

Anti-Money Laundering Literature Search

Technology

World Bank Institute

<http://www.worldbank.org/wbi/governance>

This document prepared by Christian Eigen-Zucchi, with the assistance of Massimo Mastruzzi and Erin Farnand, under the guidance of Daniel Kaufmann. It draws from a number of sources, including bibliographical information from the International Money Laundering Information Network (IMOLIN) (available at: <http://www.imolin.org/bibliogr.htm#GENERAL>), the Financial Crimes Enforcement Network (FINCEN) (<http://www.fincen.gov/>), the Organization for Economic Cooperation and Development (OECD) (<http://www1.oecd.org/daf/nocorruptionweb/moneylaundering/bib.htm>), and other sources.

Candler, L. J. 1998. "Commingled Funds: How to Seize Proceeds of Electronic Crime." Journal of Money Laundering Control, Vol.1, No.4, April.

**Economist (1997) Next, cyberlaundering? The World. July 24th.
http://Economist.com/background/displaystory.cfm?story_id=152149**

Noting that money launderers hate cash (logistical nightmare to move), the article wonders how electronic money systems, such as stored value cards and computer-based systems will impact efforts to control money laundering. Cards should have limits, and transactions should be logged in a central place. A Bank of International Settlements report notes that features designed to protect the new systems from fraud will also make the systems less appealing to launderers.

Financial Crimes Enforcement Network (FinCEN). 1992. Wire Transfer Systems: CHIPS and SWIFT. A Reference Guide. United States Department of the Treasury, Washington, DC.

Graycar, A & Grabosky, P (eds). 1996. Money-Laundering in the Twenty-First Century: Risks and Countermeasures. Australian Institute of Criminology, Canberra.

Joyce, Brian P. 2001. "E-Diligence: Money Laundering Risks in the Electronic Arena," Journal of Money Laundering Control, Vol. 5, No. 2: pp. 146-149.

Mackenzie, Robin. 1998. "Virtual Money, Vanishing Law: Dematerialisation in Electronic Funds Transfer, Financial Wrongs and Doctrinal Makeshifts in English Legal Structures," Journal of Money Laundering Control, Vol. 2, No. 1, Summer.

Maroldy, Laura M.L. 1991. "Record-keeping and Reporting in an Attempt to Stop the Money Laundering Cycle: Why Blanket Recording and Reporting of Wire and Electronic Funds Transfers is not the Answer." Notre Dame Law Review: pp. 863-92.

Morris-Cotterill, Nigel. 1996. "The Internet: Money Laundering and Fraud," Lecture held at the Shortex 96 Conference, November 20.

Mussington, David A., Peter Wilson and Roger A. Molander. 1998. Exploring Money Laundering Vulnerabilities Through Emerging Cyberspace Technologies : A Caribbean-Based Exercise, Santa Monica, CA : Critical Technologies Institute, RAND.

Nawaz, Shahid, Roddy McKinnon and Robert Webb. 2002. "Informal and Formal Money Transfer Networks: Financial Service or Financial Crime?," Journal of Money Laundering Control, Vol. 5, No. 4: pp. 330-337.

Office of Technology Assessment (Congress of the United States). 1995. Information Technologies for the Control of Money Laundering, Washington, D.C.: The Office of Technology Assessment (Congress of the United States).

Philippsohn, Steven. 2001. "The Dangers of New Technology – Laundering on the Internet," Journal of Money Laundering Control, Vol. 5, No. 1: pp. 87-95.

Swire, Peter R. 1998. "Financial Privacy and the Theory of High-Tech Government Surveillance." Draft of September 24. (Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=133340).

Abstract (from Social Science Research Network Electronic Library)

How would you like the government to have access to the records of every purchase you have ever made? Part I of this paper describes the trend toward more electronic and more traceable payments over time, and identifies some of the harms that can occur when an individual's transactions records are readily accessible. Part II introduces the metaphor of data entering a 'vault 600 feet down,' and uses that metaphor to understand the range of ways that data can 'reach the surface,' or become accessible.

Part III systematically examines the advantages and disadvantages of government access to financial transactional data. Advantages come in administration of the tax system, in avoiding welfare and other benefits fraud, and in money laundering and other rules that seek to detect, deter and prove illegal activity. These advantages, however, can be offset by troublesome ways that government officials and unauthorized third parties might misuse financial data. Part IV expands the analysis to high-tech government surveillance more generally. The arguments developed in Part III apply to key escrow, tracking of cellular phone location, transaction-generated information for telephone calls, and other surveillance systems. One important conclusion is that the government should have a greater burden in order to get 'real time' access to data than to get 'audit trail' access after the fact.