Department of the Treasury
Financial Crimes Enforcement Network

FinCENfax

2070 Chain Bridge Road, Suite 200, Vienna, VA 22182-2536
1500 Pennsylvania Avenue, NW, Suite 3210, Treasury Annex, Washington DC 20220

To:	Simson Garfinkel
Office/Agency:	
Phone:	
Fax:	508/696-8989
From:	Joyce McDonald
Office:	Communications
Phone:	703/905-3770
Fax:	703/905-3690
Date:	11/6/95
Pages including this cover page:	12

Comments:

Simson - As we discussed, Director Morris' testimony follows.

STATEMENT

of

STANLEY E. MORRIS

DIRECTOR

FINANCIAL CRIMES ENFORCEMENT NETWORK

UNITED STATES DEPARTMENT OF THE TREASURY

before the

SUBCOMMITTEE ON

DOMESTIC AND INTERNATIONAL MONETARY POLICY

of the

COMMITTEE ON BANKING AND FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

October 11, 1995

Mr. Chairman and members of the Subcommittee, I am Stanley E. Morris, Director of the Financial Crimes Enforcement Network called "FinCEN." Your series of hearings concerning the future of money are timely and very important. I am very pleased to have been asked to participate.

Two weeks ago, FinCEN sponsored a Colloquium on cyberpayment systems at New York University Law School. We brought together more than 125 people--financial services providers, software developers, academics, consumer representatives, and regulatory, policy, and law enforcement officials--to speak face-to-face about the evolution of advanced electronic payment systems. Our attendees included a number of people who appeared before this Subcommittee on July 25, as well as the Comptroller of the Currency, Under Secretary Noble, senior officials of the Federal Reserve Board and of the Treasury, and a member of your subcommittee staff.

The message we received at the Colloquium is the one you heard in July and have heard today--that advances in the design and implementation of the new payment systems are among the most complex and potentially far-reaching developments generated by the "age of the intelligent machine."

Today, I want to address possible elements of the new systems that cause concern for officials responsible for fighting money laundering and financial crime.

Note that I refer only to "possible" elements of the new systems. The systems don't have a common architecture or terminology. And representatives of the industry with whom we have spoken are alert to the risk that their systems could be misused. They are willing to work with government to do something about the risk.

I also want to emphasize that the fact that we are thinking about the new technology does not mean that we are against it--just the opposite. It means that we are keenly aware of our need, indeed of our responsibility, to understand the technology first, before deciding if there are law enforcement issues that require resolution.

A sense of FinCEN's mission--and of its evolving partnership with the financial community--helps to frame our perspective on the new systems. FinCEN establishes, oversees, and implements Treasury policies to prevent and detect money laundering. It administers the Bank Secrecy Act, or "BSA," which is the core of those efforts.

Our interest in the new systems reflects our own responsibilities as a regulator. The BSA requires recordkeeping and reporting by more than 200,000 financial institutions of all kinds and creates the largest currency transaction reporting system in the world. We have already been asked whether and how the BSA applies to the new systems, and as a result, we have come to recognize--as have you and many others--that the systems' potential uses raise issues that go beyond the jurisdiction or mission of any particular agency.

That range of issues is another reason FinCEN is involved. As its name indicates, FinCEN is itself a "network;" it serves as the nation's central point for broad-based financial intelligence and information sharing for federal, state, and local law enforcement and financial regulatory agencies. To make its own network more effective, FinCEN strives to bring enforcement agencies and the private sector together wherever it can, to create cost-effective measures to prevent and detect financial crime.

As FinCEN's Director, I am keenly aware of the potential impact that the new technologies can have on the work of financial investigators. Let me explain.

Financial investigations are recognized as the key to combating narcotics trafficking and organized and white collar crime. But such investigations are extremely difficult to carry out. First, it takes many years of working in the financial industry to understand all its intricacies. Second, no single agency possesses a sufficiently broad or cross-jurisdictional focus and information base to track financial movements; and third, the sheer size, variety, and pace of change of the financial sector make financial investigations ever more difficult.

Our strategies to deal with these difficulties have historically centered on eliminating "bank secrecy." Treasury has administered the BSA, as Congress intended, to require record keeping that would preserve a financial trail for investigators and to require reporting of significant

currency transactions, and transportation of currency and monetary instruments into and out of the United States.

For the past two years, building on legislation which originated in this Committee, we have worked diligently to "re-engineer" the BSA, enlisting proactive support of industry, cutting out unneeded regulation, and simplifying what remained. A cornerstone of our approach is the reporting of truly suspicious transactions, cutting way back on mechanical reporting that is often far more costly than its usefulness justifies.

The investigator's motto— "follow the money," relies on the need of criminals to move funds through the financial system to hide and use the proceeds of their crimes. Currency is anonymous, but it is difficult to handle and to transport in large amounts. Anyone who has seen a pallet of newly printed bills on a tour of the Bureau of Engraving and Printing, or, better still, has seen a photograph of a drug cartel's counting house or currency stashes, knows what I mean.

A large amount of currency, like an elephant, is difficult to hide. It takes time to move and attracts attention. Attention is the enemy of criminal activity.

The new payment systems have the potential to change all this. If cards can be "loaded" with value not just from banks, but from retail outlets or other sources, current systems for tracking funds could lose their value. Internet-based systems for transferring large amounts or a

way to store large sums on a "smart card" that would be recognized as "carrying" dollars at any place in the world pose the same risks.

Our reasons for concern do not stop with asking whether such transfers are transfers of "currency." The question is not to make sure we get a report simply to get a report. The new systems combine the speed of the present bank-based wire transfer system with the anonymity of currency—they create the best of both worlds. They make wire transfer equivalents anonymous, and they make currency easy to move around the world at almost the speed of light. Smart card transactions and international payments transacted over the vast Internet system could be immediate, potentially anonymous, effected in multiple currencies, and conducted entirely outside of the traditional funds transfer channels.

Is that necessarily bad? Not at all. In fact, far from it. At the Colloquium, Under Secretary Noble used an example I'd like to repeat: a U.S. retailer, let's say a shoe store, could accept smart cards for purchases. As the store's revenues increase, it could transfer the value of its revenues to a smart card or download the value into a computer. This value could in turn be transferred through the Internet to financial institutions or people around the world to pay invoices, order materials, or pay suppliers--in all cases stimulating commerce, making trade less expensive, and providing benefits to consumers.

The same systems can benefit consumers in other ways. They can reduce the hazards and inconvenience of carrying cash, and they can provide a significant degree of protection, via smart card technology, for those who do not have bank accounts. They can foster electronic commerce, and they can reduce the costs of processing cash by retailers and the risks of robbery for merchants in all areas.

But, as I have pointed out, the same efficiencies could, at least in theory, create opportunities for serious exploitation by money launderers. Suppose my Internet user is a narcotics trafficker or an agent for a gang of sophisticated criminals of any other sort. Consider the invoices the trafficker might pay, the supplies he might order and the transactions he might accomplish if, for instance, he could download an unlimited amount of cash from a smart card to a computer, and then transmit those funds to other smart cards in locations around the world--all anonymously, all without an audit trail, and all without the need to resort to a traditional financial institution.

History has shown us that as we invent new technologies, criminals are waiting on the periphery to use them--trains produce train robbery, telephones create telephone frauds, air craft hijacking and terrorism. In the same way, the possibility of virtually untraceable financial dealings, if it came to pass, would create new, but this time, perhaps unparalleled problems for law enforcement. Those of us who have fought so hard to end bank secrecy as a convenient

excuse around which criminals can cluster will have won little if we now turn to a world in which financial institutions can easily be bypassed via the Internet or use of the telephone lines.

That leads to an important point about money laundering and related financial crimes. They all involve taking acts that are themselves, in isolation, not only legal but commonplace--opening bank accounts, wiring funds, and exchanging currencies in international trade. Given that basic fact, we have few ways now to separate the malefactors from the businessmen. The new technologies will give us even fewer ways, unless we work with their developers.

How should we do so? I'll tell you frankly, I don't know yet. Technology raises the stakes in many ways and for each risk there is a benefit.

For example, I would be concerned if the new systems permitted encryption of large financial transactions in a way that would make their detection or the identification of the sending or receiving parties incapable of reconstruction, in certain cases. But encryption is vital to protect the security of electronic commerce and financial transfers, and sophisticated encryption is already in place, of course, in the interbank transfer systems. And I recognize the uses of encryption to protect privacy that consumers feel is threatened by the computer age.

We are not without tools to deal with issues as they develop, although I frankly don't know yet whether those tools will be adequate. As I indicated earlier, the BSA authorizes the

Secretary of the Treasury to require recordkeeping by financial institutions and to require reports of suspicious transactions and currency transactions. The BSA also requires the registration of money transmitters. How do these concepts apply to the new systems?

Reporting of cross-border transportation of currency and monetary instruments in excess of $10,000 is also required by the BSA. How should that requirement be applied to smart cards shipped or carried across the border? To Internet transactions using the new systems?

Here are some of the questions we will be asking:

— Do the systems create and maintain an audit trail?

— Does that audit trail extend beyond the initial transaction to subsequent transactions in the chain?

--What are the privacy implications of that audit trail?

--Will the systems be restricted to transactions below a certain dollar amount--a cap, if you will?

--Will the systems permit effective and timely monitoring of suspicious transactions, for example, repeated multiple transactions designed to evade dollar caps?

-- Are the cyberpayment systems being offered by or through a regulated entity?

--Do the systems permit self-contained, person-to-person transactions without the involvement of a financial institution or other regulated entity?

We don't know enough yet to make good decisions. We may need this Committee's assistance in dealing with the questions I've raised, but the time is not yet right to ponder whether additional legislation is required.

Too often, government regulators have attempted to thwart a potential criminal threat by imposing burdensome regulations that reflect little appreciation of the nature of the threat, or the business practices of the affected industries. We cannot make the same mistakes with cyberpayment systems. The technology is developing too rapidly, and the gains and efficiencies potentially created by the new systems are too important. At the same time, without thoughtful and balanced approval of law enforcement concerns now--before criminals begin to exploit the new technology--the prospects for abuse by organized crime, money launderers, and other financial criminals could be too great.

What does the "cyber-future" hold for FinCEN? Candidly, we are still sorting through the wealth of information, recommendations, and comments received at our Colloquium. We're working hard to support the Comptroller as he coordinates Treasury's efforts. I'm very pleased that the Defense Department's Advanced Research Projects Agency has awarded a contract to KPMG Peat Marwick to assist FinCEN in continuing its work.

That leads to a final point. This new technology requires a proactive approach from law enforcement, and I think FinCEN is in a position to assist in working out the issues raised in today's hearing. We were created in the recognition that financial crime is a problem and that it can only be alleviated by bringing together resources from many areas and leveraging their impact. In the same way, I hope that we can serve as a "network" that enables law enforcement and financial compliance officials, technology developers and bankers, to work out the details of solutions to some of the potential problems I've outlined.

We do not want to impede the development of technologies that can benefit us all. Our goal is simply to try to inoculate the new systems against crime and misuse by criminals - to permit their healthy growth into the next century.

So our task is just beginning. We look forward to working with you, and in that spirit I welcome your questions.