



## Industry & Government Information-Sharing Resources Related to Payments Fraud Updated May 3, 2012

---

This list provides resources that share information about payments fraud and related risks. The list is not comprehensive, and it does not reflect any endorsement of a given resource. Vendors that specialize in anti-fraud services are not listed individually.

### Accredited Standards Committee (ASC) X9

- ASC X9 is a financial industry standards committee whose scope is approved by American National Standards Institute. Standards and guidelines include standards to reduce financial data security risk and vulnerabilities. The ASC X9 website is [www.x9.org](http://www.x9.org).

### American Bankers Association (ABA) National and State

- The ABA provides a variety of information pertaining to payments fraud and mitigation. The ABA's website address is [www.aba.com](http://www.aba.com).
- ABA peer group benchmarking program includes groups that focus on payments fraud.
- Other ABA resources include conferences and telephone briefings, which frequently include payments fraud and related security topics, e.g., ABA Risk Management Forum's annual conference, and the ABA's resources and services pertaining to fraud and security at [www.aba.com/solutions/fraud.htm](http://www.aba.com/solutions/fraud.htm).

### Anti-Fraud Services Vendors

- Many vendors share information regarding payments fraud via website content, blogs and alerts.

### Anti-Phishing Working Group (APWG)

- APWG is a global pan-industrial and law enforcement association focused on eliminating the fraud and identity theft that result from phishing, pharming and email spoofing of all types. The APWG's public website is [www.antiphishing.org](http://www.antiphishing.org). The site provides news, white papers, best practice information, and statistics and resources including sponsoring vendors' products and services.

### Association of Certified Fraud Examiners (ACFE)

- The ACFE's focus is on fraud and white-collar crime, which includes issues associated with payments fraud. The ACFE website address is [www.acfe.com](http://www.acfe.com) makes available a wide variety of fraud resources including reports, newsletters, and tools. The bi-weekly newsletter is free and available by e-mail subscription.
- The ACFE hosts conferences, seminars and offers online learning tools.
- ACFE has over 150 chapters around the world with approximately 90 chapters in the U.S. Local chapters meet on a periodic basis, e.g., monthly or quarterly. Contact information and website links for local chapters are available on the ACFE's website.

### Association for Financial Professionals (AFP)

- The AFP is an association for treasury and finance professionals. The AFP provides a variety of information pertaining to payments including information on payments fraud through its blog, newsletter, magazine articles and its annual *Payments Fraud & Control Survey*. The AFP's website address is [www.afponline.org](http://www.afponline.org).

### ATM Industry Association (ATMIA)

- ATMIA is a worldwide organization that has several forums such as the security, anti skimming, and electronic payments forums. Groups meet via tele-conference/seminar. ATMIA groups and committees provide best practice information, training, whitepapers, articles and crime map information. The ATMIA website address is [www.atmia.com](http://www.atmia.com) and the U.S. region is [www.atmia.com/regions-united-states/united-states](http://www.atmia.com/regions-united-states/united-states).

### Bank Administration Institute (BAI)

- BAI is an education and research organization serving the financial services industry. BAI website address is [www.bai.org](http://www.bai.org).

### The Bank Fraud Forum

- The Bank Fraud Forum<sup>SM</sup> is an open forum for the fraud fighting community. It offers analysis of trends, news, best practices and a vehicle to engage in discussion. The *Fraud News* archive is searchable. The forum's website address is [www.mementosecurity.com/bankfraudforum](http://www.mementosecurity.com/bankfraudforum).

### BankInfoSecurity.com

- BankInfoSecurity.com is an online educational portal dedicated to educating the Banking Information Security community. The website address is [www.bankinfosecurity.com](http://www.bankinfosecurity.com).
- It conglomerates targeted industry news, editorials on management and regulatory issues, whitepapers, and educational events.

### Better Business Bureau (BBB)

- The BBB provides resources for consumers and businesses. BBB website address is [www.bbb.org/us](http://www.bbb.org/us).
- The BBB's Resource Library contains *Alerts*, which provide information related to recent frauds and other marketplace issues. The URL for alerts is <http://www.bbb.org/us/business-alerts/>.

### Bitpipe.com

- Bitpipe provides access to information-technology (IT) vendors' white papers, product information, Webcasts, case studies, and analyst reports. The site offers IT-focused information including information on cyber-security and threats. The site provides RSS feeds. The website address is [www.Bitpipe.com](http://www.Bitpipe.com).

### BITS

- BITS is a not-for-profit, financial service industry consortium. BITS provides information and fosters collaboration to address emerging issues across financial services, technology, and commerce. The BITS website address is [www.bitsinfo.org](http://www.bitsinfo.org).

### Canadian Anti-Fraud Centre (CAFC)

- Canadian Anti-Fraud Centre is the central agency in Canada that collects information and criminal intelligence on mass marketing fraud, advance fee frauds, internet fraud and identity theft complaints that have Canadian content, from North American consumers and/or victims. The CAFC provides education to the public about specific fraudulent schemes and investigative assistance to law enforcement agencies by collecting and sharing victim information, statistics and documentation. The website address is [www.phonebusters.com](http://www.phonebusters.com). The CAFC sponsors the Fraud Prevention Forum, a group of over 125 private sector firms, consumer and volunteer groups, government agencies and law enforcement organizations. The forum has education and information sharing events.

### Card Payment & Network Providers

- Most of these companies provide e-mail alerts pertaining to fraud and related risks. This information may also be available on their websites (see Visa [www.visa.com](http://www.visa.com), MasterCard [www.mastercard.com](http://www.mastercard.com), PULSE [www.pulsenetwork.com](http://www.pulsenetwork.com), SHAZAM Network, etc.).

### Consumer Financial Protection Bureau (CFPB)

- The Consumer Financial Protection Bureau is in the process of establishing an Office of Financial Education. That office will coordinate programs relating to financial literacy and consumer education, providing tools that will help families make financial decisions. The CFPB website address is <http://www.consumerfinance.gov/>.

### Credit Union National Association (CUNA) and Regional CU Associations

- CUNA is a credit union trade association. Fraud prevention resources and educational materials as well as links to regional credit union networks/leagues are available on its website at [www.cuna.org](http://www.cuna.org).

### CyberSource

- CyberSource, a merchant services provider, publishes an annual *Online Fraud Report* and provides information about fraud prevention tools. CyberSource website address is [www.cybersource.com](http://www.cybersource.com).

### Federal Deposit Insurance Corporation (FDIC)

- The FDIC website ([www.fdic.gov/index.html](http://www.fdic.gov/index.html)) provides financial institution (FI) letters, examiner information, news and other information some of which pertains to payments fraud and risks. Information for financial service organizations and consumers regarding fraud schemes and alerts are:
  - FDIC *Special Alerts*, alerts are related to questionable activity involving banks or banking products. Alerts are available online ([www.fdic.gov/news/news/SpecialAlert/2012/](http://www.fdic.gov/news/news/SpecialAlert/2012/)) or pushed to a receiver via e-mail subscription service.
  - *FDIC Quick Links for Consumers and Communities* ([www.fdic.gov/quicklinks/consumers.html](http://www.fdic.gov/quicklinks/consumers.html)) that lists links to FDIC consumer alerts, identity theft information, financial education, and other resources.

### Federal Financial Institutions Examination Council (FFIEC)

- FFIEC is an interagency body. Information such as bulletins and letters are issued by the agencies. FFIEC website address is [www.ffiec.gov](http://www.ffiec.gov). The FFIEC hosts several websites where resources can be accessed, such as examiner training, handbooks, educational information for the public, and whitepapers. A few of these resources are listed below:
  - FFIEC InfoBase at <http://ithandbook.ffiec.gov/>
  - Examiner White papers at [www.ffiec.gov/exam/whitepapers.htm](http://www.ffiec.gov/exam/whitepapers.htm)
  - Examiner Education Information Database at [www.ffiec.gov/exam/educationalinfobases.htm](http://www.ffiec.gov/exam/educationalinfobases.htm)

### Federal Reserve Bank of Atlanta Retail Payments Risk Forum

- The Retail Payments Risk Forum is housed at the Federal Reserve Bank of Atlanta. The forum is designed to bring together expertise residing within the Federal Reserve, financial institutions, other industry participants, regulators, and law enforcement. The forum facilitates collaboration among these diverse parties, all of whom share common interests in improved detection and mitigation of emerging risks and fraud in retail payments systems. The forum accomplishes this by providing resources to research issues and sponsor dialogue. The forum's website address is [www.frbatlanta.org/rprf/](http://www.frbatlanta.org/rprf/) and *Portals & Rails Blog* is <http://portalsandrails.frbatlanta.org/>.

## Industry & Government Information-Sharing Resources Related to Payments Fraud

---

### Federal Reserve Banks (FRB)

- FRB New York makes information about frauds involving the use of a Federal Reserve Bank's name available on its website (see [www.newyorkfed.org Banking /Consumer Protection](http://www.newyorkfed.org/Banking/Consumer%20Protection)). Criminals may invoke the name of the Federal Reserve in an attempt to give legitimacy to otherwise fraudulent transactions, financial instruments, investment opportunities, and fund raising proposals. The *Frauds and Scams* web page provides information about these fraudulent activities and schemes. Individuals may sign up to receive e-mail alerts on new warnings or report a fraud using the site tool. *Fraud and Scams* URL is [www.newyorkfed.org/banking/frauds\\_scams.html](http://www.newyorkfed.org/banking/frauds_scams.html).
- Federal Reserve System Publications Catalog is searchable and includes consumer-oriented education on a variety of topics including payments fraud risk and prevention. The publication website address is [www.newyorkfed.org/publications/frame1.cfm](http://www.newyorkfed.org/publications/frame1.cfm).
- Federal Reserve Education website ([www.federalreserveeducation.org](http://www.federalreserveeducation.org)) provides links to instructional materials and tools such as online learning, videos, downloadable content and publications. Topics cover understanding the Federal Reserve, economics and financial education. Financial education materials include topics such as avoiding common frauds and scams, ID theft, and card fraud. Materials are free.
- FRB Minneapolis Payments Information and Outreach Office publishes research on payments-related fraud and mitigation practices of businesses and financial institutions <http://www.minneapolisfed.org/about/whatwedo/paymentsinformation.cfm>.

### Federal Reserve Board of Governors (BOG)

- Federal Reserve Board and Bank Supervision promulgate payment policies and regulations that govern payments, supervise and regulate banking system and financial markets. The BOG provides regulatory guidance, e.g., SR letters, FFIEC guidance and handbooks. Information and resources are available from the BOG at [www.federalreserve.gov](http://www.federalreserve.gov).
- The BOG also provides information for consumers through the *Federal Reserve Consumer Help* at [www.federalreserveconsumerhelp.gov](http://www.federalreserveconsumerhelp.gov). Information, alerts, brochures, and resources on banking related matters are available including materials related to fraud risks and schemes.

### Federal Trade Commission (FTC)

- The FTC is a federal government agency with both consumer protection and competition jurisdiction in broad sectors of the economy. The FTC provides educational programs for consumers and businesses. The FTC's main website address is <http://www.ftc.gov> and the *Identify Theft* website address is [www.ftc.gov/bcp/edu/microsites/idtheft/](http://www.ftc.gov/bcp/edu/microsites/idtheft/).
- FTC's **Consumer Sentinel** (<http://www.ftc.gov/sentinel/index.shtm>) is an investigative cyber tool that provides members of the Consumer Sentinel Network with access to millions of consumer complaints. It provides law enforcement members with access to complaints provided directly to the Federal Trade Commission by consumers, as well as providing members with access to complaints shared by data contributors.

### Financial Action Task Force (FATF)

- FATF is an inter-governmental body whose purpose is the development and promotion of policies, both at national and international levels, to combat money laundering and terrorist financing. The FATF identifies new threats and researches money laundering and terrorist financing methods. FATF Typologies reports describe and explain the nature of these methods and threats, to increase global awareness and allow for earlier detection. The website address is [www.fatf-gafi.org](http://www.fatf-gafi.org).

### Financial and Retailers Protection Association (FRPA)

- FRPA is not-for-profit organization dedicated to fighting financial and serious retail property crimes. It focuses on local concerns and looks for global property crime trends to prevent, identify and deter these types of crimes. The FRPA manages information from financial institutions and retailers regarding common investigations concerning financial frauds and serious organized property crimes. FRPA has developed theft-reporting databases for use by its members, while actively looking for crime patterns and trends within the local community and for regional trends. Website address is [www.fraudviewer.org](http://www.fraudviewer.org).
- FRPA also offer services for citizen victims and training for business groups, such as, Law Enforcement, Financial Institutions, Retailers, and Hotel/Motel Keepers.

### Financial Services Roundtable

- The Financial Services Roundtable is an executive forum for the leaders of the financial services industry [www.fsround.org](http://www.fsround.org). BITS and the Financial Services Technology Consortium (FSTC) merged and support work of the FS Roundtable including issues associated with payments fraud (see also BITS).

### FinCEN

- FinCEN's focus is on safeguarding the financial system from the abuses of financial crime, including terrorist financing, money laundering, and other illicit activity. FinCEN's website link is [www.fincen.gov](http://www.fincen.gov).
- *SAR Activity Review* and related publications can be found at [www.fincen.gov/news\\_room/](http://www.fincen.gov/news_room/).
- Advisories and bulletins are available at [www.fincen.gov/news\\_room/advisory/](http://www.fincen.gov/news_room/advisory/).

### FraudAvengers.org

- [www.FraudAvengers.org](http://www.FraudAvengers.org) is a resource to help the public understand, identify, and prevent consumer-related payments fraud. FraudAvengers.org consists of information from industry experts to educate and motivate individuals and small businesses to take actions that can reduce their personal risk of fraud. Site is sponsored by the Foundation for Payments Fraud Abatement & Activism.

### Fraud-Net

- Fraud-Net [www.fraudnet.com](http://www.fraudnet.com) is a resource for both banking security professionals and the law enforcement community. Fraud-Net provides users with a secure platform on which to post and read alerts about criminal activities affecting FIs. The information is available by geographic regions and further categorized by the type of activity. The system has access security, email alerts, alert and user search and the capability for attachments (photos, images, and documents).

### Independent Community Bankers of American (ICBA) (National and State)

- The ICBA provides payments fraud and risk mitigation information to FIs that include education events and materials, community bank surveys, and service provider information. The ICBA's website address is [www.icba.org](http://www.icba.org) and includes links to state association websites.
- Payments fraud risks and mitigation strategies are frequent topics at meetings and conferences. The ICBA also hosts education webinars and audio conferences on fraud risk topics. Fraud/phishing and spoofing resources for banks and identify theft resources for consumers are also available on the ICBA's website.

### Information Sharing and Analysis Centers Council (ISAC Council) & Groups

- ISAC council focus is to advance the physical and cyber security of the critical infrastructures of North America by establishing and maintaining a framework for valuable interaction between and among the ISACs and with government. ISAC council website address is [www.isaccouncil.org](http://www.isaccouncil.org). See also:
  - **Multi-State Information Sharing and Analysis Center (MS-ISAC)** at [www.msisac.org](http://www.msisac.org)
  - **Financial Services Information Sharing and Analysis Centers (FS-ISAC)** is an industry forum for collaboration on critical security threats facing the financial services sector, see [www.fsisac.com](http://www.fsisac.com).
  - **Payments Processor Information Sharing Council (PPISC)** a group formed in early 2010 under the umbrella of the FS-ISAC, provides a forum for sharing information about fraud, threats, vulnerabilities and risk mitigation in the payments industry, see [www.ppisc.com](http://www.ppisc.com)

### International Association of Financial Crimes Investigators (IAFCI)

- IAFCI is a non-profit international organization, it provides services and an environment within which information about financial fraud, fraud investigation and fraud prevention methods can be collected and exchanged. Contact information for regional chapters (30 in the U.S.) is available on the IAFCI website at [www.iafci.org](http://www.iafci.org). Local chapters meet on a periodic basis.

### Internet Crime Complaint Center (IC3)

- IC3 is a partnership between the FBI, National White Collar Crime Center and the Bureau of Justice Assistance. It serves as a vehicle to receive, develop, and refer criminal complaints regarding cyber crime. IC3 website address is [www.ic3.gov](http://www.ic3.gov).
- The IC3 provides:
  - Victims of cyber crime a reporting mechanism that alerts authorities of suspected criminal or civil violations.
  - A central referral mechanism for complaints involving Internet related crimes for law enforcement and regulatory agencies.

### Internet Scambusters

- Scambusters.org is a public service website provided by Lanford Inc. of North Carolina. The site ([www.scambusters.org](http://www.scambusters.org)) provides tips for consumers on how to avoid popular scams, viruses, spyware, phishing scams, identity theft ploys, credit card fraud schemes, and spam.

### Looks Too Good To Be True

- *Looks Too Good To Be True* is a consumer education source on Internet fraud prevention. The website is maintained by a joint federal law enforcement and industry task force and is funded by the U.S. Postal Inspection Service and the FBI. The website address is [www.lookstoogoodtobetrue.com](http://www.lookstoogoodtobetrue.com).

### Merchants Risk Council (MRC)

- MRC is a merchant-led trade association focused on electronic commerce risk and payments. MRC leads networking, education and advocacy programs focused on making electronic commerce more efficient, safe and profitable. MRC website address is [www.merchantriskcouncil.org](http://www.merchantriskcouncil.org).

### Microsoft

- Microsoft TechNet Security TechCenter URL- <http://technet.microsoft.com/en-us/security/default.aspx>.
- Malware Protection Center provides threat research and response information on its website at <http://www.microsoft.com/security/portal/>.

## Industry & Government Information-Sharing Resources Related to Payments Fraud

---

### **MyMoney.gov**

- The U.S. Financial Literacy and Education Commission sponsor the MyMoney.gov website ([www.MyMoney.gov](http://www.MyMoney.gov)). The site is dedicated to teaching the basics about financial education and includes information and links related to privacy, frauds and scams.

### **National Association of Federal Credit Unions (NAFCU)**

- NAFCU is a trade association for federal credit unions. It provides information, education and a forum to discuss issues, concerns and trends. NAFCU website address is [www.nafcunet.org](http://www.nafcunet.org).

### **National Automated Clearinghouse Association (NACHA) and Regional ACH Associations**

- NACHA and regional associations provide alerts, bulletins, training and conferences related to payments fraud. NACHA website address is [www.nacha.org](http://www.nacha.org).
- NACHA also has a Risk Management Advisory Group.

### **National Check Fraud Center**

- The National Check Fraud Center provides education information, alert reports and assistance in investigations related to check fraud. The center's website address is [www.ckfraud.org](http://www.ckfraud.org). The National Crime Alert Network, a division of the National Check Fraud Center, is a network of Local Law Enforcement, Federal Agencies, Financial and Retail communities who participates in a rapid response notification network, providing "real time" information and intelligence of criminal activity and crimes within a given area which may affect one's business. For information on the crime alert network see <http://www.ckfraud.org/network.html>.

### **National Consumer Leagues (NCL)**

- NCL website address is [www.nclnet.org](http://www.nclnet.org). **NCL Fraud Center** provides fraud prevention education for consumers ([www.fraud.org](http://www.fraud.org)).

### **National Credit Union Association (NCUA)**

- The NCUA hosts a Fraud Information Center on its website in an effort to help recognize, prevent, and report fraud (<http://www.ncua.gov/Resources/Cnsmrs/Fraud/Pages/default.aspx>). NCUA fraud alerts, letters to credit unions and other resources are available through the site.

### **The National Crime Prevention Council (NCPC)**

- The NCPC is a nonprofit organization. The NCPC collaborates with government and law enforcement to prevent crime and promotes crime prevention and personal safety basics. NCPC publishes books, kits of camera-ready program materials, posters, and informational and policy reports on a variety of crime prevention subjects. Publications include information on fraud and identity theft and Internet safety, e.g., *Identity Smart: A Guide for Consumers to Help Protect Against Identity Theft (February 2010)*. NCPC website address is [www.ncpc.org](http://www.ncpc.org). NCPC also hosts the **McGruff** website for children ([www.mcgruff.org](http://www.mcgruff.org)).

### **National Cyber Forensic Training Alliance Foundation (NCFTA)**

- NCFTA is a non-profit organization that brings together local, state, and federal/international law enforcement and INTEL entities, private sector companies, and academic institutions to functionally collaborate and develop intelligence on cyber crime threats and methods. NCFTA's website address is [www.ncfta.net](http://www.ncfta.net).

### National Cyber Security Alliance (NCSA)

- NCSA's mission is to educate and empower a digital society to use the Internet safely and securely at home, work, and school, protecting the technology individuals' use, the networks they connect to, and our shared digital assets. NCSA hosts the Stay Safe Online website ([www.staysafeonline.org](http://www.staysafeonline.org)). The site provides best practice information for students, consumers and businesses.

### Office of the Comptroller of the Currency (OCC)

- The OCC charters, regulates, and supervises national banks. It also supervises the federal branches and agencies of foreign banks. The OCC website is [www.occ.treas.gov](http://www.occ.treas.gov).
- The OCC provides Anti-Fraud Resources for national banks and consumers. The website address for fraud resources is [www.occ.treas.gov/fraudresources.htm](http://www.occ.treas.gov/fraudresources.htm). Banking resources include information regarding counterfeit currency, counterfeit instruments, spoofed bank websites, and links to OCC bulletins related to fraud schemes. Consumer resources include information and descriptions of fraud schemes, suspicious checks, sources for verifying authenticity, anti-phishing and other related information.
- OCC distributes alerts regarding suspicious activity via email subscription. Listings of alerts are available by year at <http://www.occ.gov/news-issuances/alerts/2012/index-2012-alerts.html>.

### OnGuardOnline.gov

- OnGuardOnline.gov is the federal government's website geared to help consumers be safe, secure and responsible online. The site offers information on how to avoid scams, securing your computer, being safe online and protecting kids online. Free publications can also be ordered through this website.
- The Federal Trade Commission manages OnGuardOnline.gov ([www.onguardonline.gov](http://www.onguardonline.gov)), in partnership with 15 other federal agencies. OnGuardOnline.gov is a partner in the Stop Think Connect campaign, led by the Department of Homeland Security, and part of the National Initiative for Cybersecurity Education, led by the National Institute of Standards and Technology.

### Open Security Foundation

- A non-profit organization dedicated to tracking and reporting security vulnerabilities and breaches of personal information. Website sponsored by CREDANT Technologies at [www.datalossdb.org](http://www.datalossdb.org).

### Protect Your Business

- Provides information on protecting businesses from business identity theft—the crime of hijacking a business's identity and using that identity to establish lines of credit with banks or retailers. The Colorado Secretary of State sponsors their website (<http://www.ProtectYourBusiness.us>). Resources include *A Guide to Protecting Your Business and Recovering from Business Identity Theft* published in July 2010.

### SANS (SysAdmin, Audit, Network, Security) Institute

- The SANS Institute was established as a cooperative research and education organization. SANS website address is [www.SANS.org](http://www.SANS.org). Resources include research papers, podcasts, webcasts, alerts, and newsletters such as *ExecuBytes* newsletter, weekly *NewsBites* and weekly vulnerability news *@RISK*. Newsletters are available at [www.sans.org/newsletters/newsbites/](http://www.sans.org/newsletters/newsbites/).
- SANS hosts the **Internet Storm Center (ISC)**, which gathers intrusion detection data on a daily basis, identifies security issues and sites that are used in attacks, and provides data on the types of attacks that are being mounted against computers in various industries and regions around the globe. The ISC is a free service to the Internet community. The ISC makes information available through its website (<http://isc.sans.org/>), RSS feeds/alerts, daily podcasts and other methods.

### State Banking Associations

- Check with your local associations regarding fraud alerts, distribution and information sharing opportunities.

### Stop Think Connect

- **Stop. Think. Connect.**<sup>™</sup> is a coordinated message created by a coalition of private companies, nonprofits and government organizations to help all digital citizens stay safer and more secure online. The APWG and NCSA led the effort to find a unified online safety message that could be adopted across public and private sectors. The website ([www.stopthinkconnect.org](http://www.stopthinkconnect.org)) provides access to their research and education videos.

### Symantec

- Symantec.cloud is a managed service provider for electronic communications security. Symantec also provides free information on security issues related to electronic communications including monthly and annual Intelligence reports and analysis, which are available at [www.symanteccloud.com](http://www.symanteccloud.com) (see *Global Threats*). Reports describe online threat activities trends, statistics, and technical information on methods used related to threats such as viruses, spam, spyware and phishing attacks.

### Twin Cities Security Partnership (TCSP)

- TCSP is a public/private partnership dedicated to enhancing security, safety, and the quality of life in the greater Twin Cities area, i.e., greater Minneapolis/St. Paul area. The TCSP meets and collaborates on a regular basis. The TCSP website address is [www.securitypartnership.org](http://www.securitypartnership.org).
- TCSP is comprised of high-ranking and top-level business, law enforcement, community, and government leaders. The FBI is the “lead organization” for the TCSP, but the TCSP is not an official program of the FBI. When TCSP responds to a crisis, the law enforcement agency is normally in charge.

### U.S. Department of Homeland Security

- **U. S. Computer Emergency Readiness Team (US-CERT)** coordinates defense against and responses to cyber attacks across the nation. US-CERT’s website provides information and access to the National Cyber Alert System, vulnerability resources, alerts and tips, security publications, and a reporting tool. The website address is [www.us-cert.gov](http://www.us-cert.gov).
- **National Institute of Standards and Technology**
  - Computer Security Division Resource Center website address is [www.csrc.nist.gov](http://www.csrc.nist.gov).
  - National Vulnerabilities database website address is <http://nvd.nist.gov/home.cfm>.

### U.S. Department of Justice - Federal Bureau of Investigation (FBI)

- The FBI is the principal investigative arm of the United States Department of Justice. It has the authority and responsibility to investigate specific crimes assigned to it. FBI’s website address is [www.fbi.gov](http://www.fbi.gov).
- **Cyber Initiative Resource Fusion Unit (CIRFU)** combines resources and the expertise of law enforcement and the private sector that range from federal agencies, software companies, and Internet Service Providers, to merchants and members of the financial sector. Industry experts from companies, the FBI, postal inspectors, the Federal Trade Commission, and many others are brought together to share information and ideas focused on cyber threats and security breaches.
- Cyber Investigations website address is [www.fbi.gov/cyberinvest/cyberhome.htm](http://www.fbi.gov/cyberinvest/cyberhome.htm).

### U.S. Department of the Treasury - Bureau of the Public Debt

- The Bureau of the Public Debt and the U.S. Treasury are aware of several fraudulent schemes or scams that involve what are claimed to be securities issued or backed by the Treasury Department or another part of the United States Government. These scams have been directed at banks, charities, companies, and even individuals, by individuals or organizations seeking payment on the fraudulent securities. Information about these scams is available on the Frauds, Phonies, & Scams web page <http://www.treasurydirect.gov/instit/statreg/fraud/fraud.htm>.

### U.S. Department of the Treasury - Office of Critical Infrastructure Protection (CIP) and Compliance Policy

- CIP coordinates the Department's development and implementation of policies regarding protection of the critical infrastructure of the financial services sector, including money laundering, terrorist financing, and identity theft and the sharing of information among FIs and between the private and public sectors, and the sharing of suspicious information pursuant to the Bank Secrecy Act. Information about CIP can be found on [www.treasury.gov](http://www.treasury.gov) under the *About - Organization Structure* and in the *Resource Center* pages.

### U.S. Department of the Treasury - Office of Terrorism and Financial Intelligence (TFI)

- The Office of Terrorism and Financial Intelligence (TFI) marshals the department's intelligence and enforcement functions with the twin aims of safeguarding the financial system against illicit use and combating rogue nations, terrorist facilitators, money launderers, drug kingpins, and other national security threats. Information about TFI can be found on [www.treasury.gov](http://www.treasury.gov) under the *About - Organization Structure* and in the *Resource Center* pages.

### U.S. Postal Inspection Service (USPIS)

- USPIS is the law enforcement agency for the US postal service. USPIS website address is <https://postalinspectors.uspis.gov/>. In addition to investigation and enforcement, the USPIS provides alerts, education materials and videos, and posts information on its website about mail fraud schemes. Fraud schemes URL is <https://postalinspectors.uspis.gov/investigations/MailFraud/fraudschemes/FraudSchemes.aspx>.

### U.S. Secret Service (USSS)

- U.S. Secret Service website address is [www.secretservice.gov](http://www.secretservice.gov).
- The U.S. Secret Service Extranet, entitled eInformation Network, provides an information-sharing platform for the Secret Service and its business partners. E-Information network website address is [www.einformation.uss.gov](http://www.einformation.uss.gov). The eInformation provides links to *eLibrary*, *USDollars*, and *Electronic Crimes Task Force*. The eLibrary is a secure website for law enforcement and qualified financial crime investigators. The library provides a collection of resource databases for sharing information on a variety of topics. The USDollars is a secure website for qualified financial institutions and law enforcement members to search the Secret Service counterfeit note database.

### **U.S. Secret Service National Network of Electronic Crimes Task Force (ECTF)**

- U.S. Secret Service **National Network of Electronic Crimes Task Force (ECTF)** brings together federal, state and local law enforcement, prosecutors, private industry and academia. There are over 20 regional groups. Contact information for regional groups is available from the national site ([www.ectf.uss.gov](http://www.ectf.uss.gov)). The regional groups focus on sharing information and fighting crimes. Groups typically meet on a quarterly basis. Areas of electronic crime fraud within ECTF purview includes, but are not limited to, computer generated counterfeit currency, bank fraud, counterfeit checks, credit card fraud, virus and worm proliferation, access device fraud, telecommunications fraud, internet threats, computer system intrusions and cyber-attacks, phishing/spoofing, terrorism/terrorist financing nexus, and identity theft.

### **Verizon**

- Verizon's resource center provides white papers by industry focusing on information security, e.g., *2011 Data Breach Investigations Report*. White papers can be access through the *Resource Center*. Verizon's business focused website is [www.verizonbusiness.com](http://www.verizonbusiness.com).