requires companies to put in place policies and procedures that will aid in identifying any situation, such as fraud, that may adversely affect their operations and financial conditions.

In addition, the five federal financial institution supervisory agencies (i.e., the Federal Deposit Insurance Corporation, the Federal Reserve Board, the Office of the Comptroller of the Currency, the Office of Thrift Supervision, and the National Credit Union Administration) have in place extensive regulations designed, in part, to ensure that regulated financial institutions have in place their own antifraud measures to safeguard the safety and soundness of those institutions' operations. These measures, in turn, can create collateral pressures on companies that must do business with financial institutions to implement their own antifraud policies and procedures.

20. Please provide any available information on rates, trends and volumes with respect to fraud, including domestic offences and transnational offences that affect your country (please provide statistical information if available).

(a) Over the past 5 years, have fraud occurrences

(x) Increased? ( ) Decreased? ( ) Remained stable?

(b) Over the past 5 years, have numbers of fraud victims

(x) Increased? ( ) Decreased? ( ) Remained stable?

(c) Over the past 5 years, have the total proceeds of fraud

(x) Increased? ( ) Decreased? ( ) Remained stable?

(d) Over the past 5 years, have fraud occurrences involving foreign or transnational elements

(x) Increased? ( ) Decreased? ( ) Remained stable?

(e) Over the past 5 years, have fraud occurrences involving information or communications technologies[9]

(x) Increased ( ) Decreased ( ) Remained stable

Please specify.

With respect to each of these categories, U.S. law enforcement agencies believe, on the basis of their investigative experiences and information, that in general the incidence of fraud, number of fraud victims, total proceeds of fraud, occurrences of transnational fraud, and fraud involving information or communications technologies have increased over the past five years. There is a lack of population-wide survey data to provide any definitive support for these conclusions. Law enforcement must frequently rely on complaint data for indirect (and therefore less precise) measures of fraud trends. Here are several studies of complaint data trends and surveys:

- *FTC*. The Federal Trade Commission's fraud complaint data show that in general, the number of non-identity theft fraud complaints has steadily risen over the past three years: from 327,479 in 2003 to 406,193 in 2004 and 431,118 in 2005. This is noteworthy because for those same three years, the number of Internet-related fraud complaints, after rising for the two previous years (176,754 in 2003 and 210,727 in 2004) has shown a modest decline in 2005 (196,503). In contrast, other fraud complaints rose steadily, from 150,725 in 2003 to 195,466 in 2004 and 234,615 in 2005.[20]

  With respect to transnational fraud, the FTC's analysis of cross-border fraud complaints in 2005 shows that the number of cross-border complaints has risen consistently from 1999 (6,250) to 2005 (86,390) – an increase of nearly 1,400 percent over a seven-year period.[21] The percentage of cross-border fraud complaints has also risen steadily, if less dramatically, to account for 20

[9] Including wireline telephones, wireless or cellular telephones, fax machines, electronic mail or Internet applications.

percent of all non-identity theft fraud complaints in 2005.[22] The FTC data also show that for complaints by U.S. consumers against companies in countries other than Canada, the Internet/email has steadily become more popular as the initial method of contact, increasing from 51 percent of complaints in 2003 to 61 percent in 2004 and 64 percent in 2005. During that same three-year period, for companies in countries other than Canada the use of websites and other Internet communications remained virtually unchanged as the initial method of contact, accounting for 12 percent in 2003, 14 percent in 2004, and 13 percent in 2005. (With respect to complaints by U.S. consumers against companies located in Canada, mail was by far the most frequent method of initial contact, jumping from 13 percent in 2003 and 12 percent in 2004 to 42 percent in 2005. In contrast, for those same Canadian companies, email accounted for only 10 percent, and websites and other Internet communications for only 8 percent, of complaints.)[23]

- *IC3*. With respect to online fraud, the 2005 report of the Internet Crime Complaint Center (IC3) states that the number of complaints it received has risen steadily over the past five years. It received a total of 231,493 complaints in 2005 – an 11.6 percent increase over the 207,449 complaints received in 2004.[24] The IC3 also reported that the total dollar loss from all referred cases of fraud was $183.12 million in 2005. This loss is a dramatic increase from 2004, when the IC3 reported only $68 million in reported losses, and the three previous years.[25] The IC3 makes clear that this dramatic increase is the direct result "of a number of cases in 2005 that reported losses in the millions of dollars."[26]

- *NFIC*. The National Fraud Information Center (NFIC), a project of a nonprofit organization, the National Consumers League, reported that in 2005, telemarketing scams accounted for $4,921,932 in total losses (compared to $2,561,835 in total losses in 2004) and an average loss of $2,892 (compared to an average loss of $1,974 in 2004). The NFIC also reported that it received significantly more telemarketing-fraud complaints in 2005 (4,587) than in 2004 (2,814), and that Canada and countries outside the United States and Canada tied as the principal location for telemarketing-fraud criminals.[27]

  The NFIC also reported that in 2005, Internet fraud scams accounted for $13,863,003 in total losses (compared to $5,787,170 in total losses in 2004) and an average loss of $1,917 in 2005 (compared to an average loss of $895 in 2004). It should be noted that this reported increase of almost 33 percent in total losses correlates closely with the nearly 300 percent increase in total losses that the IC3 reported.) The NFIC also reported that it received more Internet fraud complaints in 2005 (12,315) than in 2004 (10,794), and that countries outside the United States and Canada were the principal location of Internet fraud criminals.[28]

- *CyberSource*. A 2005 survey of online merchants by CyberSource Corporation indicated that while the percentage of revenue lost to online revenue has been relatively stable over the past three years (1.7 percent in 2003, 1.8 percent in 2004, and 1.6 percent in 2005), "total losses from online

> payment fraud in the U.S. and Canada have steadily increased," from $1.9 billion in 2003 to $2.6 billion in 2004 and $2.8 billion in 2005. Merchants surveyed also reported that on average, "the rate of fraud associated with international orders is twice as high as the overall average" and that they "reject international orders at a rate three times higher than the overall average."[29]

Other regulatory agencies and associations, such as the North American Securities Administrators Association, have data that indicate increases in fraud trends.[30]

21. Please provide any further available information on transnational aspects of fraud, including rates and trends (i.e. any increases or decreases in rates), particularly on the types of fraud tending to involve elements of transnationality, as well as the elements of the offences themselves (e.g., targeting or deception of victims, transfer of victims) which are seen as most likely to include transnationality.

One dimension of transnational mass-marketing fraud schemes that warrants discussion is the criminals' use of multiple jurisdictions to conduct different aspects of their schemes. Unlike the traditional telemarketing-fraud "boiler rooms" of the 1990s, which housed the sales force, managers, administrative staff, and the organizers of the scheme in a single location, today mass-marketing fraud schemes, particularly transnational schemes, typically divide segments of their operations up among several different countries. Lists of prospective victims may come from one country, telephone salespeople may operate in a different country, and financial accounts for fraud proceeds may be established in one or multiple other locations. In addition, some criminals engaging in transnational mass-marketing fraud are known to use telephone technologies that create the appearance that they are located in the United States. These technologies include the use of cellular telephones with international service, Voice Over Internet Protocol, and call-forwarding centers in the United States that can forward calls from within the United States to locations around the world, including cell phones.

In the estimation of U.S. law enforcement authorities, these techniques constitute a calculated effort by mass-marketing fraud operators to enhance the difficulties of successful investigation and prosecution. Multiple countries therefore need to develop closer working relationships in sharing information and intelligence about significant transnational fraud schemes, and collaborating in investigating and prosecuting such schemes.

22. Does the law of your country allow for the extradition and/or prosecution of offenders who commit fraud in another country, and if so, please specify the legal requirements for such jurisdiction (e.g., nationality of offenders, nationality or location of victims etc.) and the specific law or regulation.

Yes. The United States extradites individuals pursuant to bilateral extradition treaties. The United States has more than 100 bilateral extradition treaties with foreign countries that permit extradition of fraud defendants to or from the United States. In general, United States courts will have subject-matter jurisdiction over fraud offenses originating from or conducted in another country if, for example, the effects of those offenses are felt in the United States (e.g., criminals outside the

United States send communications into the United States, or U.S.-based victims are induced to send money from their location to other locations inside or outside the United States). With respect to extradition to the United States, federal prosecutors demonstrate in their extradition requests the bases on which there is venue for the fraud offense or offenses in a particular federal judicial district in the United States. Depending on the type of fraud offense charged, venue may be based on factors such as the location of victims in the district, telephone calls or emails that came into or out of the district, and transfers of funds by victims or defendants into or out of the district. In federal criminal law, the nationality of the defendants is not a jurisdictional basis for, or a bar to, extradition.

23. In your opinion which forms of mutual legal assistance and other forms of international cooperation are most important for the prevention and investigation of transnational fraud?

Both formal legal mechanisms, such as Mutual Legal Assistance Treaties (MLATs) and extradition treaties, and informal cooperation mechanisms (e.g., investigator-to-investigator cooperation) are highly important in preventing and investigating transnational fraud. Most of the formal cooperation provided by the United States is done through requests for assistance pursuant to treaties, although the United States also provides assistance in response to letters rogatory. In addition, the United Nations Convention against Transnational Organized Crime provides an excellent mechanism of mutual legal assistance and international cooperation for parties to that convention. There are currently 140 signatories to the Convention, including the United States. The Council of Europe's Cybercrime Convention, with 13 parties and 29 other signatories to date, also has great potential for usefulness in this field. The United States has signed the Cybercrime Convention and intends to ratify it upon receiving the advice and consent of the United States Senate.

While MLATs and extradition treaties provide the essential legal foundation for sharing of evidence and formal rendition of defendants, informal cooperation mechanisms can play a critical role in improving mutual understanding of legal systems and investigative procedures and expediting progress in fraud investigations. Since 1998, for example, Canada and the United States have established a total of six joint task forces and strategic partnerships across Canada to facilitate the investigation and prosecution of transnational telemarketing-fraud schemes. These task forces and strategic partnerships have proved highly successful as a model for harnessing limited investigative resources and targeting significant fraud schemes for law enforcement action.

24. If the authorities of your country have had significant experience in dealing with transnational cases of fraud, please provide information on the types of mutual legal assistance afforded by and to your country's competent authorities, any other international cooperation mechanisms used to combat transnational fraud and the most serious problems encountered in practice (e.g., bank secrecy as a ground for denying cooperation).

In the United States, there is statutory authority (28 U.S.C. § 1782) for the appointment of commissioners who can issue subpoenas to obtain information on behalf of requesting foreign law enforcement authorities using a letter rogatory or comparable form of request for assistance in the absence of an MLAT. The United

States has used this authority with some frequency on behalf of various countries. The United States also has benefitted in many countries from both informal and formal legal assistance in various fraud cases. In transnational telemarketing-fraud cases, for example, Canada has rendered significant assistance in locating, arresting, and detaining major figures in telemarketing-fraud schemes and extraditing them to stand trial in the United States, as well as using compulsory process (i.e., search warrants) to obtain much-needed documentary evidence for use in U.S. criminal prosecutions. The most serious problem encountered in MLAT and letter rogatory requests to and from the United States may be the slowness with which the MLAT and letter rogatory processes work to provide the requesting country with the evidence sought. Countries need to examine their legal assistance processes closely to see where review and implementation of MLAT and other requests can be expedited.

25. Please provide information available, if any, and specific law or regulation on civil or criminal recovery and sharing of proceeds of fraud or other related offences where such proceeds have fraudulently been transferred to or hidden in foreign jurisdictions.

The criminal forfeiture statute (18 U.S.C. § 982(a)(1)) states that a sentencing court shall order that a person convicted of a federal money-laundering offense (18 U.S.C. § 1956, 1957, or 1960) forfeit "any property, real or personal, involved in such offense, or any property traceable to such property." Civil forfeiture is also available for these same offenses under 18 U.S.C. § 981(a)(1)(A). The federal money-laundering offenses apply to money laundering that may involve one or more foreign jurisdictions, so long as there is venue for the charged offense in the judicial district where the charge is brought. Federal law enforcement agencies have procedures for revenue-sharing with other law enforcement agencies when criminal proceeds are forfeited to the United States.

26. Please describe the mechanisms, if any, by which proceeds of fraud or other related offences that have been located in your country can be returned to their beneficiary.

Both criminal forfeiture and restitution, as described previously, can be used by federal courts to order the return of fraudulently obtained funds to the victims of a fraud scheme. In its use of consumer redress powers, the FTC also can provide for repayment of fraudulently obtained proceeds to victims.

27. Please provide information concerning the role of technologies, including transportation, information and communication technologies[10] and their impact on domestic and transnational fraud, including the following:

(a) The types of fraud tending to involve technological elements;

(b) The types of technology used;

(c) The evolution of offenders methods or techniques to use technologies more effectively (e.g. to increase proceeds, avoid detection or reduce risks);

---

[10] Including wireline telephones, wireless or cellular telephones, fax machines, electronic mail or Internet applications.

(d) The spread of offender expertise or other information, including the identities of potential victims from one offender or region to another;

(e) The use of technologies to identify, contact and deceive victims;

(f) The use of technologies to transfer or conceal proceeds;

(g) The use of technologies to deter, prevent, investigate, and prosecute offenders and/or to trace, identify and/or recover proceeds.

(a) A growing variety of fraud schemes depend substantially on technological elements. Telemarketing fraud, Internet fraud, credit- and debit-card fraud, and financial institution fraud are just a few of the types of fraud in which criminal seek to exploit technological vulnerabilities to their advantage.

(b) It should not be surprising that the more sophisticated transnational fraud schemes have tended to take advantage of cutting-edge developments in technology to communicate with victims. Cellular telephony, Voice Over Internet Protocol (VOIP), and Internet-based communications have made their way into the day-to-day operations of major advance-fee schemes, telemarketing schemes, and Internet fraud schemes.

(c) A common element in mass-marketing fraud schemes, whether they rely more on traditional telephone communications or digital communications (e.g., cellular telephones, VOIP, and other Internet-based communications such as email and websites), is their use of such technologies to conceal or falsify their true locations.

(d) Many transnational mass-marketing fraud schemes have become increasingly reliant on using the Internet to order and receive lists of prospective victims, rather than wait for mail-based delivery of such lists.

(e) Please see the response to question 27(b) above.

(f) In a number of transnational fraud schemes, criminals have been known to use certain Internet-based funds transfer mechanisms, such as E-Gold, rather than conventional banking channels to move funds. In an ongoing federal criminal prosecution of Shadowcrew.com, a multinational ring of individuals who trafficked in stolen credit and bank card numbers and identity information, six defendants, in pleading guilty to various charges, recently admitted "that Shadowcrew members sent and received payment for illicit merchandise and services via Western Union money transfers and digital currencies such as E-Gold and Web Money."[31]

(g) Particularly with Internet-related fraud schemes, law enforcement officers need to use state-of-the-art tools and techniques for tracing online communications, identifying the location of computer servers and desktop computers, analyzing traffic data and other code, and seizing and preserving electronic evidence for use in bringing and proving criminal charges.

28. Please provide, if possible, brief descriptions or summaries of the most indicative and representative cases in which the competent authorities of your country have dealt with domestic and transnational aspects of fraud or other related offences.

One excellent example of U.S. law enforcement agencies' response to transnational fraud, which also involves superior cooperation with foreign law enforcement agencies, is the Tri-West Investment Club case mentioned in the response to question 9 above. In the early phases of that case, the FBI quickly developed close working relationships with state securities regulators and with the Securities and Exchange Commission, as each of those agencies had developed related information on Tri-West and its principals. Later, as the scope of the fraud scheme became clearer, U.S. agents received excellent cooperation from Costa Rican and Canadian government authorities in tracing people and evidence. The case resulted in the successful extradition of the ringleader and another principal in the scheme from Costa Rica, and convictions of the ringleader and other scheme participants. Similarly, the recent case involving the fraud scheme in Amsterdam (also mentioned in the response to question 9) similarly involved close and ongoing cooperation and information-sharing between the U.S. Postal Inspection Service, the Amsterdam Police, and Dutch and U.S. prosecutors.

29. Please provide information about lessons learnt or useful practices developed[11] to combat or prevent fraud or other related offences at the national level or in the field of international cooperation where foreign or transnational aspects of fraud are involved.

Here are some examples of useful practices that various U.S. agencies and organizations have adopted to combat and prevent fraud:

- *Interagency Working Groups*. A number of U.S. law enforcement and regulatory agencies have benefitted from participation in interagency working groups on particular types of fraud. The Department of Justice, for example, chairs interagency working groups on bank fraud, securities and commodities fraud, and telemarketing and Internet fraud. These working groups, which include headquarters-level representatives from all agencies with an interest in that type of fraud, have proved invaluable as forums for discussion of fraud trends, development of joint law-enforcement training, analysis of investigative techniques, and other significant information.

- *Task Forces*. In extraordinary circumstances, where a particular type of fraud has become a source of nationwide concern, U.S. law enforcement has sometimes found it necessary to create a national task force to combat the problem aggressively and in close coordination. In 2002, President Bush established the Corporate Fraud Task Force to make the investigation and prosecution of corporate wrongdoing a high priority. More recently, in September 2005, Attorney General Alberto Gonzales established the Hurricane Katrina Fraud Task Force to provide a fully coordinated nationwide response to all types of hurricane-related fraud, including charity fraud,

[11] Best practices should include legislative action, operational or investigative techniques and preventive policies, and encompass both the private commercial and public criminal law areas. Best practices should also include information on how national authorities collect and review complaints of fraud.

emergency-benefit fraud, identity theft, insurance fraud, government-contract fraud, and public corruption. This Task Force includes representatives of the Department of Justice, the FBI, the U.S. Secret Service, the Postal Inspection Service, the federal Inspectors General, the Federal Trade Commission, and state and local law enforcement.

Even where the problem does not require a single national task force, multiagency regional task forces, like the telemarketing fraud task forces described in the response to question 23 above, may be an efficient way of attacking certain types of transnational fraud where the participating countries have a common border and investigators can readily move between the countries in accordance with mutually-agreed procedures. When fraud becomes more transnational in scope and impact, law enforcement agencies in multiple countries will need to operate as "virtual task forces," making full use of modern communications technology to share investigative information, coordinate investigative activities, and trace evidence when long distances make day-to-day meetings impractical.

- *Receipt and Analysis of Transnational Fraud Complaints*. Another technique, begun at the national level, that is paying dividends at the international level is the establishment of mechanisms in multiple countries for receiving and analyzing fraud complaints from the public. In 2001, the FTC, along with representatives of 12 other countries, established econsumer.gov, a joint effort to gather and share cross-border e-commerce complaints to improve international law enforcement agencies' ability to address cross-border Internet fraud and deception. In addition, the Internet Fraud Complaint Center has been discussing with law enforcement officials in various countries how they can establish their own mechanisms for receiving and analyzing online fraud complaints in their own countries, while taking steps where possible to facilitate international sharing of complaint data among law enforcement agencies.

PART II: IDENTITY FRAUD

30. Please provide a short description of the infrastructure(s) used in your country to establish and verify identity in both the private and public sectors, including mechanisms and procedures to ensure commercial identification, the validity of electronic signatures or the legitimacy and validity of travel or identity documents.

Electronic identification systems, electronic signatures, and other identity-related digital technologies are making their way into many aspects of public and private life, but infrastructures for establishing and verifying identity run the gamut from the lowest-tech methods (e.g, visual inspection of identification documents) to highly sophisticated digital technologies (e..g, scanning of passports at airport ticket agents, customs and border inspection points, and airline e-ticketing kiosks).

31. Please provide information on whether your country has enacted legislation concerning the disclosure of personal private information and indicate whether there are any laws regarding access to personal private information (e.g., access to documents filed in offices such as birth certificates), as well as what monitoring measures have been implemented for

handling such information.

The United States has laws relating to information about consumers held by government agencies, including the Privacy Act of 1974. These laws prohibit the unauthorized disclosure of information about individuals, and gives consumers the right to review records about themselves, find out if records have been disclosed, and request corrections or amendments of these records. Under the Fair Credit Reporting Act, consumers can seek correction of incorrect information in their credit reports.

With regard to protecting personal information, the United States has a number of laws in this area. The Federal Trade Commission Act, the general federal consumer protection statute that prohibits unfair or deceptive acts or practices, gives the Federal Trade Commission the authority to file cases against companies that are engaged in unfair or deceptive acts or practices in the area of consumer privacy. To supplement the FTC Act, there are federal statutes and regulations to protect the most sensitive consumer information. For example, under the Gramm-Leach-Bliley Act, the Federal Trade Commission has implemented rules concerning financial privacy notices and the administrative, technical and physical safeguarding of personal information. The Gramm-Leach-Bliley Act also prohibits pretexting. Another example is the Children's Online Privacy Protection Act, which gives parents control over what information is collected from their children online and how such information may be used.

In addition to federal laws, states also enact legislation relating to consumer privacy. For example, according to a recent newspaper report, the State of Florida is requiring its counties to post all public records (not including court documents) online by January 1, 2007, but to remove Social Security, bank, credit, charge and debit card numbers from all official records before then to minimize the risk of identity theft. The task is reportedly so large that there may be further postponements of the posting deadline.[32]

Congress has passed legislation – the IRAIIRA (1996) and the Real ID Act (2005) – that mandates the creation of birth documents and driver's licenses that are highly secure, formatted in a standardized manner, and with identical content, that will be in electronic sharable databases. Since the present system of documents designed and produced by each state has shown itself to be a major vulnerability in allowing people to steal identities, movement to close them off is a major positive.

32. Please indicate the types of documents or information, including intangible data, regarded as identification information[12] in your country's legal system.

While there may be some differences in definitions between particular pieces of legislation pertaining to identifying information, one general legal definition of

---

12

Generally, references to identification information in this questionnaire are intended to include information which can be used alone or in combination with other information to establish identity. Examples include not only information such as names, addresses or birth dates, but the numbers or other information needed to use bank accounts, credit cards and other public or private infrastructures. A credit-card number, for example, is commonly used in combination with the name of the card-holder, expiry date and sometimes other information to establish the identity of the card-holder for purposes of credit transactions.

identifying information can be found in the federal identity theft offense (18 U.S.C. § 1028(a)(7)). That offense defines the term "means of identification" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any—

"(A) name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

"(B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

"(C) unique electronic identification number, address, or routing code; or

"(D) telecommunication identifying information or access device (as defined in [18 U.S.C. §] 1029(e))."[33]

33. Some countries have described identity fraud as the conduct involving either the transfer, possession, or use of another (legal or natural) person's identification information (including tangible identification documents and intangible data or other information) or of a false identity, or the takeover of another person's identity[13], in connection with the commission of a crime.

(a) Does this provide a reasonably accurate description of problems encountered in your country?

(x) Yes ( ) No

(b) Has your country developed a similar or other concept or label to describe such conduct?

(x) Yes ( ) No

Please specify or indicate similarities or differences between definitions or descriptions used in your country.

The definition of identity theft in the federal identity theft offense (18 U.S.C. § 1028(a)(7)) is closely similar to the above definition. Subsection 1028(a)7) prohibits knowingly transferring, possessing, or using, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law. Similarly, the aggravated identity theft offense (18 U.S.C. § 1028A(a)(1)) prohibits knowingly transferring, possessing, or using, without lawful authority, a means of identification of another person, during and in relation to any of numerous specified federal felonies listed in that section. Most states also have some form of identity-theft offense, and these generally follow the basic concepts of the above definition.

34. Has the conduct described as identity fraud been made a crime in your country?

(x) Yes ( ) No

---

13 Including cases of hishing in which victims are induced to provide their own identity information via the Internet to offenders masquerading as commercial or authority figures.

See the response to question 33 above.

35. Are any elements of the conduct described as identity fraud or related conduct (such as the falsification, forgery or misuse of identification information or documents) a separate crime in your country?

(x) Yes ( ) No

36. If the answer to question(s) 34 and/or 35 is yes, please indicate by which offence or offences and provide text of the legislative provision or detailed description of the conduct constituting the crime(s).

The identification-document statute (18 U.S.C. § 1028(a)) contains several federal criminal offenses relating to falsifying or forging identification documents. These include (1) knowingly and without lawful authority producing an identification document, authentication feature, or a false identification document; (2) knowingly transferring an identification document, authentication feature, or a false identification document knowing that such document or feature was stolen or produced without lawful authority; (3) knowingly possessing with intent to use unlawfully or transfer unlawfully five or more identification documents (other than those issued lawfully for the use of the possessor), authentication features, or false identification documents; and (4) knowingly possessing an identification document (other than one issued lawfully for the use of the possessor), authentication feature, or a false identification document, with the intent such document or feature be used to defraud the United States. It should be noted that none of these offenses are lesser included offenses of the identity theft offenses.

Other offenses relating to identification documents include:

- False statement in application and use of passport (18 U.S.C. § 1542). This offense criminalizes any false application for a passport either for the perpetrator's own use or the use of another; and it criminalizes the use or provision to another of a falsely obtained passport.
- Forgery or false use of passport (18 U.S.C. § 1543). This statute states that it is a crime to falsely make, forge, counterfeit, mutilate or alter any passport or instrument purporting to be a passport with the intent to use it; or to use, attempt to use or to furnishes to another any passport or any such document.
- Misuse of passport (18 U.S.C. § 1544). This offense states that it is a crime to use or attempt to use any passport issued or designed for the use of another; or use or attempt to use any passport in violation of the conditions or restrictions or rules prescribed pursuant to the laws regulating issuance of passports; or furnishes, disposes of or delivers a passport to any person for use by another than the person for whose use it was originally intended.
- Fraud and misuse of visas, permits and other documents (18 U.S.C. § 1546). This statute contains a number of separate offenses criminalizing different aspects of fraud that involves immigrant and non-immigrant visas, permits, border crossing cards, alien registration cards, or other documents prescribed by statute or regulation for entry into or as evidence of authorized stay or employment. Subsection 1546(a) prohibits the forgery, counterfeiting, alteration or making of the above documents or the uttering, use, attempt to use, possession, acceptance or receipt; or who falsely applies for such a

document. Subsection 1546(b) makes it an offense to use an identification document knowing that the document was not issued lawfully, knowing that the document is false, or making a false attestation for the purpose of satisfying a requirement of Section 274A(b) of the Immigration and Nationality Act.

37. Whether or not specific offences have been established, please indicate whether, in your opinion, the problem of identity fraud is increasing or decreasing in scope or seriousness in your country, and if so what levels and trends have been encountered at the domestic level. Has the problem

(x) Increased? ( ) Decreased? ( ) Remained stable? ( ) Other? [14]

Please explain.

With respect to general trends in identity theft, there are several indications that both the scope and the seriousness of identity theft in the United States are substantial. Here are several sources of information on the issue:

- For 2004 and 2005, the Better Business Bureau (BBB) and a private sector research company, Javelin Strategy and Research, have collaborated on surveys of U.S. adults about identity fraud. In 2004, the BBB-Javelin survey found that approximately 9.3 million adults had been victims of identity fraud within the preceding year, and that total losses (individual and corporate) from identity fraud were more than $52 billion. In 2005, the BBB-Javelin survey found that 8.9 million U.S. adults had become victims of identity fraud in the preceding year, and that total losses from identity theft exceeded $56 billion. It is unknown whether the decrease of the number of victims from 2004 to 2005 is statistically significant, but it is noteworthy that with the decrease in the number of victims and the increase in total losses, the average loss to identity fraud increased in 2005.

- A recently published survey by the Department of Justice's Bureau of Justice Statistics found that in 2004, 3.6 million households reported that at least one member of the household had become a victim of identity theft in the preceding six months.[34]

- According to the Federal Trade Commission, which has statutory responsibility for receiving identity theft complaints nationwide, identity theft has consistently been the leading category of consumer complaints over the past several years. Over the past three years in particular, the number of identity theft complaints increased: from 215,177 in 2003 to 246,847 in 2004, then to 255,565 in 2005.[35]

38. With which of the following offences is identity fraud or similar conduct most commonly associated and what is the role it plays in the commission of these offences either as a preparatory step or as part of the offence itself?

[14] For example, records not kept or occurrences too few or infrequent to establish rates or trends.

(a) Fraud;

(x) Yes ( ) No

(b) Money-laundering;

(x) Yes ( ) No

(c) Unlawful access to facilities or information;

(x) Yes ( ) No

(d) Concealment of domestic or transnational organized crime or terrorist activities;

(x) Yes ( ) No

(e) Trafficking in persons;

( ) Yes (x) No

(f) Smuggling of migrants;

( ) Yes (x) No

(g) Immigration offences;

( ) Yes (x) No

(h) Other offences?

(x) Yes ( ) No

Please describe the role played by identity fraud in these offences or other relevant links to the offences.

(a) In the experience of U.S. law enforcement and regulatory agencies, fraud is the crime most commonly associated with identity fraud. Identity theft/identity fraud provides the means by which criminals engaging in fraud schemes can access victims' financial accounts, establish new financial accounts in victims' names, withdraw or transfer funds, and evade detection when banks or credit-card companies initially believe that the identity fraud victims were responsible for the fraudulent transactions.

(b) Identity fraud may also play a role to some degree in money laundering, at least in the initial phases after the criminals have received illegal proceeds from victims.

(c) Identity fraud also makes possible criminals' unlawful access to facilities or information. For example, some criminals have acquired usernames and passwords of Internet users who have accounts with online auction sites, then

conducted spurious auctions through the accounts of auction site members to make it appear that they are reputable and recognized members of that site, and obtained payments from people who believed they were successful bidders in those auctions.

(d) Identity fraud may help in concealing organized crime or terrorist activities, although it is likely that criminals engaged in organized crime or terrorist activities use identity fraud primarily to conceal their personal identities rather than their affiliation with a criminal group.

(e, f, g) In the experience of U.S. law enforcement, trafficking in persons, smuggling of migrants, and immigration offenses in the United States tend more to be associated with the creation of false identification documents to match the migrants' true names than to engage in identity fraud. However, identity fraud does frequently occur in connection with all three types of crime.

(h) Identity fraud plays a major role in passport fraud, whether in the assumption of another person's identity (living or dead) in order to fraudulently apply for a passport, or in the counterfeiting or alteration of another person's passport or the impersonation of another person in order to use the other person's passport.

39. Please identify the means used to commit identity fraud or similar conduct, including electronic and physical means to obtain identity documents or identification information and to misuse it for the purposes of other criminal offences (e.g., postal mail theft, pickpocket, computer hacking, forgery or falsification of documents, etc.).

Because information is often described in terms of "flows," it may be useful to categorize the principal means of identity fraud with respect to places or processes in society where information flows are most highly concentrated in motion or at rest. Here are some of the principal places and processes:

- *Mail*. Identity thieves often concentrate on the mail because large volumes of documents, credit cards, and financial data routinely flow through the mail system to homes and businesses. In particular, identity thieves have focused on all three phases of mail delivery:
  - *Incoming Mail*. Identity thieves often seek to steal incoming mail that contains preapproved credit-card offers, credit cards, convenience checks from credit-card companies, and financial data being delivered to people's residences. If they obtain preapproved credit-card offers, the identity thieves can submit the application form, using an address different from that of the intended recipient, and explain that they have changed addresses. If they obtain convenience checks, the criminal can simply forge the names on the checks and cash them or negotiate them.
  - *Outgoing Mail*. Identity thieves may also steal outgoing mail because it often contains bill payments and billing data. A typical credit-card payment, for example, will contain not only the billing invoice (including the number and types of the credit card) but also the check (including the account and routing numbers) of the person paying the bill.

- *Mail in Transit*. In an effort to be more efficient in obtaining large volumes of mail that they can review for valuable data, credit cards, or checks, identity thieves have been known to target various places where mail concentrates while in transit through the postal system. Some criminal have tried to break into mail collection boxes, while others may try to steal even larger quantities of mail. In a recent prosecution in Baltimore, Maryland, a former baggage handler at Baltimore-Washington International Airport was sentenced to 14 years imprisonment for his role in an elaborate identity fraud and fraud scheme. The scheme involved stealing financial documents from the U.S. mail at the airport and transferring those financial documents to others for processing. The stolen mail contained checks and credit cards which were addressed to individuals who were not part of the conspiracy. The conspirators would use the stolen financial documents to obtain cash advances and withdrawals from lines of credit, as well as obtain goods and services paid for by credit accounts to which they were not entitled.[36]

At the same time, it is important to note that the United States mail remains one of the most secure means of transmitting personal information. A survey by the Federal Trade Commission of ID theft victims disclosed that 96 percent believed their identity had been stolen through electronic breaches, dishonest employees of financial institutions or data processors, theft of wallets or pursues, or by a trusted family member or friend - none of which have anything to do with mail. Issued in late 2003, the FTC study is the most recent comprehensive, independent survey of identity theft in the United States. The same study disclosed that victims were:

- 3 times more likely to have information stolen via a financial transaction—from a credit card receipt or during a purchase, or purchases via the Internet, mail, or phone.
- 3 ½ times more likely to have information stolen by a known individual, such as a family member, friend or co-worker.
- 3 ½ times more likely to have identity stolen as the result of a lost or stolen wallet, checkbook, or credit card.

According to Bank Technology News, March 2005, more than 80 percent of identity crimes today are attributed to electronic sources and the creation of fake identities through technology. Since January 2005, there were almost 52 million instances of identity compromise involving electronic commerce, involving data secured by well-known entities such as MCI, Time Warner, Citifinancial, Bank of America, and the FDIC. This number is substantial, and far outweighs the incidents of mail theft during the same period.

- *Trash*. Once people receive documents containing valuable personal data at their homes or places of business (e.g., bank and credit-card statements, customer lists), they often discard the documents without making any efforts to shred the documents or to render the data unusable. As a result, some criminals in identity-fraud operation engage in what is known as "dumpster diving" (or "bin raiding" in the United Kingdom). The value of the discarded data far outweighs the momentary discomfort of rummaging through trash.

- *Theft from Personal Areas*. Some identity thieves use primitive methods to obtain people's credit cards and identification document, by simply breaking into cars or health club lockers while they are unattended. The thieves can then provide the stolen cards and documents to others in the identity-fraud operation, who manufacture counterfeit identification documents to match the credit cards. Still other participants in the operation then use the counterfeit identification and the credit cards to purchase valuable items in the names of the identity theft victims. In some cases, the identity thieves with access to the victims' personal areas prove to be family members, friends, acquaintances, and employees. The 2006 BBB/Javelin survey cites lost or stolen wallets, credit and debit cards, or checkbooks as the most commonly reported means of identity fraud.[37]

- *Commercial and Academic Institutions*. Large businesses often acquire substantial amounts of valuable personal data from its own customers, or from transactions that they process for other entities. Academic institutions also have large aggregations of personal data about their students and applicants. Identity thieves often target these types of institutions for large-scale identity fraud. In some cases, the methods are high-tech, involving computer hacking of computers where valuable data are stored. In other cases, criminal groups often seek to compromise an employee already inside the institution and obtain the employee's help in obtaining large quantities of data, or even arranging for an affiliate of the criminal group to get a job at the institution that they can then exploit to obtain the data.

- *Home Computers and the Internet*. In addition to attacking business computer systems, identity thieves also have used a variety of techniques to obtain valuable personal information from home computers or from Internet users while they are online. One of the fastest-growing techniques for engaging in this type of identity fraud is "phishing." Phishing refers generally to the creation and use of emails and websites that are designed to look as though they belong to legitimate businesses or government agencies. In a typical phishing scheme, criminals send large volumes of emails to people across the Internet. Each email purports to come from a legitimate business or agency, and warns or advises the recipient that he or she must "reverify" or "confirm" their personal data with the company or agency by clicking on an email link in the body of the "phishing" email. If the recipients click on the link, they are often taken to what appears to be a legitimate corporate or government website, which directs them to enter a variety of personal information (e.g., credit-card number, expiration date, PIN number, Social Security number, and sometimes bank account numbers). None of these data, of course, are actually requested by the company or agency. Instead, the criminals in the phishing scheme harvest the data submitted through their spurious website, then sell the stolen data to others or use it to commit financial fraud.

  Phishing has grown dramatically over the past two years. According to a leading industry coalition on phishing, the Anti-Phishing Working Group (APWG), in March 2006 APWG researchers found a total of 9,666 unique

phishing sites worldwide (compared to only 2,870 phishing sites found in March 2005). This total also appears to be reflective of a continuing trend. In contrast to December 2005, when 7,197 phishing sites were found (the highest total for any month in 2005), the total number of phishing sites had exceeded 9,000 for each of the first three months of 2006. In addition, APWG received 18,480 reports of phishing attacks in March 2006 – the most ever recorded for a one-month period.[38]

One reason that phishing is a substantial concern for financial institutions that that phishing schemes typically target the financial sector. The APWG reported that in March 2006, the financial sector continued to be the most heavily targeted industry sector, accounting for 90 percent of all phishing attacks that month.[39] In addition, the APWG reported that "for the first time in many months, a bank was the number one phished company, by a large margin. This would potentially indicate that the phishers have found a way to easily monetize the phished credentials for this particular financial institution."[40]

Phishing schemes also have been making increasing use of malicious computer code to conduct identity theft. In some schemes, the APWG reports, clicking on the link in a phishing email can trigger the downloading of a "Trojan horse" program to the Internet user's computer. In some cases, the Trojan horse contains software that allows the criminals behind the phishing attack to log all of the pertinent keystrokes when the user whose computer is infected tries to access his or her online bank account. The phishing scheme can then retrieve the keylogged code and use it to access the Internet users' bank accounts. In other cases, the Trojan horse may contain a "backdoor" program that allows the participants in the phishing scheme to access the Internet users's computer at any time and access any files and data in that computer. In March 2006, APWG researchers found an all-time high of 197 unique phishing-based Trojan horses.[41]

It should be noted that persons wishing to assume a new identity have also purchased document packages from document vendors; purchased citizenship and identity documents from unscrupulous individuals, or assumed the identity of known living or deceased individuals. In the last case, a criminal would research obituaries or a cemetery until he or she found someone who died at an early age. The criminal would then apply for and obtain a birth certificate, and with that document, build an identity.

40. Please indicate which types of identification document or information are most commonly encountered or involved in identity fraud or similar conduct in your country:

(a) Domestic government identification documents (e.g., birth certificates, identity cards etc.);

(x) Yes ( ) No

(b) Domestic commercial identification documents (e.g., credit cards, debit cards or other bank identification);

(x) Yes ( ) No

(c) Passports, visas or other international travel or identity documents;

(x) Yes ( ) No

(d) Intangible identification information (e.g., personal data, credit or debit card access numbers, e-mail addresses, etc.

(x) Yes ( ) No

41. With respect to the involvement of organized criminal groups in the commission of identity fraud, please identify how such groups are organized or structured (e.g., on the basis of ethnicity, hierarchical concepts or systems of mutual obligation and/or benefit) and what, if any, trends exist in this regard.

In the United States, there is no single predominant type of organized criminal group engaging in identity fraud. In some identity-fraud rings, members are predominantly from a particular Eastern European country, such as Russia or Romania, or from West African countries such as Nigeria. In many other identity-fraud rings that would meet the definition of "organized crime" under the United Nations Transnational Organised Crime Convention, there is no common ethnicity or national affiliation.

In general, identity-theft operations involving more than two or three multiple individuals do not have an elaborate hierarchical structure. As indicated in the responses to previous questions, more elaborate schemes seem to be divided mostly by functional responsibility: some engage in theft of credit and debit cards and identification documents (or identifying data); others manufacture counterfeit documents; still others engage in purchases with the stolen cards, identification, or data; and one or two individuals serve as ringleaders and directors of the operation.

42. Please identify the impact, if any, of social, cultural or ethnicity factors on the formation of such groups (e.g. prior meetings and affiliation of group members through places of origin, involvement in travelling communities or drug culture, or contact in prison systems).

Even in cases involving more extensive identity fraud operations, law enforcement authorities do not always know how the members of the operation first met each other. Methamphetamine users are often cited by law enforcement agencies as a subcategory of drug users who become involved in identity fraud.

43. Please provide any qualitative or quantitative information available about the harm or damage caused by identity fraud, including monetary and non-monetary losses, and what individuals or interests are adversely affected, including persons whose identities are taken or misused and persons who may be victims of other related offences such as frauds[15].

[15] The victims of identity fraud could be seen as including both the persons whose identity is exploited who may suffer harm ranging from loss or reputation and commercial damage to mistaken arrest and the victims of frauds or other offences committed using false identification.

Individual identity fraud victims can suffer a wide variety of monetary harms. The Federal Trade Commission's 2005 complaint data on identity theft listed the following types of misuse of identity fraud victims' data:

- Credit card fraud (26 percent of all complaints), including creation and use of new accounts and misuse of existing accounts;
- Phone or utilities fraud (18 percent), including creation of new wireless, telephone, and utilities accounts and unauthorized charges to new accounts;
- Bank fraud (17 percent), including electronic funds transfer, misuse of existing accounts, and creation of new accounts;
- Employment-related fraud (12 percent);
- Loan fraud (5 percent), including business/personal/student loans, auto loans and leases, and real estate loans; and
- Other identity theft (25 percent), including apartment or house rental and bankruptcy.[42]

The 2006 BBB/Javelin survey reported a total of $56.6 billion in identity fraud losses in 2005; this figure includes both individual and corporate losses. It is significant that this survey found from 2003 to 2005, the average fraud amount per victim had increased substantially (21.6 percent) to $6,383 in 2005. The survey also found that while 68 percent of victims incurred no costs related to their fraud cases, average consumer costs in 2005 were $422 but average time to resolve identity fraud cases had increased substantially from 33 hours in 2003 to 40 hours in 2005.[43]

In addition to monetary costs that many identity fraud victims incur – though many do not if the identty theft involved credit cards in their names – victims may also suffer various types of non-financial harm. This can include adverse credit ratings, difficulties in getting loans, and adverse inferences that lenders or prospective employers about their financial stability. In some cases, where criminal have used the victims' names in encounters with the criminal justice system, such as arrests and court appearances, victims unknowingly have criminal records created under their names and sometimes have even been mistakenly subject to arrest.

44. What is the impact of commercial factors, such as banking and credit-card systems, on the commission of identity fraud or other similar conduct?

As is true for fraud (see the response to question 17 above), banking and credit-card systems, as well as computer-based technologies such as the Internet, can be both targets and instrumentalities for identity fraud. Identity thieves have been known to hack into financial institution databases and to persuade employees of financial institutions to disclose valuable customer data.

45. How, in your opinion, could the public and commercial sectors most effectively deter, prevent and control identity fraud, and in what areas could they collaborate most effectively with one another?

One of the most productive approaches that the public and commercial sectors have been using to deal with identity-theft and identity-fraud issues is the creation of multi-sectoral working groups, organized by private companies, that provide a common forum for discussion of technological and other solutions to identity fraud

with each other and with government agencies. The following descriptions of two multi-sectoral working groups interested in identity theft indicate the types of approaches that such groups can develop to address various aspects of identity fraud:

- *Anti-Phishing Working Group*. The Anti-Phishing Working Group (APWG) is an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing. The APWG has more than 2,300 members and more than 1,500 companies and government agencies participating in the APWG's activities. It provides a forum to discuss phishing issues, define the scope of the phishing problem in terms of hard and soft costs, and share information and best practices for eliminating the problem. Where appropriate, the APWG will also look to share this information with law enforcement. Membership is open to qualified financial institutions, online retailers, ISPs, the law enforcement community, and solutions providers.

- *Liberty Alliance*. Formed in September 2001, the Liberty Alliance is a global consortium of more than 150 leading merchants, service providers, technology vendors, and government organizations that work together to address the technical and business issues associated with federated network identity. The Alliance is engaged in the ongoing release of open technical specifications as well as business and policy guidelines to help companies deploy federated identity services across a broad range of products, services, and devices.[44] In recent months, the Alliance has held workshops on identity theft prevention in Chicago and Tysons Corner, Virginia. These workshops brought together law enforcement and private-sector representatives to explore potential technological and procedural solutions to the problem of identity fraud.

In this context, it should be noted that federal regulators have been focusing on the need for improved safeguards for information. Not all companies have implemented appropriate protection for consumer information. The Federal Trade Commission (FTC) has brought suit against companies whose failure to implement reasonable security put consumers at risk. To date, the FTC has brought 13 such cases. These cases were brought under three statutes enforced by the Commission: Title V of the Gramm-Leach-Bliley Act ("GLBA"), Section 5 of the Federal Trade Commission Act ("FTC Act"), and the Fair Credit Reporting Act ("FCRA"). For example, in its recent case against ChoicePoint, Inc., the Commission alleged that this major data broker failed to use reasonable procedures to screen prospective subscribers and monitor their access to sensitive consumer data, in violation of the FCRA and the FTC Act. The Commission's complaint alleged that ChoicePoint's failures allowed identity thieves to obtain access to the personal information of over 160,000 consumers, including nearly 10,000 consumer reports. In settling the case, ChoicePoint agreed to pay $10 million in civil penalties for the FCRA violations – the highest civil penalty ever levied in a consumer protection case – and $5 million in consumer redress for identity theft victims. The order also requires ChoicePoint to implement a number of strong data security measures, including biennial audits to ensure that these security measures are in place.

In another recent action, the Commission reached a settlement with CardSystems Solutions, Inc., the card processor allegedly responsible for last year's breach of credit and debit card information for Visa and MasterCard, which exposed tens of millions of consumers' credit and debit card numbers. This case addresses the largest known compromise of sensitive financial data to date. As in the ChoicePoint case, the FTC alleged that CardSystems engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for sensitive consumer data. These settlements provide important protections for consumers and also provide important lessons for industry about the need to safeguard consumer information. Information on other FTC data security cases can be found at http://www.ftc.gov/privacy/index.html.

46. Please provide any available information on transnational aspects of identity fraud, including rates and trends (i.e. any increases or decreases in rates), the types of identity fraud which tend to involve elements of transnationality, as well as whether the transnational nature refers to the identity fraud per se or the underlying offence(s) supported or facilitated by the identity fraud.

Phishing is one type of identity fraud that routinely has transnational aspects. According to the APWG, the top ten countries where phishing websites were hosted in March 2006 included the United States (35,13 percent), China (11.93 percent), Republic of Korea (8.85 percent), Germany (3.57 percent), Canada (3.52 percent), Japan (2.39 percent), Romania (2.29 percent), Spain (2.13 percent), Brazil (1.97 percent), and Argentina (1.92 percent). In addition, the top ten countries that hosted malicious code involving keylogging software were the United States (39.87 percent), Spain (10.7 percent), China (6.02 percent), Russia (2.94 percent), Brazil (2.67 percent), Republic of Korea (2.2 percent), United Kingdom (2.09 percent), Argentina (1.26 percent), Portugal (1.1 percent), and Germany (0.94 percent).[45]

It is important to note that the mere fact that a phishing or keylogger website is located in a particular country does not necessarily mean that the criminals behind the phishing scheme are also located in that country. Because criminals can engage in unauthorized access to computers in many countries, it is entirely possible that criminals will choose to host their phishing sites in countries far removed from their actual location. Even so, international cooperation in these types of cases is essential, as law enforcement authorities in the country where the site is hosted may be able to obtain evidence that will be of assistance to law enforcement authorities in another country where many of the victims are located.

Even more than phishing, the type of identity fraud that has the most immediate and visible transnational aspects is passport fraud and (in some cases) visa fraud. Both passport and visa fraud allow perpetrators to travel internationally. If the fraud is well done there can, in some cases, be low risk of detection. Travel document-related identity fraud is often associated with other transnational crimes, whether illegal migration for employment, or in furtherance or organized criminal activity or terrorism.

47. If the authorities of your country have had significant experience in dealing with transnational cases of identity fraud, please provide information on the types of mutual legal assistance afforded by and to your country's competent authorities, any other

international cooperation mechanisms used to combat identity fraud and the most serious problems encountered in practice.

Both formal and informal legal assistance are essential in pursuing transnational cases of identity fraud. In the Shadowcrew case mentioned in the response to question 27(f) above, U.S. law enforcement authorities benefitted from extensive cooperation with law enforcement authorities in multiple countries.

48. What relationships exist between information and communications technologies[16] and identity fraud and how these are encountered or perceived in your country, given the extent to which technologies are available and identity and related systems are paper-based or electronic?

Law enforcement authorities generally believe that the growth of the Internet vastly increased the access of criminals to valuable personal data in home computers and enterprise systems, and to ecommerce sites where they can order high-value merchandise with stolen or fraudulently obtained credit and debit cards. As preceding responses should indicate, identity fraud can be committed through low-tech methods (e.g., theft of wallets or compromise of employees), high-tech methods (e.g., hacking and phishing), or a combination of both. Law enforcement responses to identity fraud must therefore address low-tech and high-tech methods.

49. Please provide, if possible, brief descriptions or summaries of the most indicative and representative cases illustrating how identification information was obtained or fabricated and used and how the problem was detected or reported and investigated.

The following summaries highlight some federal prosecutions, involving various types of identity fraud, that took place in 2005 and 2005. These summaries are not intended to suggest that these are the only types of identity fraud cases that U.S. law enforcement authorities will investigate and prosecute, or that they are the only types of cases that can be successfully investigated. These cases represent only a small percentage of all the identity fraud case that the U.S. Department of Justice prosecutes nationwide.

Central District of California

- U.S. v. Calvin Guidry (C.D. Cal., indictment filed July 6, 2005)
  - On July 6, 2005, a federal indictment in the Central District of California charged Calvin Guidry and John Wayne Avery on federal conspiracy charges (18 U.S.C. § 371), for their involvement in an identity theft scheme targeting retired employees of Toyota Motor Corporation and numerous other victims and financial institutions. The scheme involved the use of stolen identities and homemade counterfeit identification to obtain tens of thousands of dollars of fraudulent personal loans from multiple banks. Guidry and Avery were arrested previously by the Long Beach Police Department at a bank in Long Beach, California, while picking up a check drawn on a

[16] Including wireline and wireless or cellular telephones, fax machines, electronic mail and Internet applications.

bogus loan. After their arrest, the Long Beach Police Department searched their residences and seized extensive evidence related to identity theft, including hundreds of counterfeit credit cards and identity documents in the names of countless of identity theft victims. Further investigation revealed that a third man, Eric Thomas, was found to be a primary source of illegally obtained credit reports used in the scheme to commit identity theft. Thomas used his own company, Title Wave Real Estate, to gain unauthorized access to numerous consumer credit reports which were then used by the fraud ring to create false identity documents and to fraudulently obtain loans, credit, and goods.

- On February 25, 2006, Guidry, who had been a fugitive for months after his 2005 indictment, was arrested by the Hawthorne (California) Police Department for a misdemeanor violation and was transported to the custody of the FBI on an outstanding federal felony warrant for identity theft. Guidry's trial was set for April 25, 2006 and Thomas's trial was set for April 18, 2006. Avery has pleaded guilty.[46]

- U.S. v. Lateef Oyewo (C.D. Cal., pleaded guilty Feb. 1, 2006)
  - Two Southern California residents who possessed thousands of print-outs containing personal information fraudulently obtained from ChoicePoint Service and other companies pleaded guilty to federal credit-card fraud charges. On February 1, 2006, Lateef Oyewo pleaded guilty to conspiracy, computer intrusion and credit card fraud. Previously in this case, on November 29, 2005, Babaranti Jemiri pleaded guilty to conspiracy and credit card fraud. When entering their guilty pleas, Oyewo and Jemiri admitted working together to obtain personal data - including names, dates of birth and social security numbers - and to use that data to fraudulently sign up for new credit cards or to "take over" already existing accounts. Both defendants also admitted having access to a storage locker containing thousands of ChoicePoint print-outs and credit card profiles, documents that were found by law enforcement authorities in July 2005. Oyewo specifically admitted to accessing the Intelius database service under false pretenses and using that service to fraudulently obtain personal information belonging to other people. Oyewo also admitted to using a fraudulently obtained credit card to make unauthorized ATM withdrawals totaling $1,160 from just one account.
  - When he pleaded guilty in 2005, Jemiri admitted using credit cards obtained during the scheme to withdraw more than $3,300 in cash from a single account and to order more than $3,000 in goods from Internet retailers. Jemiri ordered the goods to be delivered to mailboxes he had opened up under assumed identities. Jemiri also pleaded guilty to possessing more than 15 credit cards belonging to other people. The government estimates that the actual loss associated with the credit card fraud tied to Jemiri and Oyewo is more than $1 million.[47]

Southern District of Florida

- U.S. v. Angela Blount (S.D. Fla., sentenced Oct. 7, 2005)
  - On October 7, 2005, Angela Blount was sentenced to fifty-seven (57) months' imprisonment and ordered to pay $136,568.01 in restitution, which includes $50,000 in restitution to the victims for legal bills. Blount pleaded guilty on July 22, 2005 to six (6) counts of an indictment charging her with identity theft, in violation of 18 U.S.C. § 1028, and access device fraud, in violation of 18 U.S.C. § 1029. This identity theft investigation commenced when Blount fraudulently purchased a 2004 Audi A6 at Champion Auto Sales in Pompano Beach, Florida. Thereafter, as a result of an extensive collaborative effort between the Broward Sheriff's Office and the U.S. Secret Service, investigators uncovered evidence revealing that Blount had applied for and received numerous credit cards, personal loans, home mortgages, and automobile loans, all using the Social Security numbers of two unsuspecting victims, between July 11, 2001 and January 23, 2004. Once Blount obtained these loans and credit cards, Blount went on a spending spree. Before her arrest, Blount had successfully obtained over $341,000 in financing, credit, and property.[48]

Georgia - Northern District

- U.S. v. Teresa Knight et al. (N.D. Ga., pleaded guilty January 11, 2006)
  - On January 11, 1006, Teresa Knight and Lori Lackey, who organized and engaged in a scheme of identity fraud that spanned several counties, pleaded guilty to possession of stolen mail. Knight and Lackey acknowledged that, throughout 2004, they illegally dealt methamphetamine and were often paid by their "customers" with stolen mail. The two women would then use financial documents or instruments contained in the stolen mail -- such as paychecks, credit cards or bank statements -- to commit identity fraud. Knight and Lackey eventually compiled over 700 pieces of stolen mail either as payment for drugs or through their own theft, as they moved from receiving stolen mail from their meth "customers" to stealing it themselves from residential mailboxes. The mail was taken from homes in several different counties, including Jasper, Rockdale and Newton Counties. A common ploy executed by the duo was to alter the name of the payee on a stolen check to one of their names, and then cash the check at a local grocery store. They would also make charges on credit cards recovered from stolen mail.[49]

Eastern District of Louisiana

- U.S. v. Joseph Bartholomew III et al. (E.D. La., indictment filed June 3, 2005)
  - A federal grand jury in the Eastern District of Louisiana indicted Joseph Bartholomew III, Joyell Patrice Dabon, and Tracy Bright Thomas. Bartholomew was charged with one count of conspiracy in

violation of 18 U.S.C. 371; three counts of forging endorsements on a U. S. Treasury check in violation of 18 U.S.C. § 510(b); and three counts of theft of mail by an employee, in violation of 18 U.S.C. § 1709. Dabon and Thomas were both charged with one count of conspiracy in violation of 18 U.S.C. § 371; along with three counts of forging endorsements on a U.S. Treasury Check in violation of 18 U.S.C. § 510(b); and three counts of theft of mails, in violation of 18 U.S.C. § 1708. According to the Indictment, Bartholomew, in his position as a Postal employee, would steal U.S. Treasury checks from the U. S. mail. Once the U.S. Treasury checks had been stolen, Dabon allegedly would then take the stolen U.S. Treasury checks to Thomas, who worked as a cashier at a local Winn Dixie, and cash the stolen U.S. Treasury checks. According to the indictment, as a result of the criminal scheme, they stole fifty-one (51) U.S. Treasury checks for an approximate total of more than $34,000.[50]

Western District of Louisiana

- U.S. v. Isaac Carloss (W.D. La., convicted February 15, 2006)
  - On February 15, 2006, Isaac H. Carloss, Jr., was convicted at trial on one count of conspiracy, one count of theft of mail, and two counts of theft of public money. Carloss's wife and co-defendant, Debbie Anderson, pleaded guilty in January 2006 to one count of conspiracy. Testimony at trial revealed that Anderson met an evacuee at a rescue shelter following Hurricane Katrina and gave that individual permission to use Anderson's address to receive their mail. When an express mail package arrived at Anderson's residence addressed to the evacuee, Anderson signed for the mail with a fictitious name and opened the mail, which contained two FEMA disaster assistance checks which were intended for the evacuee. Carloss and Anderson took the checks and went to a local car dealership and persuaded the salesman to allow them to use one of the checks to purchase a car. Carloss and Anderson took the other check to a bank in Jonesville, Louisiana, and persuaded the teller to cash the check for them because they were victims of the hurricane. The total amount of the checks was $4,358.[51]

Maryland

- U.S. v. Kehinde Oladapo (D. Md., pleaded guilty May 9, 2005; sentenced Sept. 21, 2005)
  - On September 21, 2005, the U.S. District Court for the District of Maryland sentenced Kehinde Akintola Oladapo to 14 years imprisonment for theft or receipt of stolen mail and conspiracy to commit bank fraud. The court further ordered that Oladapo pay $7 million in restitution and further ordered the liquidation of his assets in payment of restitution.
  - According to the statement of facts presented at his guilty plea on May 9, 2005, Kehinde Oladapo was a Southwest Airlines ramp agent.

Sometime before or during 2001, Oladapo conspired to steal financial documents from the U.S. mail at BWI airport and transfer those financial documents to others for processing. The stolen mail contained checks and credit cards which were addressed to individuals who were not part of the conspiracy. The conspirators would use the stolen financial documents to obtain cash advances and withdrawals from lines of credit, as well as obtain goods and services paid for by credit accounts to which they were not entitled. Kehinde Oladapo received proceeds exceeding $2,000 per month for the stolen financial documents and credit cards which he had sent to co-conspirators in New York and other locations using Express Mail.[52]

Massachusetts

- U.S. v. [Juvenile] (D. Mass., pleaded guilty and sentenced September 8, 2005)
  - On September 8, 2005, a Massachusetts juvenile pled guilty in federal court and was sentenced in connection with a series of hacking incidents into Internet and telephone service providers; the theft of an individual's personal information and the posting of it on the Internet; and making bomb threats to high schools in Florida and Massachusetts; all of which took place over a fifteen month period. Victims of the Juvenile's conduct have suffered a total of approximately $1 million in damages. The Court imposed a sentence of 11 months' detention in a juvenile facility, to be followed by 2 years of supervised release. During his periods of detention and supervised release, the Juvenile is also barred from possessing or using any computer, cell phone or other electronic equipment capable of accessing the Internet.
  - The sentence is the result of the Juvenile's guilty plea to both the Massachusetts and Arkansas charges. The basis for the charges was a course of criminal conduct that took place over a fifteen-month period beginning in March, 2004 when the Juvenile sent an e-mail to a Florida school that contained highly threatening language that included a bomb threat. As a result of this bomb threat, the school was closed for two days, while a bomb squad, a canine team, the fire department and Emergency Medical Services were called in
  - In August, 2004, the Juvenile logged into the Internet computer system of a major Internet Service Provider ("ISP") using a program he had installed on an employee's computer. This program allowed the juvenile to use the employee's computer remotely to access other computers on the internal network of the ISP and gain access to portions of the ISP's operational information. In January, 2005, the Juvenile gained access to the internal computer system of a major telephone service provider that allowed him to look up account information of the telephone service provider's customers. He used this computer system to discover key information about an individual who had an account with the telephone service. He then accessed the information stored on this individual's mobile telephone, and posted the information on the Internet. During this same time period, the

Juvenile used his access to the telephone company's computer system to set up numerous telephone accounts for himself and his friends, without having to pay for the accounts. Also in January, 2005, an associate of the Juvenile set-up accounts for the Juvenile at a company which stores identity information concerning millions of individuals allowing the Juvenile to look at the identity information for numerous individuals, some of which he used for the purpose of looking up the account information for the victim whose personal information he posted on the Internet. In the spring of 2005, the Juvenile, using a portable wireless Internet access device, arranged with one or more associates to place a bomb threat to a school in Massachusetts and local emergency services, requiring the response of several emergency response units to the school on two occasions and the school's evacuation on one. In June, 2005, the Juvenile called a second major telephone service provider because a phone that a friend had fraudulently activated had been shut off. In a recorded telephone call, the Juvenile threatened the telephone service provider that if the provider did not provide him access to its computer system, he would cause its web service to collapse through a denial of service attack - an attack designed to ensure that a website is so flooded with request for information that legitimate users cannot access the website. The telephone service provider refused to provide the requested access. Approximately ten minutes after the threat was made, the Juvenile and others initiated a denial of service attack that succeeded in shutting down a significant portion of the telephone service provider's web operations.[53]

Minnesota

- U.S. v. Billy Felder (D. Minn., pleaded guilty Oct. 12, 2005; sentenced March 15, 2006)
  - On March 15, 2006, Billy Felder, who admitted filing false federal and state tax returns using other individuals' names, was sentenced to 30 months in prison; $58,829 in restitution to the Internal Revenue Service; and $47,473 in restitution to the Minnesota Department of Revenue. Felder pleaded guilty on October 12, 2005 to one count of making a false or fraudulent claim against the United States and to one count of identity theft, both felonies. At the time of his plea, Felder admitted that he filed numerous false tax returns with both the Internal Revenue Service and with the Minnesota Department of Revenue claiming over $300,000 in fraudulent refunds. His scheme involved stealing the identities of deceased persons and then filing tax returns in their names. He used the identities of other deceased persons to claim dependency exemptions on the fraudulent returns, which he in turn used to claim refunds based upon the Earned Income Tax Credit on the federal returns and upon Minnesota's Working Family Credit on the Minnesota returns. Felder filed all of the returns electronically, and he fraudulently induced the Internal Revenue Service and the Minnesota Department of Revenue electronically to transmit the refunds to bank

accounts controlled by Felder.[54]

Eastern District of New York

- U.S. v. Rasheta Bunting et al. (E.D.N.Y., complaint unsealed Feb. 22, 2006)
  - Federal criminal charges were filed against four defendants in an identity theft ring that used personal information from the Social Security Administration's computer system to steal tens of thousands of dollars in Social Security benefit payments and other money from elderly and disabled beneficiaries in the New York City area and across the country between January 2004 and February 2006. According to the complaint, which charged the defendants with conspiracy to commit wire fraud, defendant Rasheta Bunting was employed as a Teleservice Representative at the Social Security Administration ("SSA") with access to the SSA's database of personal information, including names, social security numbers, and bank account information, for Social Security beneficiaries throughout the United States. Bunting used her access to beneficiaries' information to change the bank accounts designated by beneficiaries for direct deposit of their Social Security benefit payments to bank accounts controlled by Bunting and her co-conspirators Sherrell Footman, Rahkeem Sales, and Vladimir Anilus. Once a benefit payment was deposited into one of the controlled accounts, the defendants would switch the bank account information in the database back to the beneficiary's actual account in order to conceal the fraud. The process of altering and then restoring a victim's actual bank account information would frequently be repeated several times as the defendants continued to divert the payments to accounts they controlled.
  - The scheme to defraud was uncovered when Footman and Anilus were arrested by the New York Police Department (NYPD) after attempting to cash a check drawn on the account of one of the victims whose personal information Bunting had accessed in the SSA's computer database. The NYPD, in conjunction with the United States Secret Service, SSA, and the Queens County District Attorney's Office, then executed a search warrant at the residence of Footman and Sales.[55]

Northern District of Texas

- U.S. v. Jackie Allen Jones, Jr. (N.D. Tex., pleaded guilty Aug. 23, 2005)
  - On August 23, 2005, Jackie Allen Jones, Jr., pleaded guilty to one count of unlawful production of a false identification document. Sentencing is set for December 1, 2005. In March 2005, Jones was charged in a six-count indictment with various counts relating to his possession of stolen mail matter, as well as three additional counts relating to identity theft. Jones admitted in court documents that from October 1, 2004 through October 27, 2004, he stole many pieces of mail from several apartment complexes and other locations throughout areas in and around Dallas and Mesquite, Texas. Jones also admitted that on October 27, 204, he caused another individual to produce a

fraudulent Texas drivers license. This fraudulent drivers license was in the name of another individual, a victim of identity theft. This fraudulent document appeared to be the drivers license of the victim. During the same time frame mentioned above, Jones used this fraudulent Texas driver's license to pass several checks drawn on the account of the victim. On October 27, 2004, while driving on south Jupiter Road in Garland, Texas, Jones was stopped by Garland Police Officers and at the time of the traffic stop, Jones presented the police officers with the fraudulent drivers license he had been using. Jones also had in his possession four blank checks drawn on the same victim's account. In addition, police officers found a tub of stolen mail, including monthly bank statements, monthly credit card statements and monthly telephone bills, in the trunk of Jones's vehicle.[56]

Southern District of Texas

- U.S. v. Adeshina Olanrewaju Lawal (S.D. Tex., convicted Jan. 11, 2006)
  - On January 1, 2006, Adeshina Olanrewaju Lawal was convicted at trial of attempted bank fraud and possession of a counterfeit security. During the two-day trial, the jury heard that a cooperating witness contacted an inspector with the U.S. Postal Inspection Service, telling the inspector that Lawal, a friend of hers, had asked her to help him steal high-end bank account information. The cooperating witness was an employee of Washington Mutual Bank. The cooperating witness told the agent Lawal was involved in an identity theft and bank fraud scheme. Under the direction of the U. S. Postal Inspector, the cooperating witness (CW) contacted Lawal and told him she could not access the type of account information he wanted without the effort being easily traced to her. Given this circumstance, Lawal asked the CW whether she would be willing to deposit fraudulent checks into her bank account for him. Lawal also asked the CW to obtain a cashiers check so that he could use it as a sample to counterfeit large checks. On September 19, 2004, the CW gave Lawal a $20 Washington Mutual check as a sample as requested. On November 1, 2004, while under surveillance by U. S. Postal Inspectors, the CW met with Lawal in a parking lot at Westheimer and Wilcrest in Southwest Houston. At this meeting, Lawal delivered to the CW a counterfeit check in the amount of $435,361 that he claimed he had received from his contacts in Nigeria with instructions to deposit the check into her account, then withdraw the money, and spilt it with him when the check cleared. Lawal was arrested by agents after he delivered the counterfeit check to the CW.[57]

Eastern District of Virginia

- U.S. v. Occident (E.D. Va., convicted at trial April 19, 2006)
  - On April 19, 2006, Constance Occident was convicted in the U.S. District Court for the Eastern District of Virginia of conspiracy to

commit wire fraud, conspiracy to commit credit-card fraud, conspiracy to disclose individually identifiable health care information, and aggravated identity theft. The maximum potential sentence is 33 years imprisonment, $1,500,000 in fines, and full restitution. U.S. District Judge Gerald Bruce Lee set sentencing for July 14, 2006. On April 14, 2006, Judge Lee sentenced Occident's co-defendant, Beurn Daphne Ferdinand to 71 months imprisonment, restitution of $244,370 and five years of supervised release.

- According to papers filed in court, from February 2004 through June 2005, Occident was a Care Team Specialist in the Intermediate Care Unit at INOVA Alexandria Hospital in Alexandria, Virginia. She took the individually identifiable personal information, including Social Security numbers, of approximately 100 patients and employees at the hospital. Occident provided the information to Ferdinand who opened fraudulent credit card accounts, and the two defendants then incurred charges on those accounts exceeding $240,000. Before Occident's and Ferdinand's arrests in July 2005, they had stolen and used the information of 44 patients and seven nurses at the hospital. Many of the patients were older than 65 and several are now deceased. Occident admitted at the trial that she and Ferdinand had targeted the information of older patients.[58]

Western District of Washington

- U.S. v. Evangelos Soukas (W.D. Wash., pleaded guilty July 22, 2005)
  - On July 22, 2005, Evangelos Dimitrios Soukas pleaded guilty to conspiracy to commit wire and mail fraud, conspiracy to commit fraud using another person's identifying information, and numerous individual counts of identity fraud and of submitting fraudulent claims to the Internal Revenue Service. In his plea agreement, Soukas admits to using a variety of schemes from 1999 to 2004, in his attempts to defraud his victims of more than a million dollars. Soukas was arrested on January 14, 2005, as he arrived at the airport in Cyprus. The FBI had alerted Interpol that Soukas was wanted in the United States.
  - According to the plea agreement, Soukas posted false and fraudulent advertisements for merchandise on various Internet auction web sites, knowing he did not have the merchandise and having no intention of delivering it. Soukas used a variety of user names and email addresses when he posted the ads. Soukas sometimes would advertise and deliver inexpensive items to buyers in order to obtain positive reviews on the web sites. He would also use different user names and email addresses to "purchase" items he advertised. He did this so he could then post positive reviews of himself on the web site to increase the likelihood that other buyers would trust him. Soukas advertised expensive electronic equipment such as laptop computers, camcorders and cell phones. But after purchasers mailed Soukas checks or paid into a PayPal account, they never received the merchandise. One purchaser was sent a box containing rocks and Styrofoam packing. Soukas also used at least 15 victims' names, Social Security Numbers and dates of

birth to open bank accounts, to apply for lines of credit and loans on the internet, and to purchase merchandise. Using the false identities, Soukas had more than $18,000 of Dell computer equipment shipped to his Monroe address. He had more than $5,000 worth of Target merchandise and gift cards shipped to his address, again using fraudulent identities. Using false identities, he fraudulently applied for home equity lines of credit in his victims' names. Soukas also filed false income tax returns in his victims' names in an attempt to obtain tax refunds to which he was not entitled. He even applied for refund anticipation loans in his victims' names.

- In early 2000, Soukas fled the United States for Greece and avoided arrest. However, he continued to use false identities to commit fraud. In December 2003, he made a failed attempt to transfer $285,000 from a victim's Fidelity Investment account into Soukas's bank account in Greece. Soukas also had blank checks from two of his victims' bank accounts mailed to him in Greece. In Athens, Soukas forged and deposited one of these checks for $8,000. He forged and deposited another one of these checks for $60,000. He attempted to run up charges on his victims' credit card accounts, to obtain cash advances, and to raid E-Trade and bank accounts. In all, Soukas's fraud totaled $1,136,067.03.
- On December 19, 2005, Soukas was sentenced to 92 months imprisonment, restitution in the amount of $107,075.95, and a special assessment fee of $3,900.[59]

50. Please provide information about lessons learnt or useful practices developed[17] to combat or prevent identity abuses at the national level or in the field of international cooperation where foreign or transnational aspects of identity fraud are in issue.

Law enforcement in the United States has developed several useful practices to combat identity fraud:

- *Task Forces*. In various areas of the United States, federal, state, and local law enforcement authorities have formed multiagency identity fraud task forces. These task forces typically share intelligence and investigative information about identity-theft activities in their region, and provide participating agencies to make the most efficient use of their respective resources to pursue significant identity fraud cases.

- *Identity Theft Subcommittee*. Since May 1999, the Department of Justice has chaired the Identity Theft Subcommittee of the Attorney General's Council on White Collar Crime. The membership of this national-level working group includes all of the key federal law enforcement agencies that investigate identity fraud, as well as the Federal Trade Commission (FTC), federal bank regulatory agencies, and state and local law enforcement representatives. The Subcommittee, which meets monthly, provides participating agencies with

[17] Useful practices could include legislative action, operational or investigative techniques and preventive policies, and encompass both the private commercial and public criminal law areas. Best practices should also include information on how national authorities collect and review complaints of fraud.

regular updates on significant identity fraud prosecutions and trends and developments in identity fraud enforcement, prevention, and legislation, as well as a venue for cooperative efforts in identity fraud training for law enforcement agencies.

- *Law Enforcement Training*. Under the sponsorship of the Subcommittee, for example, since 2002 several federal law enforcement agencies – the Department of Justice, the Postal Inspection Service, the Secret Service, the FTC, and the FBI – and the American Association of Motor Vehicle Administrators have jointly sponsored a series of more than 20 regional training seminars on identity fraud for state and local law enforcement agencies around the United States. In addition, the Department of Justice has incorporated training modules on identity fraud into a variety of courses for federal prosecutors at its National Advocacy Center.

- *Public Education and Prevention Measures*. The FTC also has created a substantial online resource on identity fraud for members of the public at a special website, www.consumer.gov/idtheft. This set of webpages includes information about identity fraud, guidance on how to recognize and report identity fraud and how identity fraud victims should address the problems they encounter, and an online complaint form to report identity fraud.

- *Legislation*. A key component in the federal law enforcement response to identity fraud has been the enactment of the two federal identity theft offenses, 18 U.S.C. §§ 1028(a)(7) and 1028A. (See the responses to questions 32-33 above.) Even though federal prosecutions of identity fraud can use a variety of fraud-related offenses in charging defendants, the identity theft offenses make clear that identity theft is itself a form of criminal conduct that warrants criminalization and prosecution. Most states have now adopted some form of identity-theft legislation. In addition, recent federal legislation - the Fair and Accurate Credit Transactions Act (FACTA) - provides consumers with a greater measure of access to and control over their personal data. Consumers, for example, can now annually order one free credit report from each of the three major credit bureaus.[60] This allows them to review their credit reports to see whether there are any outstanding lines of credit or debts that they did not authorize.

Private-sector entities also are pursuing a variety of measures to reduce the incidence and severity of identity fraud. These include the following:

- *Identity Theft Assistance Center*. The Identity Theft Assistance Center (ITAC) is a cooperative initiative of the financial services industry that provides a free victim assistance service for customers of member companies. The ITAC is run by the Identity Theft Assistance Corporation, a not-for-profit membership corporation sponsored by two other private-sector organizations, The Financial Services Roundtable and BITS. ITAC helps victims of identity theft by reducing the delay and frustration that consumers often experience as they restore their financial identity. First, the identity theft victim and the ITAC member company resolve any issues at that company. Then ITAC

walks the consumer through his or her credit report to find suspicious activity, notifies the affected creditors, and places fraud alerts with the credit bureaus. In addition, ITAC shares information with law enforcement and the Federal Trade Commission to help catch and convict the criminals responsible for identity theft.

- *Multifactor Authentication*. U.S. banks are increasingly considering the use of multifactor authentication for online transactions. In a survey of 21 of the top 50 retail U.S. banks, a research organization, the Aite Group, found that 57 percent of those banks are planning to roll out online multifactor authentication by the end of 2006, 10 percent of the banks will start their rollout of multifactor authentication in 2006 and complete it in 2007, and 24 percent will finalize their plans in 2006 and start rolling out multifactor authentication in 2007. To date, according to the survey, 5 percent of the banks surveyed have already rolled out online authentication.[61]

* * *

May 15, 2006

ENDNOTES

1. Available at http://www.census.gov/prod/2005pubs/06statab/banking.pdf.

2. *See* http://www.irta.com/Page.asp?Script=27.

3. *See* http://www.sba.gov/gopher/Business-Development/Success-Series/Vol8/barter.txt.

4. *See* http://www.census.gov/prod/2005pubs/06statab/infocomm.pdf.

5. *See* FEDERAL TRADE COMM'N, CONSUMER FRAUD AND IDENTITY THEFT COMPLAINT DATA, JANUARY 1 - DECEMBER 31, 2005 at 4 (2006), *available at* http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

6. *See* NATIONAL WHITE COLLAR CRIME CENTER AND FBI, IC3 2005 INTERNET CRIME REPORT at 3 (2006), *available at* http://www.ic3.gov/media/annualreport/2005_IC3Report.pdf.

7. *See, e.g.,* HURRICANE KATRINA FRAUD TASK FORCE, A PROGRESS REPORT TO THE ATTORNEY GENERAL: FEBRUARY 2006 (2006), *available at* http://www.usdoj.gov/katrina/Katrina_Fraud/HKFTF_Docs/katrinareportfeb2006.pdf.

8. *See, e.g.,* Florida Division of Financial Services, Division of Insurance Fraud, http://www.fldfs.com/fraud/.

9. *See* BINATIONAL WORKING GROUP ON MASS-MARKETING FRAUD, MASS-MARKETING FRAUD (2003), *available at* http://www.usdoj.gov/opa/pr/2003/May/remmffinal.pdf.

10. *See* U.S. Dep't of Justice, Press Release (October 5, 2004), *available at* http://www.usdoj.gov/opa/pr/2004/October/04_crm_680.htm.

11. *See* U.S. Attorney's Office for the District of Connecticut, Press Release (January 11, 2006), *available at* http://www.usdoj.gov/usao/ct/Press2006/20060111.html.

12. *See* Office of the Coordinator for Counterterrorism, U.S. Dep't of State, Country Reports on Terrorism 2005 *passim* (2006)

13. *See* United States v. Hammoud, 381 F.3d 316 (4th Cir. 2004) (en banc), on remand, 405 F.3d 1034 (4th Cir. 2005).

14. *See* Prepared Statement of Dennis M. Lormel, Chief, Terrorist Financial review Group, FBI, Before the Subcommittee on Technology, Terrorism, and Government Information of the Committee on the Judiciary, United States Senate (July 9, 2002), *available at* http://www.fbi.gov/congress/congress02/idtheft.htm.

15. *See* U.S. Dep't of Justice, Press Release (March 23, 2006), *available at* http://www.usdoj.gov/opa/pr/2006/March/06_crm_167.html.

16. *See, e.g.,* U.S. Attorney for the Eastern District of California, Press Release (May 16, 2003), *available at* http://www.usdoj.gov/criminal/cybercrime/waagePlea.htm.

17. *See* 18 U.S.C. §§ 1956(a)(7)(A) and (D), 1961(1).

18. NATIONAL WHITE COLLAR CRIME CENTER, THE 2005 NATIONAL PUBLIC SURVEY ON WHITE COLLAR CRIME at 2 (2006).

19. *See* SYNOVATE, FEDERAL TRADE COMMISSION - IDENTITY THEFT SURVEY REPORT (2003), *available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf; JAVELIN STRATEGY AND RESEARCH, IDENTITY FRAUD SURVEY REPORT (2006), *summary available at* http://www.javelinstrategy.com/uploads/2006IDFBrochure.pdf; Bureau of Justice Statistics, U.S. Dep't of Justice, Identity Theft, 2004 (2006), *available at* http://www.ojp.usdoj.gov/bjs/pub/pdf/it04.pdf.

20. FEDERAL TRADE COMM'N, *supra* note 5, at 4.

21. *See* Federal Trade Comm'n, Cross-Border Fraud Complaints, January - December 2005 at 4 (2006), *available at* http://www.ftc.gov/bcp/conline/edcams/crossborder/PDFs/Cross-BorderCY-2005.pdf.

22. *Id*. at 5.

23. *Id.* at 11.

24. NATIONAL WHITE COLLAR CRIME CENTER AND FBI, *supra* note 6, at 4.

25. *Id.* at 3, 6.

26. *Id.* at 8.

27. National Fraud Information Center, Telemarketing Scams, January - December 2005 (2006), *available at* http://www.fraud.org/toolbox/2005_Telemarketing_Fraud_Report.pdf.

28. National Fraud Information Center, Internet Scams Fraud Trends, January - December 2005 (2006), *available at* http://www.fraud.org/2005_Internet_Fraud_Report.pdf.

29. CYBERSOURCE CORPORATION, 7TH ANNUAL ONLINE FRAUD REPORT at 3 (2006), *available at* http://www.cybersource.com.

30. *See* NASAA, *available at* http://www.nasaa.org.

31. *See* U.S. Attorney's Office for the District of New Jersey, Press Release (November 17, 2005), *available at* http://www.usdoj.gov/usao/nj/publicaffairs/NJ_Press/files/shad1117_r.htm.

32. *See* Ian Katz, *Cities, counties walk a fine line to keep public records open and personal information secret*, South Florida Sun-Sentinel, April 30, 2006, *available at* http://www.tmcnet.com/usubmit/2006/04/30/1625164.htm.

33. 18 U.S.C. § 1028(d)(7).

34. *See* Bureau of Justice Statistics, *supra* note 19.

35. Federal Trade Comm'n, *supra* note 5, at 4.

36. *See* U.S. Attorney's Office for the District of Maryland, Press Release (September 21, 2005), *available at* http://www.usdoj.gov/usao/md/press_releases/press05/OladapaKehindeSent.pdf.

37. *See* JAVELIN STRATEGY AND RESEARCH, *supra* note 19, at 7.

38. *See* ANTI-PHISHING WORKING GROUP, PHISHING ACTIVITY TRENDS REPORT: MARCH, 2006 at 2 (2006), available at http://www.antiphishing.org/reports/apwg_report_mar_06.pdf.

39. *Id.* at 4.

40. *Id.* at 3.

41. *Id.* at 6-7.

42. *See* Federal Trade Comm'n, *supra* note 5, at 13.

43. *See* JAVELIN STRATEGY AND RESEARCH, *supra* note 19, at 1.

44. *See* Liberty Alliance, http://www.projectliberty.org/.

45. *See* Anti-Phishing Working Group, *supra* note 38, at 4, 8.

46. *See* FBI Los Angeles Division, Press Release (March 6, 2006), *available at* http://losangeles.fbi.gov/pressrel/2006/la030606.htm.

47. *See* U.S. Attorney's Office for the Central District of California, Press Release (February 1, 2006), *available at* http://www.usdoj.gov/usao/cac/pr2006/012.html.

48. *See* U.S. Attorney's Office for the Southern District of Florida, Press Release (October 11, 2005), *available at* http://www.usdoj.gov/usao/fls/051011-02.html.

49. *See* U.S. Attorney's Office for the Northern District of Georgia, Press Release (January 11, 2006), *available at* http://www.usdoj.gov/usao/gan/press/01-11-06.pdf.

50. *See* U.S. Attorney's Office for the Eastern District of Louisiana, Press Release (June 3, 2005), *available at* http://www.usdoj.gov/usao/lae/hotnews/internal_postal_arrests.htm.

51. *See* U.S. Attorney's Office for the Western District of Louisiana, Press Release (February 15, 2006), *available at* http://www.usdoj.gov/usao/law/news/wdl20060215.html.

52. *See* U.S. Attorney's Office for the District of Maryland, Press Release (September 21, 2005), *available at* http://www.usdoj.gov/usao/md/press_releases/press05/OladapaKehindeSent.pdf.

53. *See* U.S. Attorney's Office for the District of Massachusetts, Press Release (September 8, 2005), *available at* http://www.usdoj.gov/usao/are/pr/PR2005/September2005/BostonJuvenileHackerPlea.pdf.

54. *See* U.S. Attorney's Office for the District of Minnesota, Press Release (March 15, 2006), *available at* http://www.usdoj.gov/usao/mn/press/econ/econ0075.htm.

55. *See* U.S. Attorney's Office for the Eastern District of New York, Press Release (February 22, 2006), *available at* http://www.usdoj.gov/usao/nye/pr/2006feb21.htm.

56. *See* U.S. Attorney's Office for the Northern District of Texas, Press Release (August 23, 2005), *available at* http://www.usdoj.gov/usao/txn/PressRel05/jones_jackie_ple_pr.html.

57. *See* U.S. Attorney's Office for the Southern District of Texas, Press Release (January 12, 2006), *available at* http://www.usdoj.gov/usao/txs/releases/January2006/060112-Lawal.pdf.

58. *See* U.S. Attorney's Office for the Eastern District of Virginia, Press Release (April 19, 2006), *available at* http://www.usdoj.gov/usao/vae/Pressreleases/04-AprilPDFArchive/06/20060419occidentnr.pdf.

59. *See* U.S. Attorney's Office for the Western District of Washington, Press Release (July 22, 2005), *available at* http://www.usdoj.gov/usao/waw/press/2005/jul/soukas.htm.

60. *See* Federal Trade Comm'n, FREE Annual Credit Reports, *available at* http://www.ftc.gov/bcp/conline/edcams/freereports/index.html.

61. *See* Aite Group, Press Release (April 17, 2006), *available at* http://www.aitegroup.com/reports/200604171.php?PHPSESSID=f5ca28f34f2c8853e0b8082559f7476c.