RAND

Cyberpayments and Money Laundering

Problems and Promise

Roger C. Molander, David A. Mussington, Peter A. Wilson

Prepared for the
Office of Science and Technology Policy and
Financial Crimes Enforcement Network

Critical Technology Institute

The research described in this report was conducted by RAND's Critical Technologies Institute.

ISBN: 0-8330-2616-X

Published 1998 by RAND
1700 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1333 H St., N.W., Washington, D.C. 20005-4707
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact Distribution Services: Telephone: (310) 451-7002; Fax: (310) 451-6915; Internet: order@rand.org

SUMMARY

PURPOSE AND APPROACH OF THIS REPORT

Background

Cyberpayments are an emerging new class of instruments and payment systems that support the electronic transfer of value. These transfers may take place via networks, such as the Internet, or through the use of stored value-type smart cards. Because of the efficiency and ease with which they transfer value, these systems may also present new challenges to law enforcement. Technology exists which could permit these systems to combine the speed of the present bank-based wire transfer systems with the anonymity of currency. As a result, there are issues that must be addressed as these systems are being developed to ensure the prevention and detection of money laundering and other illegal financial transactions.

The Financial Crimes Enforcement Network (FinCEN), an agency of the U.S. Department of the Treasury, sought RAND's assistance as part of an overall effort to examine potential money laundering concerns raised by the deployment of Cyberpayment systems. In furtherance of this general objective, FinCEN supports an extensive ongoing dialogue with the Cyberpayments industry.

FinCEN's first step in advancing this dialogue took place in September 1995, when it conducted a Cyberpayments Colloquium at the New York University School of Law. The Colloquium brought together financial services providers, software developers, academics, consumer representatives, and regulatory, policy, and law enforcement officials to discuss advances in the design and implementation of emerging electronic payment systems. In addition, in May 1996, FinCEN, in cooperation with the National Defense University, hosted a computer-based cyber-money laundering simulation exercise in which the participants used advanced decision making techniques to create hypothetical Cyberpayment-based money laundering scenarios.

Cyberpayment systems have also been a topic of interest to the White House, the United States Congress and various other law enforcement and regulatory agencies. In July 1997, the President released a report on the Global Information Infrastructure (GII), entitled "A Framework for Global Electronic Commerce," a portion of which directly addressed Cyberpayment issues. In addition, Cyberpayment systems were the subject of hearings conducted in 1996 by the Subcommittee on Domestic and International Monetary Policy of the House Banking and Financial Services Committee.

Internationally, Cyberpayment systems have also received extensive attention. Multilateral discussions and studies have been undertaken by both the G-7's Financial Action Task Force (FATF) and the G-10's Working Party On Electronic Money. In June 1996, a new recommendation #13 was added to the FATF's 40 Recommendations. It states that "[c]ountries should pay special attention to money laundering threats inherent in new or developing technologies that may favor anonymity, and take measures, if needed, to prevent their use in money laundering schemes."

The RAND Effort

To address FinCEN's interest in this emerging area, RAND designed, conducted and analyzed a strategic decision-making exercise directed at both the potential problems and opportunities that the emergence of Cyberpayment systems pose for U.S. and global anti-money laundering efforts.

This report presents a description and findings of that exercise. These findings reflect the widely divergent views expressed by the participants and are based on conclusions from research RAND performed independently. The report also identifies potential alternative law enforcement and regulatory approaches to address patterns of Cyberpayment system misuse. The report reaches two basic conclusions: first, if sufficient precautionary measures are not considered while these systems develop, Cyberpayment systems could have the potential to undermine current law enforcement strategies for combating illegal money laundering; and second, this issue must be viewed as international in scope, necessitating governments to collaborate in formulating new strategies to counter any potential money laundering threats.

The overall conclusions expressed in this report are those of the RAND Corporation and do not necessarily reflect the positions of FinCEN or the U.S. Department of the Treasury.

The Exercise

This summary presents the results of the exercise's four principal tasks:

1. Describe current Cyberpayment concepts and systems.
2. Identify an initial set of Cyberpayment characteristics of particular concern to law enforcement with respect to money laundering.
3. Identify major issues Cyberpayment policies will need to address to guard against abuse by money launderers.
4. Provide alternate approaches to address potential Cyberpayment system abuse in a set of potential action plans.

Participants in the exercise included a range of representatives from the Executive Branch, the Cyberpayments industry, the banking industry, the Congress, and academia. Responses to potential Cyberpayment misuse were compiled through recording the exercise experiences of participants, and through observation and analysis of dilemmas posed by the scenario itself. During this process, traditional law enforcement and regulatory measures were compared to the potentially new challenges posed by Cyberpayment technologies. The extensive participation of Cyberpayment industry representatives made it possible to gain a working knowledge of the rapidly evolving state of the art.

Because of the challenge of educating exercise participants about both Cyberpayments and money laundering, the exercise was built on a familiar framework - drug cartels and money laundering. The hypothesis was that Mexican drug cartels would become early adopters of Cyberpayments for money laundering. The time frame for the scenario was intended to be far enough into the future (2004) so that Cyberpayment systems would have progressed

substantially, but not to the point where the market and technology for such systems had fully matured.

In support of this scenario, a "future history" was developed that described: (1) hypothetical developments in Cyberpayment systems; (2) the emergence of criminal exploitation of Cyberpayment systems for money laundering; (3) international and U.S. responses to this challenge; and (4) hypothetical drug cartel exploitation of Mexican Cyberpayment systems for money laundering in the context of a Mexican drug war.

TRADITIONAL MONEY LAUNDERING PROCESSES

In most financial transactions, there is a financial trail to link the funds to the person(s) involved. Criminals avoid using traditional payment systems, such as checks, credit cards, etc., because of this paper trail. They prefer to use cash because it is anonymous. Physical cash, however, has some disadvantages. It is bulky and difficult to move. For example, 44 pounds of cocaine, worth $1 million equals 256 pounds of street cash worth $1 million. The street cash is more than six times the weight of the drugs. The existing payment systems and cash are both problems for criminals. Even more so for large transnational organized crime groups. Regulations and banking controls have increased costs and risks.

The physical movement of large quantities of cash is the money launderer's biggest problem. To better understand the potential for abuse of Cyberpayment systems to launder money, a brief explanation of how criminals "legitimize" cash through the traditional money laundering process is provided.

Placement, *layering* and *integration* are terms used by law enforcement to describe the three stages through which criminal proceeds are laundered.

Placement. Placement is the first stage in the money laundering process and it is when illegal proceeds are most vulnerable to detection. It is during the placement stage that physical currency enters the financial system. When illicit monies are deposited at a financial institution, placement has occurred. The purchase of money orders using cash from a criminal enterprise is another example of placement. The Bank Secrecy Act (BSA) and related regulations mandate the reporting of certain types of financial transactions which involve cash and/or certain monetary instruments. To conceal their activities money launderers must either circumvent the legitimate financial system entirely, or violate reporting/record-keeping rules established under the BSA. Accordingly, law enforcement officials, working in cooperation with the financial industry, are in a unique position to combat money laundering during this stage.

Layering. Layering describes an activity intended to obscure the trail which is left by "dirty" money. During the layering stage, a launderer may conduct 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 funds transfers would constitute layering. Activities of this nature, particularly when they involve funds transfers between tax haven and bank secrecy jurisdictions, can make it very difficult for investigators to follow the trail of money.

Integration. During the final stage in the laundering process, illicit funds are integrated with monies from legitimate commercial activities as they enter the mainstream economy. The

illicit funds thus take on the appearance of legitimacy. The integration of illicit monies into a legitimate economy is very difficult to detect unless an audit trail had been established during the placement or layering stages.

THE CURRENT STATE OF CYBERPAYMENT TECHNOLOGY

Progress toward technical and commercial standards in the Cyberpayment industry has been steady and the emergence of Cyberpayment systems is gathering momentum. At present, a small number of stored-value type smart card and network-based products are undergoing pilot testing. These tests are taking place on a global basis, thus underscoring the international nature of the emerging Cyberpayments infrastructure.

Some Cyberpayment instrument features such as peer-to-peer value transfer and payer anonymity offer to the consumer an instrument with much of the flexibility and convenience of cash together with an enhanced ability to conduct purchases on an almost global basis. This technology suggests that law enforcement must begin to consider the potential implications of an environment where the wide availability of Cyberpayment instruments could substantially reduce the use of physical currency in consumer-level transactions. The features of Cyberpayment instruments that deliver this new functionality are discussed in the next chapter.

In considering the potential Cyberpayments-money laundering nexus, it should be noted that the same technologies underlying Cyberpayment products could also be used as new information gathering tools by law enforcement and payment system regulators. The privacy implications of enhanced government surveillance of information networks is an issue that was addressed at considerable length during the exercise. Any policies in this area would have to be carefully crafted so as to meet constitutional protections of individual privacy and governmental concerns with critical infrastructure protection.

THE POTENTIAL EXPLOITATION OF CYBERPAYMENT SYSTEMS FOR MONEY LAUNDERING

The RAND exercise focused on identifying potential characteristics in Cyberpayment systems that could be exploited by money launderers. By their nature, Cyberpayment systems have the potential to eliminate the money launderer's biggest problem, the physical movement of large amounts of cash. The globalization of many proposed Cyberpayment systems may also offer money launderers opportunities to exploit national differences in security standards and oversight rules to conceal the movement of illicit funds.

Previous forums such as the Financial Action Task Force (FATF) have identified a number of features that law enforcement must consider with respect to Cyberpayment transactions. Among them are (1) Disintermediation; (2) A Potential Wide Variety of Cyberpayment Service Providers; (3) Peer-to-Peer Transfers; (4) Transaction Anonymity and; (5) Denomination Limits and Expiration Dates. Each of these basic features is described in more detail below. While these basic features make Cyberpayments attractive as a potential means to reduce transaction costs in commerce and contribute to the increased efficiency of payment methods, these features are also consistent with existing vulnerabilities that have been exploited by criminals conducting financial transactions using traditional means.

Disintermediation. Historically, law enforcement and regulatory officials have relied on the intermediation of banks and other regulated financial institutions to provide "choke points" through which funds must generally pass and where records would be maintained. Disintermediation involves the transfer of financial value between entities without the intermediate involvement of an identifiable third party subject to governmental oversight (e.g., record-keeping requirements via a bank). Should Cyberpayment systems permit disintermediated value transfers in unlimited amounts, money launderers could use this as an opportunity to avoid traditional law enforcement money tracing methods.

Potential Wide Variety of Cyberpayment Service Providers. Bank and non-bank entities may be subject to different rules regarding their operation of Cyberpayment systems. This difference is already the case in several nations where non-bank Cyberpayment issuers are currently subject to a different set of rules from banks. A simple extension of traditional payment system oversight to new non-bank Cyberpayment issuers may address some of the concerns regarding potential system abuse by money launderers. However, the new systems are configured differently and constantly mutating, so a "one size fits all" regulatory approach is not necessarily appropriate or even possible.

Peer-To-Peer Transfers of Value. Some Cyberpayment systems allow consumers to transfer value peer-to-peer (and thus, disintermediated) using an electronic "wallet," a telephone, or via the Internet. Such value transfers pose perhaps the most direct challenge to governmental oversight of Cyberpayment systems. In the absence of intelligence information or evidence from non-Cyberpayment system sources (e.g., physical surveillance) triggering an investigation into specific suspect stored value instrument activity, clearly illicit or suspicious peer-to-peer transfers of value are unlikely to be detected.

Transaction Anonymity. In some emerging Cyberpayment products, the origins of funds are relatively opaque and the identity of the individual or entity transferring them difficult to determine. In fact, payer anonymity (the identity of the party initiating a Cyberpayment value transfer) is a central characteristic of some proposed systems. For Cyberpayment value transfers (e.g., via the Internet or the basic telephone system), transaction anonymity could be an almost insuperable barrier to law enforcement detection. While candidate solutions for this problem have been put forward, they raise issues concerning individual privacy.

Denomination Limits and Expiration Dates. Cyberpayment product issuers are likely to limit the maximum amounts that can be stored on smart cards or other devices, to reduce the risks of fraud or other losses. As with credit cards, Cyberpayment issuers will also likely establish needs-based denomination limits that would be determined by commercial and market factors. (Recent consumer tests of Cyberpayment systems indicate likely consumer limits of approximately $1,000 - $3,000). Cyberpayment products held by retailers are likely to have a much larger value limit than those for most individuals and differ widely between retailers. Cyberpayment value could also be programmed to expire after a certain number of transfers. As early technology adopters, money launderers could be expected to exploit whatever limits are established, just as they do now by structuring transactions under currency reporting limits, obtaining multiple cards (credit or debit), using multiple names, or employing multiple issuers.

THE EXERCISES

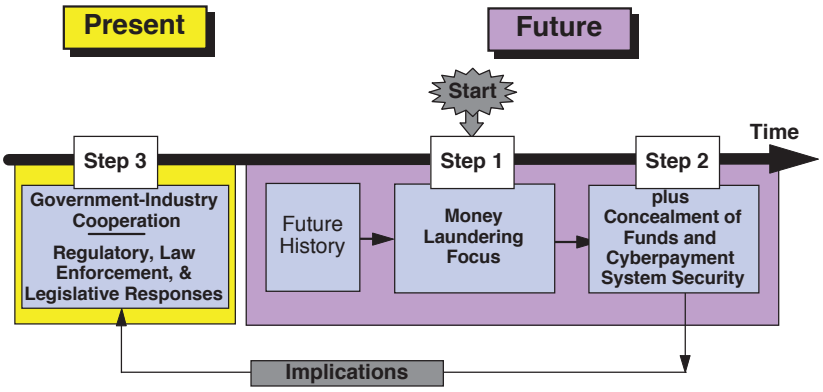

Figure 1. Exercise Methodology

The first two steps of the exercise (see Figure 1) were set in the year 2004. The time frame for the exercise was intended to be far enough in the future so that Cyberpayment systems would have progressed substantially. The third step returned to the present or, more precisely, the very near future. The basic steps of the exercise were:

STEP ONE. First phase of the crisis. Competing Mexican and Colombian drug traffickers increasingly exploit Cyberpayment technologies for money laundering. U.S. decision-makers face a series of difficult tactical and strategic issues in the areas of law enforcement, international financial institution collaboration, and bilateral initiatives to improve U.S.-Mexican Cyberpayment system oversight.

The participants were asked to consider, debate and select appropriate tactical responses to the emerging crisis.

STEP TWO. Second phase of the crisis. Escalation in the "Mexican Drug War" and further exploitation of Cyberpayment systems for money laundering by the drug cartels, in spite of more aggressive law enforcement efforts. Cartel efforts threaten the financial and perhaps political stability of Mexico.

The participants discovered that Mexico was in the middle of a financial crisis, that the new Cyberpayment system had a flawed encryption scheme and that Mexican drug cartels were taking advantage of the situation. By laundering money, the cartels were causing major economic and price destabilization through manipulating Cyberpayment systems. As the Mexican crisis escalated to the point where money was flowing out of the country in massive amounts, the participants were again asked to prepare a memorandum with the objectives of protecting the U.S. Cyberpayment industry

from spillover damage caused by the Mexican Crisis. The participants were to recommend short term measures to respond to security problems in the systems and attempt to stimulate broader international measures to improve the industry.

STEP THREE. Return to the present/near future; lessons learned/ implications stage of the exercise. Participants were asked to address the challenge of formulating a strategy and policy "Action Plan" that would make the hypothetical events portrayed in the foregoing scenario impossible, less likely, and/or more manageable.

Specific focus was placed on the development of ideas for: (1) government-industry cooperation and (2) regulatory, law enforcement, and legislative recommendations to prevent the potential abuse of Cyberpayment systems for money laundering.

A Hypothetical "Cyberpayment Network Targeting Order"

The exercise used a hypothetical analogue to a law enforcement technique used currently, the Geographic Targeting Order (GTO). A GTO gives the Treasury Department the authority to require a financial institution or a group of financial institutions in a geographic area to file special reports or maintain records beyond the ordinary requirements imposed by BSA regulations.

A recent GTO in New York in 1996-97 required 3,200 money transmitter agents to report identifying information on all cash remittances of $750 or more to Colombia. This led to a dramatic reduction in the volume of suspected drug-related funds flowing through money transmitters to Colombia, and triggered a number of large seizures of cash at air and sea ports along the eastern seaboard as traffickers shifted to more vulnerable means of moving their money.

The physical movement of cash remains a critical weak point in drug trafficker attempts to launder illicit funds. Therefore, GTOs are especially effective because of their ability to target a particular area of cash movement. The RAND exercise employed a hypothetical Cyberpayment Network Targeting Order (CNTO). The CNTO enabled law enforcement authorities to trace transfers of value within Cyberpayment networks. A combination of traditional investigative methods and the hypothetical CNTO was seen by some as a means of more effective detection of illicit activity within cyberspace. Others, however, saw it as beyond the bounds of existing law and technology.

The exercise illuminated potential problems flowing from the possible use of Cyberpayment systems by money launderers working for international narcotics cartels. Participants in the exercise discussed law enforcement and Cyberpayment oversight problems that flowed from the perceived abuse of these systems and evaluated potential remedial measures, such as the CNTO, for safeguarding Cyberpayment network security.

POTENTIAL POLICY IMPLICATIONS

Five general policy issues were identified in the exercise as areas of money laundering-related concern: (1) law enforcement issues; (2) regulatory issues; (3) international policy coordination; (4) Cyberpayment system architecture and design issues; and (5) traditional definitions of currency. Each of these issue areas carries important implications for the future of government and industry roles in managing these new payment system technologies so as to prevent their abuse. Because the exercise participants represented the entire spectrum of interests in this evolving technology, the responses to the exercises varied dramatically.

Participants considered these hypothetical policy issues within a decision-making process linked to the events of the scenario. Their responses were collected by exercise designers and reported to all participants during a discussion session led by the group chairpersons. This information was in turn analyzed by using the participants' annotated briefing books which contained individual responses to the questions presented during the exercises and operational notes taken by conference designers during exercise deliberations.

While no clear consensus on any overall approach to the potential concerns in the Cyberpayment-money laundering nexus was identified during the exercise, an important structuring and focusing of the debate in the five areas did occur. The findings listed below reflect RAND's evaluation of the focused discussion of the participants as well as RAND's independent research.

Due to the breadth of the subject, other larger issues concerning monetary policy and regulatory oversight emerged that were outside the direct scope of the exercise. Additional consideration of these issues, over time, will be needed to evaluate Cyberpayment systems and to ensure an effective and consistent process for governmental oversight.

Law Enforcement

The discussion of law enforcement issues focused predominantly on the perceived potential value of Cyberpayment instruments to money launderers and others attempting to conceal financial activities from government oversight. The second focus of these deliberations was on potential regulatory and law enforcement responses to perceived Cyberpayments abuse, and the place of computer-based investigative techniques alongside more traditional investigative techniques, in countering patterns of abuse.

Without proper precautions, Cyberpayment systems could have the potential to undermine traditional law enforcement investigative tools and techniques. Current anti-money laundering law enforcement strategies and techniques rely on extensive use of manpower and paper trails left by traditional monetary transactions. Since Cyberpayments are not personnel-intensive and could potentially leave little or no paper trail, they could facilitate a means for circumventing current techniques.

Law enforcement authorities may require new tools and techniques in order to conduct effective surveillance and analysis of Cyberpayment network information flows. Some international sharing of these information resources may also be required.

Computer-based investigative techniques may allow Cyberpayment system regulators and law enforcement authorities to trace questionable electronic fund flows. Law enforcement authorities may employ computer investigative techniques to evaluate information regarding suspected Cyberpayment system abuse. This evaluation depends, however, on some sort of infrastructure being developed for identifying value flows within networks that meet certain suspicious criteria, or more pointedly on differentiating Cyberpayment value from broader traffic flows within the Internet. International information sharing in pursuit of coordinated Cyberpayment system oversight and protection may involve risk. Jurisdictional issues involving federal, state, and local government law enforcement activities pertaining to potential Cyberpayment system abuse will need to be addressed if effective counters to potential abuse are to be implemented.

Individual privacy concerns are a significant issue in the design of oversight procedures for Cyberpayment systems. As noted, government concerns with the potential abuse of Cyberpayment systems create calls from some for extensive surveillance capabilities to be developed for Cyberpayment networks. However, this suggestion raises privacy concerns for individuals and potential constitutional issues for society. Consumer privacy advocates, in particular, have warned of possible abuses of surveillance techniques. Reconciling divergent perspectives on this issue will likely require continuous dialogue between and among the many stakeholders in the Cyberpayments arena.

Regulatory Issues

During the exercise, regulatory questions were perhaps the most vigorously discussed of any of the defining concerns involved with Cyberpayment systems. As an overlapping area of interest, regulatory concerns are themselves dependent on more general decisions on the importance of international policy coordination on the oversight of Cyberpayment systems, and on decisions regarding the legal character of Cyberpayment value as a payment instrument. Beginning with the issue of which institutions or entities would have the legal authority to provide Cyberpayment services, participants voiced a number of differing perspectives on the topic. A majority of participants argued that whichever regulatory approach was adopted, it should be based on the ongoing collaborative public-private partnership. Under this rubric, however, differences of opinion were voiced on the character and intrusiveness of governmental *mandates* with respect to both Cyberpayment system operators and the electronic payment instruments themselves.

Public-private collaboration will be key to crafting and implementing a coherent and sustainable Cyberpayment system infrastructure protection process. The expanding dialogue between government and private industry on Cyberpayment network standards and product features in the U.S. and elsewhere is a major positive step towards coming to grips with potential abuses of Cyberpayment systems. Many participants voiced concern that, at least initially, cyberpayment system providers that operate with or through banks should be subject to laundering controls analogous to those that apply to banks and other financial institutions.

Policy, regulation, and enforcement in the Cyberpayment area will consistently be challenged to keep up with the rapidly evolving technology. For the foreseeable future, law enforcement and financial payment system regulators will not experience a stable technical environment in the Cyberpayment arena. National regulations imposed in the absence of mature

international technical and market standards will need to be inherently flexible in responding to this evolutionary environment. This situation could also inhibit the development of reliable technical means for tracing transactions within Cyberpayment networks when investigating illicit financial activity. One suggestion for addressing this concern was developing minimum standards for appropriate government access to Cyberpayment data as a condition of licensing – without prejudice to the particular encryption and product protection technologies implemented in a particular application.

Domestically, the U.S. government may need to play a facilitating role for both industry and consumers to accelerate the achievement of effective standards for Cyberpayment systems. Because of the centrality of financial payment systems to the U.S. economy and the potential impact of a commercially mature and successful Cyberpayment industry on our economy, a Cyberpayment system failure could negatively affect the credibility of the entire Cyberpayment industry. It was also suggested that the public perception that these systems are more (or less) prone to fraud or financial abuse than traditional payment methods may significantly affect consumer acceptance of Cyberpayment transactions. Any regulatory and law enforcement actions designed to monitor consumer behavior within the Cyberpayment environment will need to be closely integrated into a broader infrastructure assurance policy in order to protect the industry's acceptance in the financial marketplace.

International Policy Coordination

The discussion on international policy issues raised by the Cyberpayment systems focused on the degree to which national guidelines and regulations on system characteristics could be rendered ineffective and/or circumvented by international variation in oversight and regulations. Participants agreed that Cyberpayment products were inherently international in nature, and that any longer-term governmental actions would need to be international in scope.

International strategy and policy coordination will be central to effective Cyberpayment system oversight. The global nature of the Cyberpayment infrastructure suggests that some harmonization of guidelines and standards for Cyberpayment system operators will be imperative for effective oversight of the Cyberpayment industry. Because the Cyberpayment industry is evolving, a comprehensive and thorough regulatory regime is unlikely to be achieved prior to the stabilization of commercial and technical conditions. The recent discussions within a number of relatively recently established international bodies such as the G-7 Financial Action Task Force (FATF) have been an especially effective means for sharing insights on international Cyberpayment system oversight.

Cyberpayment System Architecture and Design

The discussion of Cyberpayment systems examined the question of whether this type of payment instrument posed potential impediments to law enforcement and payment system regulators in their investigation and enforcement of money laundering activity or whether particular types of Cyberpayment products constituted unique risks of abuse. Participants did not articulate a consensus on these issues, other than to observe that for security reasons, Cyberpayment system operators would tend to invest heavily in designing systems that

minimized their degree of exposure to fraudulent use. These same measures could also be used against money laundering.

Both industry and government share an interest in developing technical and system standards that adequately reduce the possibility of fraud and financial crime. This observation was interpreted to mean that governments should attempt to achieve traditional oversight goals in the Cyberpayment area through voluntary compliance rather than through mandates.

The output from government/industry efforts to evaluate Cyberspace risks in key national infrastructures such as telecommunications, electric power and transportation need to be fed into the policy process for determining necessary actions for Cyberpayment infrastructure protection from money laundering. The President's Information Infrastructure Task Force recently stated that the Administration has already taken steps that will foster trust in encryption and provide safeguards that society will need. It also stated that it was working with Congress to enact legislation to facilitate development of voluntary management infrastructures that would govern the release of information to law enforcement officials pursuant to lawful authority.

Definitional Issues

Any interim definition of Cyberpayment value as possessing legal characteristics similar or equivalent to traditional paper currency (i.e., cash) will have to be monitored and perhaps adjusted due to frequent changes in the design of Cyberpayment products by industry. The issue of how Cyberpayment's value is to be defined, e.g., as cash, as funds transfers, monetary instruments or a new term, centered on establishing an appropriate regulatory oversight regime for Cyberpayment systems, while at the same time not imposing onerous (and costly) requirements on an evolving industry. It was generally felt that regulatory decisions should be made with an eye to not disadvantaging (or advantaging) any particular Cyberpayment system type, but rather that the marketplace should be allowed to make such determination.

RAND'S ANALYSIS

Three Models of Cyberpayment Oversight

The exercise deliberations yielded a number of differing viewpoints concerning the potential issues and opportunities created by the deployment of Cyberpayment systems. Participants offered perspectives on the role of government in Cyberpayment system oversight, the potential for industry self-regulation, and the difficulties of designing regulatory guidelines for a brand new industry.

RAND's analysis of participant deliberations has been categorized into three broad schools, or models, of potential Cyberpayment System Oversight. While a consensus on any one of the approaches was lacking, debate returned again and again to some general themes. The models, described below, are not mutually exclusive, but are related to one another. Combinations of these approaches will most likely eventually become the focus of the actual

decision making on the appropriate oversight regime for Cyberpayment systems. It is important to point out, however, that controversies over whether government or industry are best suited to regulate this evolving industry are not ended by the adoption of any particular perspective on Cyberpayment system regulation. The *process* through which these issues are to be resolved may in fact be of greater importance than the particular end-point argued by proponents of any of the models in question.

Listed below each model are candidate plans that could be considered for that model in an attempt to shape constructively the emerging Cyberpayment system environment. Consistent with the debate among exercise participants, the plans and the models do not represent mutually exclusive approaches. The different perspectives are linked by critical assumptions such as the timing of Cyberpayment system deployments by private industry, and on the pace and character of consumer acceptance of the new payment instruments.

Model 1: Government Lead. Cyberpayment oversight could include a strong role for government in directing industry responses to potential Cyberpayment system vulnerabilities. This approach to oversight would anticipate only a few highly structured occasions where industry would be allowed to react to prospective rules.

Model 1 Candidate Plan

I. Issue an administrative finding that Cyberpayment value is to be treated as a cash equivalent for the purposes of anti-money laundering oversight.

II. Identify key Cyberpayment system features and begin a regulation writing process designed to bring these payment instruments into close scrutiny. Regulations drafted during this process would include:

- A definition of Cyberpayment instrument functionality including: denomination limits, peer-to-peer value transfer capabilities, system interoperability, and transaction frequency;
- Rules on the permissible issuers of Cyberpayment value;
- Mandates on the technologies contained in Cyberpayment instruments; and
- Mandates on system-audit and remote system management (under legal supervision) capabilities.

III. Initiate preparation of an international meeting involving senior finance ministry officials with a view to creating an international convention on the operation of Cyberpayment systems. Preparatory work would seek to establish common regulatory treatment of Cyberpayment issuers in all participating countries; to work out procedures to ensure the ability of states to enforce legal orders against Cyberpayment issuers or instrument holders whatever their country of residence; and to coordinate law enforcement action against international crime groups;

IV. The Administration would propose legislation, when necessary, establishing federal primacy in the oversight of Cyberpayment systems, and establishing tampering with Cyberpayment instruments (network or card-based) as a federal crime analogous to counterfeiting.

Model 2: Collaborative. This model emphasizes a more collaborative public-private sector partnership in Cyberpayment system oversight. This model envisions expanded governmental consultations with Cyberpayment system operators as the basis for regulatory action. Technical standards within Cyberpayment products would be decided by industry with government mandates only existing for systems used by government agencies to deliver services. Under this model, an independent government agency would administer a fixed set of rules governing the industry.

Model 2 Candidate Plan

I. Continue incremental regulatory action on Cyberpayment systems consistent with the pace of their introduction;

II. Begin a structured six-month set of consultations with industry designed to elicit input for a draft policy paper on Cyberpayment system oversight. The paper would address technology, regulatory, and law enforcement issues in both domestic and international dimensions. This paper would also support the U.S. negotiating position at the proposed meeting to establish an international convention on Cyberpayments system oversight. Industry and government officials would be equally represented in a steering committee through which the policy paper would be drafted.

III. Initiate experts meetings within the G-7 FATF or other international groups to discuss a short-list of the most pressing money laundering concerns of Cyberpayment systems from the points of view of payment system regulators and law enforcement authorities. These meetings would support a major international conference two years hence, at which senior finance ministry officials would be asked to draft a statement on the international oversight of Cyberpayment systems.

IV. Consult Cyberpayment industry representatives on the technical features necessary to establish CNTO-like system interrogation capabilities within planned Cyberpayment networks. Begin a regulation writing process in consultation with privacy advocates to mandate such capabilities for Cyberpayment systems if contacts with industry do not yield desired results.

V. Begin consultations where necessary with the U.S. Congress on the drafting of legal guidelines for law enforcement access to Cyberpayment records. In the interim, establish administrative guidelines for the use of these records by law enforcement authorities in criminal investigations.

Model 3: Self-Regulatory. Industry would be charged with setting and enforcing its own anti-money laundering standards under this regime, with government authorized to oversee this activity to ensure effective compliance. International oversight of Cyberpayment systems would take place on a government-to-government basis, but with industry enjoying key representation in governmental bodies charged with setting overall controls and oversight.

Model 3 Candidate Plan

I. Initiate a series of consultations with Cyberpayment industry representatives with a view to encouraging the establishment of an industry-wide association to represent commercial concerns in policymaking.

II. Seek legislation assigning functional responsibility for Cyberpayment systems to an established agency or new administrative body. A board made up equally of industry and government representatives would coordinate regulations in this functional area.

III. The Cyberpayment industry would be asked to provide – on demand – Cyberpayment records for government as needed during criminal investigations. This information access would be governed by administrative guidelines set up by the independent Cyberpayment oversight body, and would not be subject to judicial review.

It appeared that Model 1 conflicted the most with the contemporary trend which favors allowing the market to develop more fully before a regulatory scheme is adopted. Model 2 could be interpreted as a transitional stage, where models of industry-government collaboration could provide a "proof of principle" for concepts of industry self-regulation and governmental "arms length" supervision. This interpretation would leave Model 3 as an oversight framework perhaps best-suited when the market has matured. With established frameworks of industry-government and inter-governmental information and knowledge sharing, it is possible that this sort of oversight model could allow for the reconciliation of market efficiency and competitiveness concerns with public issues regarding financial privacy and the safety and soundness of the Cyberpayment industry.

The material that follows looks at the common action elements that might be included in a preparatory phase to any government oversight approach.

Common Elements

The introduction of Cyberpayment systems raise: (1) law enforcement issues; (2) regulatory issues; (3) need for international policy coordination; (4) Cyberpayment system architecture and design issues; and (5) non-traditional forms of payment with currency attributes. Work in any area would necessitate essentially *preparatory activity* for any more overarching regulatory project aimed at influencing Cyberpayment industry trends to reduce any money laundering vulnerabilities. A common preparatory phase of government action to guard against illicit uses of those systems could include:

- Conducting a baseline analysis of the technologies being used in proposed Cyberpayment system designs. This analysis would address: (1) the potential vulnerability of proposed technologies to "hacker" attack; (2) the ability of the system to deliver information on Cyberpayment value transfers to auditors; (3) the privacy implications of different Cyberpayment system architectures.

- Asking banks and non-banks (see Glossary) interested in operating Cyberpayment systems to respond to a list of security and abuse concerns generated by law

enforcement and payment system regulators. (For the purpose of this report, non-banks will be identified as money services businesses (MSBs).) Required responses would address the critical information access concerns of the government in anticipation of broad deployment of Cyberpayment systems, and to react to scenario-based insights regarding potential patterns of abuse by criminals.

- Collecting and analyzing the results of the Cyberpayment industry submissions prior to the release of a preliminary policy paper by the U.S. Government (agency or agencies to be decided) that would constitute an initial government statement of regulatory preferences on Cyberpayment systems.

- Calling a special meeting of the FATF or some other international group, in order to begin structured experts meetings to discuss the technical standards and law enforcement issues raised by the emergence of Cyberpayment systems. This activity would be designed to coordinate with the U.S.-initiated Cyberpayment issuer requirement for response listed above.

- Convening a major conference involving senior Cyberpayment industry representatives, senior staff from the law enforcement community and potential payment system regulatory agencies, and international observers from international financial institutions as a final activity prior to the initiation of a formally introduced Cyberpayment anti-money laundering oversight policy. The objective of such a conference would be to achieve a degree of consensus on the character of emerging Cyberpayment systems, a consciousness of common regulatory and law enforcement challenges, and – where possible – agreement on the elements of a strategy for conducting such international oversight of Cyberpayment systems.

Candidate plans for addressing the potential money laundering problems posed by Cyberpayment systems share many common features. The principle differences among the plans are in the level of government mandates imposed upon Cyberpayment system operators. In turn, the scope of administrative action also varies, with the Models 1 and 2 seeking a binding international convention on Cyberpayment system oversight, and Model 3 initiating an industry-centered approach whose international version would likely include the largest private global financial institutions managing the sector on behalf of governments.

Combinations of these approaches, rather than any one perspective, are the most likely outcomes given the necessity for consensus-based action. Participants within the exercise considered the merits of government and industry-led actions to counter perceived Cyberpayment system vulnerabilities. While no clear consensus emerged, the predominant perspective in the deliberations supported close industry-government collaboration to address potential problems.

PREPARATION FOR ACTION

Participants in the exercise, whatever their particular positions on the action to be taken, did broadly share the idea that government needed to begin thinking of the appropriate regulatory and law enforcement actions necessary to adapt effectively to emerging Cyberpayment systems. Because new technologies are currently under pilot testing, government already confronts the potential need to include Cyberpayment system operators under some regulatory regime. This

inclusion might be achieved in part through the creative extension of current anti-money laundering requirements of banks and money service businesses to those seeking to deploy Cyberpayment products.

Analysis of the technologies and features of the new electronic payment systems is the first step toward understanding their implications for traditional anti-money laundering oversight rules. The entities most aware of the fast-changing technical state of the art are -- not surprisingly -- the commercial firms designing Cyberpayment products. Consequently, it is advisable that governments expand the dialogue with the private sector on the character of Cyberpayment products, including the security-related technical details intended to protect the financial integrity of Cyberpayment systems. Information gained during this process could contribute to a thoroughgoing evaluation of the appropriate policy environment for Cyberpayment products.

A BOTTOM LINE

What overall conclusions can be drawn from RAND's analysis of Cyberpayment systems and money laundering? The exercise experience revealed a wide scope of issues facing potential payment system regulators and the law enforcement community.

Prompt collaborative action by industry and government and among governments to prevent the exploitation of Cyberpayment system vulnerabilities is a critical way to respond to this still-nascent threat of exploitation by money launderers. Collaboration on standards, regulatory transparency, and vigorous surveillance of possible vulnerability exploitation offers the key to successful protection of Cyberpayment systems from such abuse. Furthermore, the scope of the potential money laundering problem is international. Effective law enforcement will require national governments to collaborate in setting the ground rules for Cyberpayment systems' deployment and operation.

The exercise provided a valuable arena in which policy and law enforcement issues raised by Cyberpayment systems could be examined. In the future, an extension of the simulation to include international participants would allow for a deeper understanding of the challenges involved. In turn, the exercise highlighted the importance of a harmonization of approaches to Cyberpayment system oversight to guard against and detect the illicit use of these systems. The danger that criminals will seek to exploit weaknesses in regulations wherever they appear suggests that governments need to coordinate investigative and enforcement activities aimed at minimizing this potential abuse.

While it is premature to draft a comprehensive oversight regime for Cyberpayment products, a structured dialogue involving government, issuing companies, and other stakeholders, will help to shape the direction of any such regime. The authors hope that the insights outlined in this report will assist in the advancement of public debate on Cyberpayment system security and the appropriate role for government in this rapidly growing segment of the Global Information Infrastructure.