Testimony Presented By Texas Deputy Banking Commissioner Randall S. James To The Texas House Of Representatives Subcommittee On Internal Consumer Protection Austin, Texas

Date: March 11, 1998

SUMMARY OF INTERNET BANKING TESTIMONY

Internet banking is expanding at a rapid pace, as it offers financial institutions an opportunity to expand markets without incurring substantial additions to overhead.

Banks use technologies (such as digital signatures) to allow the Internet to be used for secure electronic commerce transactions. But, these are not necessarily used by all providers, and there remain possibilities for breeches and compromises of controls. Due to the open nature of the Internet and the rapid pace of change, risks such as disclosure of confidential information, identity theft, and outright fraud, remain important considerations.

A new industry of "authenticators" has emerged to play a role in verifying and encoding Internet messages. There is debate regarding the extent to which authentication technology or providers should be regulated.

Federal banking regulators and the Conference of State Bank Supervisors (CSBS) have initiated activity to ensure that Internet banking systems are operated safely and soundly. Also, a joint interagency pilot project is slated to track down fraudulent depositories operating on the Internet, and refer these to law enforcement authorities for prosecution.

Although many states have passed legislation related to electronic commerce, the development of a patchwork of conflicting rules and protocols is considered a threat to global trade and could ultimately trigger preemptive federal legislation. Recent court actions have overridden some states' efforts. Federal legislation has been filed to address certain aspects of electronic commerce. But one of the most promising efforts is that of the National Conference of Commissioners on Uniform State Laws (NCCUSL), which is drafting model state legislation to provide interstate consistency while maintaining state jurisdiction over commerce.

Considerations for future action include consumer education efforts, establishment of funding for strategies to monitor the Internet offerings, and possible new legislation to enhance law enforcement over electronic activity.

Overview of Internet Banking

Internet banking can be categorized into three distinct levels: information-only systems (which only allow access to marketing or other publicly available material on a bank); electronic information transfer systems (which provide the ability to transmit messages, documents or files

such as loan or deposit account applications); and electronic payment systems (wherein payments from bank accounts can be transacted). Because of the relatively low cost (approximately $50,000 for an interactive web site), Internet banking is an especially attractive means for community banks to expand their market without constructing new branch locations. An informal tally maintained by the FDIC indicates that there are currently 139 banks in the United States offering Internet banking, with many of these being community institutions. (Attachment I) Banks have been extremely cautious to ensure that their Internet systems are secure and controlled.

I. Risks to Consumers

The Internet is inherently insecure. By design, it is an open network which facilitates the flow of information between computers. Unless adequately controlled, the risks of Internet banking include the disclosure of confidential information, identity theft, and outright fraud. Banks use technologies (such as digital signatures) to allow the Internet to be used for secure electronic commerce transactions. But, these are not necessarily used by all providers, and there remain possibilities for breeches and compromises of controls. Some protection is available to consumers through the federal Electronic Fund Transfer Act, which limits consumer liability on unauthorized electronic debits from their bank accounts. The following are the most commonly cited concerns with Internet banking:

A. Data Privacy and Confidentiality

Unless protected, data is susceptible to being monitored or read by others when it is being transferred or when it is stored in a connected system in a bank, including a network drive. "Sniffer" programs can be set up at opportune locations on a network, like web servers (i.e., computers that provide services to other computers on the Internet), to simply look for and collect certain types of data. Data collected from such programs can include account numbers (e.g., credit cards, deposits, or loans) or passwords. Access to this information can allow criminals to duplicate the identity of the consumer, and thus initiate electronic transactions at the consumer's expense, obtain loans in the consumer's name, etc. (See Attachment II)

B. Data Integrity

The open architecture of the Internet can allow those with specific knowledge and tools to alter or modify unprotected data during a transmission. The risk to the consumer is that an unauthorized party may change the amount of an electronic transaction, or redirect a funds payment.

Unprotected bank account data could also be compromised within the data storage system itself, both intentionally and unintentionally, if proper access controls are not maintained. Therefore, bank records could become inaccurate if unauthorized parties tamper with transaction information accessible to potential Internet intrusion.

C. Fraudulent Depositories

With the ease of creating a web page, any person or entity can solicit unsuspecting consumer dollars into "high-earning deposit accounts." The requirements of existing commercial law would generally preclude a consumer from opening a deposit account and making an initial deposit over the Internet, due to the need to obtain a signature on the account agreement. Yet,

because the account holder may not be aware of his or her protections under the law, there is anecdotal evidence that consumers are being swindled into transmitting money to unauthorized and/or uninsured "banks."

D. Authentication

Without a means of authenticating the identity of each of the parties to an electronic transaction or inquiry, both the bank and consumer have a risk of dealing with an unauthorized party. For example, through a variety of techniques generally known as "IP spoofing" (i.e., impersonating), one computer can actually claim to be another. User identity can be misrepresented as well. Thus, equipped with the right information, it would be relatively simple for an unauthorized party to represent itself as an account holder to a bank. Similarly, a hacker could redirect a consumer contact to a duplicate "shadow" site of a bank web page, and thus intercept confidential transmissions.

II. Security Measures

Due to their closed and secure nature, private electronic networks with limited applications, such as ATMs, have successfully existed with limited security, generally a simple PIN number. However, much stronger security is needed to transact commerce on the Internet. Since there is no central authority on the Internet to assign passwords or PIN numbers to control access or authenticate use, third parties have arisen to offer the service of certifying the identity of each party and scrambling the message to ensure that it cannot be read by any unauthorized eavesdroppers.

Methods for electronic authentication include digital signatures, retina and facial scans, and fingerprint identification. Of these, digital signatures are the most widely used as a means of both authenticating the parties to the transaction/message, and encrypting the information. A digital signature is a coded message that is assigned to a particular individual, entity or machine for the purposes of communicating electronically. Through a highly complex data encryption process offered by the intermediary, an electronic message is "hashed" and "signed" by the transmitter using a private key. Upon receipt, the recipient uses a public key to authenticate the identity of the sender and descramble the message.

To the extent that the authentication service effectively introduces a new set of participants into the payment system, there is some uncertainty regarding the regulation of these entities and their obligations to banking customers. Can certificates of authentication be obtained through the Internet, or must a party present themselves in person to some authority to verify their identity? What sort of standards should be imposed, if any, to provide public assurance of the authenticator's ability to stand behind their obligations? A subsidiary of Zion's Bancorp in Utah recently obtained approval from the Comptroller of the Currency to act as a certificate authority, i.e. to issue, store and certify digital signatures. (Attachment III) Some in the banking industry believe that banks can use their core competencies in security, data management, and telecommunications to branch into authentication activities, which would assure them a seat at the table of electronic commerce.

III. Regulatory Initiatives

Federal banking regulators and the Conference of State Bank Supervisors (CSBS) have initiated activity to ensure that Internet banking systems are operated safely and soundly. Also, a joint interagency pilot project is slated to track down fraudulent depositories operating on the Internet, and refer these to law enforcement authorities for prosecution.

A six-month Interagency Internet Monitoring pilot program will be initiated in April 1998 to identify and prevent bank-related fraud on the Internet. The pilot program combines the forces of CSBS, the FDIC, the Comptroller of the Currency, and the Office of Thrift Supervision, and consists of an organized "surf and destroy party." Regulators hope that efforts such as these will discourage fraudulent banking activity on the net. The Federal Trade Commission has a similar Internet Monitoring Program aimed at identifying fraudulent marketing schemes and con games.

The Department of Banking has the authority to cooperate with other state and federal authorities in the effort to curtail improper Internet activity. However, we are not currently funded nor staffed to participate in a meaningful way. Should any person or entity located in Texas be detected as offering unauthorized banking on the Internet, under Subchapter C of the Finance Code the agency is empowered to investigate and refer the entity to the State Attorney General for prosecution.

Electronic Banking examination procedures were adopted in mid-1997 by the FDIC to assess the adequacy of control systems in banks offering Internet access. These procedures are employed at every bank offering Internet banking (including phone banking) during each regularly scheduled commercial examination. Banks which offer interactive Internet banking are also reviewed by the FDIC's Information Systems examiners. These reviews have been important in identifying potentially weak or compromised systems.

Numerous regulatory web sites offer excellent information to consumers to assist in avoiding Internet fraud. The FDIC's site (www.fdic.gov/) contains a searchable list of insured banks which consumers can use to verify the existence of an institution operating on the Internet. The Federal Trade Commission's home page (www.ftc.gov/) contains tips advising consumers how to avoid scams operated on the Internet.

IV. Legislative Initiatives

A tension exists between those concerned that electronic commerce requires better definition of jurisdictions, obligations, and authorities, and, those concerned that technology-specific legislation will effectively impair the development of Internet commerce.

Presently, all commerce in the U.S. is subject to state contract law, commercial law and administration of justice under state rules of evidence. According to Ben Wright, the editor of the EDI Forum: The Journal of Electronic Commerce, even in the absence of special state legislation, state law generally allows for electronic signature and authentication methods.

The federal government is proceeding very cautiously, and has declined to regulate Internet commerce at the current time. A number of individual states have stepped into the void and attempted to impose standards on some aspects of electronic banking, most commonly

addressing registration requirements and standards for electronic authentication. This effort has been generally ill-received by the industries engaged in electronic commerce due to concern that it is exceedingly difficult to monitor and comply with conflicting standards in the global arena of the Internet. Several federal bills are under consideration which would establish varying degrees of standards for electronic commerce, and which could preempt any conflicting state statutes.

In the meantime, the industry is working to adopt voluntary shared protocols to ensure that developing technologies can work harmoniously. MasterCard, Visa and the Bank of America recently announced that they are voluntarily limiting the amount of liability for debit cards to that of credit cards, which is $50. In addition, Visa and MasterCard have put together a secure electronic transaction protocol ("SET") which uses electronic authentication.

The following is a summary of broad federal and legislative initiatives:
In July 1997, the White House issued a Report on Electronic Commerce. Among other things, the report identifies "five principles to guide government support" of electronic commerce. These are: 1) The private sector should lead the development of the Internet as a free and open marketplace; 2) Governments should avoid undue restrictions on electronic commerce and should refrain from imposing new and unnecessary regulations, procedures, taxes or tariffs on this activity; 3) Government should support a minimalist and simple legal environment for electronic commerce; 4) Governments should recognize the unique qualities of the Internet in framing any necessary regulatory regimes; and 5) Electronic commerce should be facilitated on a global basis so that to the greatest extent possible, the legal and commercial framework for activity is consistent and predictable, regardless of the jurisdictions in which buyers and sellers reside.

The Treasury Department has created a Consumer Electronic Payments Task Force, which has held several public meetings.

The National Conference of Commissioners on Uniform State Laws (NCCUSL) has a Uniform Electronic Transactions Act (UETA) project underway. The UETA is scheduled for a first reading before the full body in August 1998 and a final reading and approval in August 1999. The goal of NCCUSL is to maintain electronic regulation at the state level while still ensuring consistency through the creation of model legislation. A draft bill addresses the applicability of other laws and the responsibility for a loss due to the use of commercially unreasonable security procedures.

Approximately 20 states have passed laws relating to electronic commerce. Most recognize a digital signature, create presumptions and apportion liability. Utah recently passed a highly prescriptive state law on the subject, which provides for licensing of certification authorities and sets detailed standards for implementing regulations. The more recent trend in other states does not specify one particular technology as necessary to create a legally enforceable electronic signature, nor does it create statutory government intervention in liability apportionment between parties. Two recent federal court decisions overruled state regulation as conflicting with the Constitution's Commerce Clause.

As of March 5, 1998, the following federal bills had been filed relating to Internet banking: Senate Bill 1594 by Senator Bennett: to amend the Bank Protection Act of 1968 for purposes of facilitating the use of electronic authentication techniques by financial institutions and for other purposes.

House Resolution 2937 by Representative Baker: to provide for the recognition of digital and other forms of authentication as an alternative to existing paper-based methods, to improve efficiency and soundness of the Nation's capital markets and the payment system, and to define and harmonize the practices, customs, and uses applicable to the conduct of electronic authentication and for other purposes. This bill would establish the National Association of Certification Authorities (NACA), an organization modeled after the National Association of Securities Dealers, and under the jurisdiction of the Secretary of the Treasury. Membership would be required by all providing electronic certification services. Liability of consumers and certification authorities, standards, and codes of conduct would be established by this national body.

House Resolution 2991 by Representative Eshoo: to enhance electronic commerce by requiring agencies to use digital signatures, which are compatible with standards for such technology used in commerce and industry, to enable persons to submit Federal forms electronically. This bill would require that all federal forms be available over the Internet and allow for the filing of federal forms over the Internet. The bill also creates some national uniformity for the use of digital signatures but defers to state law in many areas.

Senate Bill 874 by Senator Faircloth, House Resolution 3099 by Representative McNulty, and House Resolution 156 by Representative English to amend title 31, United States Code, to provide for an exemption to the requirement that all Federal payments be made by electronic funds transfer.

Italy, Germany and Malaysia have recently passed national digital signature laws addressing the licensing of certification authorities.

The United Nations Commission on International Trade Law is in the process of drafting model international digital signature legislation.

The European Union released in October a policy communication suggesting that the European Commission will be developing legal uniformity for digital signatures.

V. Options for Future Action

Consumer education efforts are necessary to limit the amount of potential losses through fraudulent activity. Initiatives to alert citizens against fraud through designated web sites or consumer brochures may be worthwhile. The Legislature may also consider funding strategies to study or monitor Internet offerings.

Another option for future action would be the promulgation of laws providing more specific authority to investigate and refer apparently illegal Internet activity. Laws could also be

established to provide for penalties against perpetrators of fraud or theft over the Internet. The Department is available to assist elected officials in any of these tasks.

Testimony of Randall S. James
Deputy Banking Commissioner
Presented to the House Subcommittee on Internal Consumer Protection March 11, 1998