

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.

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

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.

Debit Cards -- Payment instruments which, when used to pay for an item or gain access to cash, debit an 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.

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.

Financial Action Task Force (FATF) -- The FATF is one of the key organizations that addresses the global problem of money laundering. Formed by the G-7 Economic Summit in 1989, the FATF is comprised of 26 countries, the European Commission and the Gulf Cooperation Council. It is dedicated to promoting the development of effective anti-money laundering controls and enhanced cooperation in counter-money laundering efforts 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 one model of FIU and others exist in such countries as Great Britain, France, Belgium, the Netherlands, Argentina, and Australia. The Egmont group is an international organization formed in June 1995 by 24 countries and 8 international organizations and is comprised of FIUs from member states and international organizations interested in collaborating to combat money laundering.

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) specializing in anti-money laundering policy and regulatory coordination. FinCEN brings together government agencies and the private sector to identify ways to prevent and detect

financial crime. It is responsible for administration of the Bank Secrecy Act under which domestic financial institutions are required to keep records and file reports of certain transactions and to implement anti-money laundering programs and compliance procedures.

Geographic Targeting Order (GTO) -- A legal order of limited duration issued by the Treasury Department under the Bank Secrecy Act (BSA) requiring a domestic financial institution or group of domestic financial institutions in a geographic area to maintain records or file reports, above and beyond the record-keeping requirements of the BSA, concerning certain specific transactions.

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 a network traffic or in network usage by identifiable actors and aggregate this information into a structured presentation suitable for law enforcement use.

Internet Banking -- The delivery of traditional banking services over 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 systems 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.

Money Laundering -- The process of transforming the proceeds of illegal activities into legitimate tax-free capital. 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.”

Money Services Businesses (MSBs) – This term refers to a broad range of non-bank businesses that provide certain financial products to the public. MSBs include money transmitters, check cashiers, sellers and issuers of money orders and travelers checks, retail currency exchangers and providers of stored valued products.

Network Targeting Order (NTO) -- A postulated future legal order involving the utilization of network-borne Cyberpayment system control elements to interrogate stored value-type Smart Cards when they are used at a retail merchant or Cyberpayment issuer (financial institution or non-bank Cyberpayment firm) for value transfers.

Offshore: Foreign or overseas jurisdictions.

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 Encryption -- A system of encryption utilizing a single private key to both encrypt and decrypt messages. An example of a private key encryption standard is DES. Originally developed by the US Government, this algorithm lies at the center of many privately deployed encryption systems, including those used to protect electronic funds transfer systems.

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.

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. In connection with an NTO, such a concept may assist governmental authorities in detecting criminal misuse of Cyberpayment systems.

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