

GLOSSARY

Active - X Control: A software component capable of independent data manipulation through a structured set of commands.

ADSL: Asymmetric Digital Subscriber Line - A protocol used to deliver high bandwidth communications over conventional copper wire telephone networks.

Artificial Intelligence – Artificial Intelligence is defined as the a field of endeavor where computers and software programs are designed to mimic human reasoning and learning processes through the discovery of heuristics (rules) and algorithms that are then used to characterize an uncertain environment.

Bandwidth: The amount of data that can be sent through a given communications circuit per second.

Biometric Identification Devices – Biometric Identification Devices are hardware and software systems which authenticate the identities of human beings through the capture of unique data characterizing physical features of the human body. Examples include images of a person's finger or palm print, a laser-scan of an individual's retina, and a voiceprint.

Caribbean Financial Action Task Force (CFATF) - 23 Member States: The CFATF is the Caribbean affiliate of the FATF. It was established in November 1992 and has adopted the FATF 40 Recommendations \and an additional 19 regional recommendations. The CFATF conducts mutual evaluations and typologies exercises similar to those of the FATF. The CFATF continues to be the region's key regional anti-money laundering body. In recognition of its increased scope and pace of activities the EU and the U.S. have made the CFATF the implementing body for a comprehensive five-year training and technical assistance program.

Credit Cards -- Payment instruments that allow a user to pay for goods through funds credited to him/her by a credit card issuing company.

Cryptography -- The science and technology of keeping information secret from unauthorized parties by using a mathematical code or a cipher.

Cyberpayments – Cyberpayments are payments instruments utilizing advanced computing and network communications techniques to transfer monetary value between businesses, consumers, and financial service providers. Examples of Cyberpayment instruments include stored value-type smart cards, Internet-based E-cash systems, and hybrid payment systems with both network and smart card features.

Debit Cards -- Payment instruments which, when used to pay for an item or gain access to cash, debit a funds-holding account at a financial institution up to the users available balance.

Denomination Limits -- The upper limit beyond which value can no longer be added to a Cyberpayment instrument - typically discussed in the context of Smart Cards.

Digital Links – See Digital Signatures below.

Digital Signatures – A Digital Signature is a label attached to email, data, or electronic value within a network that authenticates the identities of particular individuals or entities.

Disintermediation -- The potential of Cyberpayments systems to allow “non-intermediated” transfers of value to take place without the involvement of an identifiable third party subject to legal and regulatory oversight.

The Egmont Group -- The Egmont Group is an international organization formed in June 1995 by 24 countries and 8 international organizations. It is comprised of Financial Intelligence Units (see below) and focuses on coordinating member states efforts at combating international money laundering.

Financial Action Task Force (FATF) -- The FATF, an inter-governmental body, is recognized as the leading organization that addresses the global problem of money laundering. Formed by the G-7 Economic Summit in 1989, the FATF is comprised of 26 jurisdictions, and two international organizations, representing the world’s major financial centers. It is dedicated to promoting the development of effective anti-money laundering controls and facilitates enhanced international cooperation among its members and around the world.

Financial Intelligence Unit (FIU) -- FIUs have been established in various countries around the world to detect criminal abuse of the financial system, ensure adherence to laws against financial crime and protect the banking community. FinCEN is a model of an FIU and others exist in such countries as Great Britain, France, Belgium, the Netherlands, Argentina, and Australia.

FinCEN (Financial Crimes Enforcement Network) -- An agency of the U.S. Treasury Department established in 1990 by Treasury Order 105-08. FinCEN is a financial intelligence unit (FIU) which supports financial investigations, develops and administers anti-money laundering regulations, and promotes international coordination and cooperation to fight money laundering.

Global Information Infrastructure (GII) -- The term used to describe the convergence of local and wide area information networks fostered by the emergence of open standards in networks. Within the GII, common protocols allowing geographically separated dissimilar computer networks to interact with one another and exchange information (text, pictures, audio, or video) in a digital form. The redundant nature of the GII permits communications between networks to be routed around malfunctioning systems.

Integration -- The final phase of the three generic phases of money laundering where a criminal, having successfully concealed the origin of illicit proceeds, desires to use the money for legitimate financial purposes such as business or real estate purchases. To facilitate such transactions, the laundered funds may be integrated with money from legitimate commercial activities. The illicit funds thus take on the appearance of legitimacy.

Intelligent Software Agents -- Software programs designed to accomplish tasks independent of user intervention. In a network environment such programs may seek out patterns in network traffic or in network usage by identifiable actors and aggregate this information into a structured presentation suitable for law enforcement use.

Interpol – The International Criminal Police Organization (Interpol) was founded to promote the widest possible mutual assistance among all law enforcement authorities, within the limits of the laws of member states. Interpol has 176 member states and a headquarters linked together by a secure encrypted network.

Internet Banking – The delivery of traditional banking services cover the Internet. Internet banking provides basic financial services such as funds transfers, bill paying and purchases of financial instruments to customers through an online connection.

Internet Gambling – The delivery of gaming opportunities through the Internet. These activities involve the playing of games of chance through a site of the world wide web, as well as the delivery of bookmaking services to gamblers connected through an online service.

ISDN: Integrated Services Digital Network - A hardware and software system for the delivery of high bandwidth data communications over fiber optic networks.

Key Escrow -- Key Escrow encryption plans envision the use of a trusted agent or third party (governmental or non-governmental in nature) which would store an extra copy of a private key used in a Public-key encryption implementation. Under legal and administrative guidelines such a key would be made available to authorized agencies (e.g., Law Enforcement Agencies) for investigative purposes. With access to private keys, authorized agencies would be able to decrypt cyphertext (the encrypted information) containing potentially valuable data.

Key Recovery -- Key Recovery encryption plans envision the filing - by creators of encryption products - of plans for the recovery of private keys used in implementations of Public Key encryption. Such recovery plans would be deposited with the Department of Justice, and would allow - under court order - Law Enforcement and other authorized government agencies to gain access to procedures and techniques which would allow the recovery of a Private Key used in a Public Key encryption system. This proposal originated after widespread criticism of earlier Key Escrow proposals. Specific implementations of Key Recovery have yet to be offered.

Layering -- The second phase of the three generic phases of money laundering where the criminal obscures the trail left by illicit proceeds (*aka* “dirty money”). The objective of this phase is to carry out a series of financial transactions in order to build layers between the funds and their illicit source. For example, a series of bank-to-bank wire transfers would constitute layering. Activities of this nature, especially when they involve funds transfers between tax haven and bank secrecy jurisdictions, make it very difficult for investigators to follow the trail of money.

Letters Rogatory – A request by one court of another court in an independent jurisdiction, that a witness be examined upon interrogatories sent with the request.

Money Laundering -- The process of transforming the proceeds of illegal activities into legitimate wealth. Another definition often cited is “the process by which one conceals the existence, legal source, or illegal application of income, and then disguises that income to make it appear legitimate.”

Mutual Legal Assistance Treaty – A binding agreement between two countries to cooperate on a request for information in criminal investigations. Such information would include bank account information or information that would be provided in the deposition of a witness in a criminal prosecution.

Network-borne Tracking Device – A Network-borne Tracking Device is a software or hardware system designed to trace data as it transits a packet-switched network. Systems in this category include network analyzers used by systems administrators to oversee local area networks, and “sniffers” designed to detect the origins of packets within a network.

Offshore: Foreign or overseas jurisdictions.

Organization of American States/Inter-American Drug Abuse Control Commission (OAS/CICAD) - 29 Members: CICAD is the specialized OAS body dealing with drugs and money laundering control which was established in 1986. CICAD reconvened its Experts Group on Money Laundering in 1996 to deal with the issue of implementation of the Summit of Americas Communiqué Plan of Action against money laundering. OAS progress on money laundering has increased significantly in the Experts Group which is also revising the 1992 OAS model regulations and is developing a comprehensive anti-money laundering training and technical assistance program for regulators, law enforcement, and FIU.

Payer Anonymity -- Smart Card and Internet-based payments systems allow a high degree of anonymity for the payer (or initiator) of transfers of value in a transaction. Anonymity may allow criminals to conceal their identities in Cyberpayments value transfers, thus facilitating money laundering. Restrictions on anonymity in SMARTCARD systems will assist law enforcement in tracking money laundering, but also involve difficult issues of privacy and security.

Peer-to-Peer Value Transfers -- Peer to Peer Value Transfers are a facility enabled by Smart Cards and Internet-based Cyberpayments systems that allows the holder of a Smart Card or Cyberpayments “wallet” to transfer some of its value to another Smart Card or Cyberpayments “wallet” holder. These value transfers are disintermediated, that is, they do not involve an identifiable third party subject to regulatory and law enforcement oversight.

Placement -- The initial phase of the three generic phases of money laundering where cash enters the financial system. For example, placement occurs when illicit cash is deposited in a bank or money orders are purchased using cash from a criminal enterprise. It is during the placement stage that illicit funds are most vulnerable to detection by law enforcement authorities.

Private-Key – the private (secret) key associated with a person or entity’s public key or a public key encryption system.

Public Switched Network (PSN) -- the term commonly used in the U.S. telecommunications industry and elsewhere for the public telephone system.

Public-Key Encryption – A system of encryption utilizing a public key to authenticate the identity of an actor sending or receiving information through an encryption-enabled communications system. Public key encryption uses separate keys to encrypt and decrypt messages meant for an authorized user. The public key is widely distributed and is used to encrypt messages meant for the public key’s legitimate holder. The holder (owner of the public key) can then decrypt a message using a secret private key secure in the knowledge that the message had not been altered in transit. Public key encryption systems also allow for the authentication of the identity of the sender in that they can be adjusted to include information regarding the identity of the sending party.

Purse Integrity -- The integrity of the “holder” of value contained within a Smart Card payment instrument. Because Smart Cards typically use a combined Public Key - Private Key encryption system to store value, these purses are subject to the vulnerabilities of established encryption systems.

SET – SET stands for the Secure Electronic Transactions encryption protocol for securing electronic commerce. This standard was created collaboratively by Visa International, IBM, MasterCard, Microsoft, and other large corporations.

Stale-dating of Smart Card Value -- A concept for manipulating the “aging” of stored value within Cyberpayment instruments for the purposes of regulatory and law enforcement oversight.

Smart cards – Smart cards are electronic instruments with the form factor of a conventional credit or debit card. These cards have embedded microchips that enable them to hold sensitive digital information. Smart cards are currently under development as replacements for credit and debit cards, and as a new stored value vehicle enabling the storage of electronic currency within the card itself.

Sniffers – Sniffers are software programs that allow for the covert gathering of password and other information from computers as they are operated in an authorized user environment. Hackers typically use sniffers to detect passwords in normal network traffic, and then seek to gain unauthorized access to the information systems so compromised.

Value Tagging -- A concept for tagging the value in a stored value instrument so that it can be tracked as it transits a Cyberpayment infrastructure.