Industry & Government Information-Sharing Resources Related to Payments Fraud
Updated April 2018

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.

AARP Fraud Watch Network

- AARP hosts the Fraud Watch Network which provides scam alerts, prevention tips, resources and other anti-fraud information. Sign up is free to all at: https://action.aarp.org/site/SPageNavigator/FWN_Registration_Page.html.

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.

American Bankers Association (ABA)

- ABA provides a variety of information pertaining to payments fraud and mitigation. The ABA website address is www.aba.com.
- The ABA's Center for Payments and Cybersecurity (http://www.aba.com/Tools/Function/Pages/center-payments-cybersecurity.aspx) offers resources to help banks mitigate fraud. The ABA's peer group benchmarking program includes groups that focus on payments fraud. ABA publishes an *ABA Deposit Account Fraud Survey Report* that discusses fraud trends and prevention methods.

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 website is www.antiphishing.org**.** The site provides news, white papers, best practice information, 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 and 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 and seminars and offers online learning tools.

- The 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)

- AFP is an association for treasury and finance professionals. 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 website address is 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 and the U.S. region URL is www.atmia.com/regions/united-states.

Bank Administration Institute (BAI)

- BAI is an education and research organization serving the financial services industry. The BAI website address is www.bai.org.

BankInfoSecurity.com

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

Better Business Bureau (BBB)

- BBB provides resources for consumers and businesses. The BBB website address is www.bbb.org.
- The BBB's *News and Events* tab provides *Scam Alerts* and *Warnings*, which provide information related to recent frauds and other marketplace issues. The URL for BBB News is www.bbb.org/council/news-events/.

Bitpipe.com

- Bitpipe.com 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 cybersecurity and threats. The site also provides RSS feeds. The website address is www.Bitpipe.com.

Business Payments Coalition

- The Business Payments Coalition is a volunteer group of organizations and individuals working together to promote greater adoption of electronic business-to-business (B2B) payments and remittance data. The Coalition's overarching goal is to make B2B payments more efficient across the end-to-end process. The website address is https://fedpaymentsimprovement.org/payments-efficiency/business-payments-coalition/

- The Small Business Payments Toolkit offers plain-language, practical education about various payment types, explains the benefits of electronic payments and describes how small businesses can avoid being victimized by payment fraud. The toolkit also contains an extensive resource section with links to additional information. The toolkit is available here https://fedpaymentsimprovement.org/payments-efficiency/business-payments-coalition/small-business-payments/.

Canadian Anti-Fraud Centre (CAFC)

- The 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 CAFC website address is www.antifraudcentre-centreantifraude.ca.

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, MasterCard www.mastercard.com, PULSE www.pulsenetwork.com, SHAZAM Network www.shazam.net, etc.).
    - All of the above websites include information on fraud management and mitigation.

Carnegie Mellon University

- Carnegie Mellon's Software Engineering Institute (SEI) has a digital library (http://resources.sei.cmu.edu/library/) with thousands of documents related to software engineering, including information on fraud and risk, such as the *Common Sense Guide to Mitigating Insider Threats.*
- SEI also has a CERT Division dedicated to studying and solving cybersecurity problems. The CERT Division collaborates with government organizations, such as the U.S. Department of Defense and the Department of Homeland Security, as well as various industry stakeholders to measurably improve the security of the cyber environment. See https://www.sei.cmu.edu/about/divisions/cert/index.cfm for more information.

Consumer Financial Protection Bureau (CFPB)

- The Consumer Financial Protection Bureau was established by Congress to protect consumers by carrying out federal consumer financial laws. The CFPB 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 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.

CyberSource

- CyberSource, a merchant services provider, publishes an annual *Online Fraud Report* and provides information about fraud prevention tools. The CyberSource website address is www.cybersource.com.

Federal Deposit Insurance Corporation (FDIC)

- The FDIC website (www.fdic.gov) provides Financial Institution Letters (FILs), examiner information, news and other information, some of which pertains to payments fraud and risks.
- The *FDIC Quick Links for Consumers and Communities* (www.fdic.gov/quicklinks/consumers.html) contains information for financial service organizations and consumers regarding fraud schemes and lists links to FDIC consumer alerts, identity theft information, financial education, and other resources.

Federal Financial Institutions Examination Council (FFIEC)

- The FFIEC is an interagency body with website address 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.

Federal Reserve Banks (FRB)

- A U.S. payments system that is safe, efficient, and broadly accessible is vital to the U.S. economy, and the Federal Reserve plays an important role in promoting these qualities as a leader, catalyst for change, and provider of payment services to financial institutions and the U.S. Treasury. The Fed Payments Improvement Initiative provides a forum for stakeholders to advise the Federal Reserve on payment security matters, and identify and promote actions that can be taken by payment system participants collectively or by the Federal Reserve System. See www.fedpaymentsimprovement.org for more information.
    - The Secure Payments Task Force was concluded, however, their *Information Sharing Data Sources*, *Payment Life Cycles and Security Profiles*, and other information are available at this link https://securepaymentstaskforce.org/.
- FRB Minneapolis' Payments, Standards, and Outreach Group publishes research on payments-related fraud and mitigation practices of businesses and financial institutions, information on payments fraud liability, and this resource list. See https://www.minneapolisfed.org/about/what-we-do/payments-information for more information.
- The Retail Payments Risk Forum, housed at FRB Atlanta, 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/ and *Take On Payments* blog is http://takeonpayments.frbatlanta.org/.
- The Federal Reserve Education website (www.federalreserveeducation.org) provides links to free 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.

- FRB Boston Payment Strategies contributes to the development of innovative technology solutions for mobile and digital payments through analysis, primary and secondary research, examining risks and benefits, any convening, and education to influence adoption. See https://www.bostonfed.org/payment-studies-and-strategies.aspx for more information.
- FRB Boston's Consumer Payments Research Center conducts surveys, and econometric and theoretical research on consumer payments, including publications and data on fraud and security. See https://www.bostonfed.org/about-the-boston-fed/business-areas/consumer-payments-research-center.aspx for more information.
- The Fed in Print website (https://fedinprint.org/) catalogs all publications of the Federal Reserve System. Librarians throughout the System contribute to content and add publications as they become available in full-text.
- FRB Philadelphia's Payment Cards Center provides insight into developments in consumer credit and payments that are of interest to the Federal Reserve, businesses, academia, policymakers, and the general public. Publications include discussion papers, conference summaries and working papers and can be accessed at https://www.philadelphiafed.org/consumer-credit-and-payments/payment-cards-center/publications.
- The Federal Reserve Bank Services web site (https://www.frbservices.org/resources/resource-centers/index.html) provides a wide variety of services and information, including the Risk Management Toolbox and other resource centers. Additionally, FRB Services provides access to the Federal Reserve Payments studies, which contain information on the value and volume of payments and payments fraud and can be found at https://www.frbservices.org/news/research.html.
- FRB New York hosts the *Frauds and Scams* web page (www.newyorkfed.org/banking/frauds_scams.html) which provides information on various fraudulent activities and schemes. Individuals may signup to receive e-mail alerts on new warnings or report a fraud using the site tool. Additionally, information on fraud involving the use of the Federal Reserve's name in an attempt to give legitimacy to otherwise fraudulent transactions, financial instruments, investment opportunities, or fund raising proposals, is available at https://www.newyorkfed.org/banking/frscams.html.

Federal Reserve Board of Governors (BOG)

- Federal Reserve Board of Governors and Bank Supervision promulgate payment policies and regulations that govern payments and supervise and regulate the 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.
- The BOG also provides information for consumers through the *Federal Reserve Consumer Help* at 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 www.ftc.gov. Under *Tips and Advice* the FTC has information for consumers including scam alerts (https://www.consumer.ftc.gov/scam-alerts).
- The FTC hosts the https://www.identitytheft.gov/ website, which is a resource for identity theft victims. The site provides information and checklists on steps consumers can take if they are an ID theft victim.
- The 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.
- OnGuardOnline (www.onguardonline.gov) is geared to help consumers be safe, secure, and responsible online. The site offers information on avoiding scams, securing your computer, being safe online, and protecting kids online. Free publications can also be ordered through their website.

Financial Action Task Force (FATF)

- The 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 and researches new threats and produces FATF Typologies reports to describe and explain the methods and nature of these threats, to increase global awareness, and allow for earlier detection. The FATF website address is http://www.fatf-gafi.org/.

Financial and Retailers Protection Association (FRPA)

- FRPA is a 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. FRPA manages information from financial institutions and retailers regarding common investigations concerning financial frauds and serious organized property crimes. FRPA has also developed theft-reporting databases for use by its members, while actively looking for local and regional crime patterns and trends. The FRPA website address is www.frpafraudviewer.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 (FSR)

- The Financial Services Roundtable is an executive forum for the leaders of the financial services industry. The FSR website is www.fsroundtable.org.
- The FSR technology policy division, 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.fsroundtable.org/category/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. The FinCEN website address is www.fincen.gov.
- Advisories, bulletins, *SAR Stats* and related publications can be found at www.fincen.gov/news-room/.

Fraud-Net

- Fraud-Net (www.fraud-net.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 financial institutions. Fraud-Net is available in some states.

Identity Theft Resource Center (ITRC)

- The ITRC is a non-profit organization established to support victims of identity theft in resolving their cases, and to broaden public education and awareness in the understanding of identity theft, data breaches, cybersecurity, scams/fraud, and privacy issues. The ITRC website address is www.idtheftcenter.org.

Independent Community Bankers of America (ICBA)

- ICBA provides payments fraud and risk mitigation information to financial institutions including education events and materials, community bank surveys and service provider information. The ICBA website address is www.icba.org and includes links to state association websites.
- Payments fraud risks and mitigation strategies are frequent topics at meetings and conferences. ICBA also hosts education webinars and audio conferences on fraud risk topics.

National Council of Information Sharing and Analysis Centers (ISACs) & Sector ISACs

- The focus of the National Council of ISACs is to advance the physical and cybersecurity of the critical infrastructures of North America by establishing and maintaining a framework for valuable interaction between and among the ISACs and with government. The National Council of ISACs website is www.nationalisacs.org. See also:
  - **Multi-State Information Sharing and Analysis Center (MS-ISAC)** at 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 for more information.
  - **Retail Cyber Intelligence Sharing Center (R-CISC)** is a cybersecurity resource for retailers, consumer products/goods/services, and cybersecurity industry partners worldwide. The R-CISC provides community-driven threat intelligence, industry-specific research and development, and ongoing, peer-driven and professional education and training opportunities. See https://r-cisc.org/ for more information.

International Association of Financial Crimes Investigators (IAFCI)

- IAFCI is a non-profit international organization that 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 (32 in the U.S.) is available on the IAFCI website at www.iafci.org. Local chapters meet on a periodic basis.

Internet Crime Complaint Center (IC3)

- The 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 cybercrime. The IC3 website address is www.ic3.gov.
- The IC3 provides:
  - Victims of cybercrime a reporting mechanism that alerts authorities of suspected criminal or civil violations. Report can come from actual victim or from a third party to the complaint.
  - A central referral mechanism for complaints involving Internet related crimes for law enforcement and regulatory agencies.

International Organization for Standardization (ISO)

- ISO is an independent, non-governmental membership organization and is the developer of voluntary International Standards. The ISO Technical Committee 68, Subcommittee 2 (ISO/TC68/SC2) develops financial standards related to security. The ISO website address is www.iso.org.

Merchants Risk Council (MRC)

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

Microsoft

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

MyMoney.gov

- The U.S. Financial Literacy and Education Commission sponsor the MyMoney.gov website (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. The NAFCU website address is www.nafcu.org.

National Automated Clearinghouse Association (NACHA) and Regional ACH Associations

- NACHA and regional associations provide alerts, bulletins, training, and conferences related to payments fraud. The NACHA website address is www.nacha.org.
- NACHA also has a Risk Management Advisory Group.

National Consumer Leagues (NCL)

- The NCL website address is www.nclnet.org.
- Fraud.org (previously the Fraud Center) provides fraud prevention education for consumers (www.fraud.org).

National Credit Union Administration (NCUA)

- NCUA hosts a Fraud Information Center on its website in an effort to help recognize, prevent, and report fraud. NCUA fraud alerts, letters to credit unions, and other resources are available through the site at www.ncua.gov.
- NCUA also hosts the mycreditunion.gov website which contains a Fraud Prevention Center that provides information on fraud scams, identity theft, and online security, as well as fraud alerts resources. More information can be found at http://www.mycreditunion.gov/fraud/Pages/default.aspx.

National Crime Prevention Council (NCPC)

- NCPC is a nonprofit organization that collaborates with government and law enforcement to prevent crime and promote 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, identity theft, and Internet safety. The NCPC website address is www.ncpc.org.
- NCPC also hosts the McGruff website for children (www.mcgruff.org).

National Cyber Forensic Training Alliance Foundation (NCFTA)

- The 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 cybercrime threats and methods. NCFTA's website address is 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) which provides best practice information for students, consumers, and businesses.

National Institute of Standards and Technology (NIST)

- NIST is a non-regulatory federal agency within the U.S. Department of Commerce. Their mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. More information can be found at www.nist.gov.
- In support of the executive order, *Improving Critical Infrastructure Cybersecurity* issued in February 2013, NIST has worked with stakeholders to develop a voluntary framework (based on existing standards, guidelines, and practices) for reducing cyber risks to critical infrastructure. See http://www.nist.gov/cyberframework/index.cfm for more information.
- NIST produces *Federal Information Processing Standards Publication (FIPS)* which are standards and guidelines used government-wide. See https://www.nist.gov/itl/itl-publications/federal-information-processing-standards-fips for more information.
- NIST's Computer Security Resource Center website address is https://csrc.nist.gov/.
- The National Vulnerabilities Database website address is http://nvd.nist.gov/home.cfm.

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.
- The OCC provides Anti-Fraud Resources for national banks and consumers. Banking resources include information regarding counterfeit currency, counterfeit instruments, spoofed bank websites, and links to OCC bulletins and alerts related to fraud schemes (http://www.occ.gov/news-issuances/index-news-issuances.html). The OCC distributes alerts regarding suspicious activity via email subscription.
- Consumer resources include information and descriptions of fraud schemes, suspicious checks, sources for verifying authenticity, anti-phishing and other related information. See http://www.occ.gov/topics/consumer-protection/fraud-resources/index-fraud-resources.html for more information.

PCI Security Standards Council

- The PCI Security Standards Council is responsible for the development, management, education, and awareness of the PCI Security Standards. The website www.pcisecuritystandards.org/ provides more information and access to the standards.

Protect Your Business

- 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 this website (http://www.ProtectYourBusiness.us). Resources include A *Guide to Protecting Your Business and Recovering from Business Identity Theft* published in January 2012.

SANS (SysAdmin, Audit, Network, Security) Institute

- The SANS Institute (www.SANS.org) was established as a cooperative research and education organization. Resources include research papers, podcasts, webcasts, alerts and newsletters such as *OUCH!* monthly newsletter for computer users, semiweekly *NewsBites* containing summary information for the week and weekly *@RISK newsletter* on new attack information and vulnerability news. Newsletters are available at http://www.sans.org/newsletters/.
- 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/), such as RSS feeds/alerts, daily podcasts, and other methods.

Secure Technology Alliance

- The Secure Technology Alliance (formerly the Smart Card Alliance) is a digital security industry association. The Alliance exists as a neutral forum that brings together leading providers and adopters of end-to-end security solutions designed to protect privacy and digital assets in a variety of vertical markets. The Secure Technology Alliance's website is www.securetechalliance.org.
- The Alliance hosts EMV Connection (www.emv-connection.com) a website to provide education and assist all industry stakeholders with EMV migration.
- The Alliance hosts the U.S. Payments Forum. The forum is a cross-industry body focused on addressing issues that require broad cooperation and coordination across many constituents in the payments industry. This cooperation and coordination is vital to promote the efficient, timely, and effective

introduction of EMV chip technology and other new and emerging payments technologies in the United States that protect the security of, and enhance opportunities for payment transactions within the U.S. Topic areas the Forum engages in include EMV implementation, tokenization, card-not-present transactions, encryption, and mobile and contactless payments. The U.S. Payments Forum's website is http://www.uspaymentsforum.org/.

State Banking Associations

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

Stop. Think. Connect.

- Stop. Think. Connect. 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) provides access to their research and education videos.

Symantec

- Symantec is a managed service provider for electronic communications security. The website to the security center is https://www.symantec.com/security-center.
- Symantec also provides free information on security issues related to electronic communications including monthly and annual Intelligence reports and whitepapers, which are available at https://www.symantec.com/security_response/publications/monthlythreatreport.jsp. 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)

- The 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.
- The 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 the TCSP responds to a crisis, the local 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.

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.

- Cyber Initiative Resource Fusion Unit (CIRFU) brings together resources and expertise of law enforcement and the private sector, as well as industry experts from companies, the FBI, postal inspectors, the Federal Trade Commission, and many others to share information and ideas focused on cyber threats and security breaches.
- The Cyber Investigations website address is https://www.fbi.gov/investigate/cyber.
- Safe Online Surfing (SOS) is a website providing education for teachers and students. The site features six grade-specific "islands"— third- through eighth-grade — highlighting various aspects of cybersecurity through games, videos, and other interactive features. The site can be accessed at https://sos.fbi.gov/.
- InfraGard is a partnership between the FBI and the private sector dedicated to sharing information and intelligence to prevent hostile acts against the U.S. InfraGard has over 80 regional chapters. More information can be found at https://www.infragard.org/.

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 (OCIP) and Compliance Policy

- The Office of Critical Infrastructure Protection and Compliance Policy coordinates the Department's efforts to enhance the security and resilience of financial services sector critical infrastructure and reduce operational risk. The office works closely with financial sector companies, industry groups, and government partners to share information about cybersecurity and physical threats and vulnerabilities, encourage the use of baseline protections and best practices, and respond to and recover from significant incidents. Contact information can be found at https://www.treasury.gov/about/organizational-structure/offices/Pages/--Office-of-Critical-Infrastructure-Protection-and-Compliance-Policy.aspx.

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

- The 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. More information about the TFI can be found at https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Terrorism-and-Financial-Intelligence.aspx.

U.S. Postal Inspection Service (USPIS)

- The USPIS is the law enforcement agency for the U.S. postal service. The 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. The fraud schemes URL is https://postalinspectors.uspis.gov/investigations/MailFraud/fraudschemes/FraudSchemes.aspx.

U.S. Secret Service (USSS)

- The U.S. Secret Service website address is 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. The eInformation Network website address is www.einformation.usss.gov. The eInformation Network provides links to *eLibrary* and *USDollars*. 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 Network of Electronic Crimes Task Force (ECTF) and Financial Crimes Task Force (FCTF)

- U.S. Secret Service network of ECTFs and FCTFs brings together federal, state and local law enforcement, prosecutors, private industry and academia for information sharing and crime fighting. Regional groups that typically meet on a quarterly basis and can be found at https://www.secretservice.gov/investigation/. Areas of electronic crime fraud within ECTF purview include, 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., *Data Breach Investigations Report.* White papers can be accessed through Verizon's business focused website (www.verizonbusiness.com).