NCUA LETTER TO CREDIT UNIONS

NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street, Alexandria, VA 22314

DATE: July 2004 **LETTER NO.: 04-CU-09**

TO: Federally Insured Credit Unions

SUBJ: ATMs: Triple DES Encryption

ENCL: Triple DES

DEAR BOARD OF DIRECTORS:

The purpose of this letter is to ensure credit unions are aware of the new minimum encryptions standards being required by the major ATM switch network vendors. The new encryption standard, called Triple DES (3DES), was adopted by MasterCard and VISA to ensure the security of their networks. Eventually, all ATMs connected to the networks must be capable of handling the new encryption standard which uses 2 encryption keys, chosen independently at random, to encrypt a message multiple times.

The original data encryption standard (DES) that has been universally used since 1981 in the ATM market to encrypt personal identification numbers (PINs) is vulnerable to attack because of the exponential increase in computing power from personal computers. In addition, the ATM market is moving towards transacting business over the Internet, which brings its own set of risks.

Since April 2002, all new ATM installations were required to be 3DES capable. The primary issue is migrating the thousands of legacy (old but in current use) ATM machines across the country to the new standard. In many cases, upgrades in the software and keypads will make them compliant. In other cases, the machine will need to be replaced. Costs associated with the conversion/upgrade vary depending on the ATM vendor and age of the machine.

The primary responsibility for ensuring compliance with the 3DES requirement, by the published dates, rests with ATM vendors and individual owners. However, because of the potential systemic risk posed by some ATM owners' failure to upgrade, or replace, their legacy systems and the resulting possible loss of service to members, credit unions should be proactive in meeting the migration deadlines (see enclosure, section III, The Migration).

Should you have any questions or concerns, please contact your NCUA Regional Office or State Supervisory Authority.

Sincerely,

/S/

JoAnn Johnson
Chairman

Enclosure

TRIPLE DES

I. **HISTORY** – The original data encryption standard (DES) was standardized in 1981 for the encryption of sensitive or personal information such as personal identification numbers (PINs), customer account numbers, and balances. This mathematical algorithm uses a 56-bit key length to encrypt and decrypt data providing approximately 72 thousand-million-million values for any single DES key.[1] In 1999, a computer called DES Cracker was built that used the combined strength of nearly 100,000 personal computers to crack the key in under two days.

II. **THE NEW STANDARD** – Triple DES, on the other hand, uses two keys and specifies three rounds of encryption; increasing the key length to 168 bits. It is not feasible – now or in the near future – to search the individual bits of the Triple DES key in order to crack the code.

III. **THE MIGRATION** – The financial ATM network includes host processors, switches, and the individual ATM or point-of-sale (POS) terminals connected to the network. For the entire system to be secure, the Triple DES standard must be utilized from the top down. Mastercard and VISA recognized this requirement in the 1990's and started migrating towards that end. The individual ATMs are just one part of the system to be overhauled – but it is the one part that is the most geographically dispersed and in the hands of multiple, individual owners such as credit unions, banks, and small regional networks. To facilitate the upgrade process, implementation dates were established for the major network players as noted in the following table (shaded dates have already passed):

Network	Host to Network	Existing ATM Installations	New ATM Installations	End to End Processing
CO-OP Network	Apr 1, 2004	Dec 31, 2005	Dec 31, 2003	Dec 31, 2005
Mastercard	Apr 1, 2003	Apr 1, 2005	Apr 1, 2003	Apr 1, 2005
VISA	Jan 1, 2004	Jan 1, 2003	Jan 1, 2003	Jul 1, 2007
STAR	Jun 30, 2004	Dec 31, 2005	Jun 30, 2003	Dec 31, 2005
NYCE	Dec 31, 2004	Dec 31, 2005	Jun 30, 2003	Dec 31, 2005
PULSE	Jun 1, 2005	Dec 31, 2005	Dec 31, 2005	Dec 31, 2005
ACCEL/Exchange	Jun 30, 2005	Dec 31, 2005	Dec 31, 2005	Dec 31, 2005
Shazam *	Unknown	Unknown	Unknown	Unknown

* None of the sources reviewed could verify the Shazam network's implementation dates.

** Table reprinted from "Managing ATM Capital Investments" CO-OP Network, December 2003

[1] Colette Broadway, Project Manager, Thales e-Security, in "Triple DES Dare You", ATM Marketplace.com, October 13, 2003

IV. **IMPACT TO CREDIT UNIONS** – Credit unions who purchased ATM machines before the original 2002 Triple DES requirement will have limited options – mainly to upgrade or completely replace the legacy system. The following upgrades must be made:

a. Software – An upgrade to the ATM's operating software allowing it to communicate using the Triple DES standard. A memory upgrade will also be needed in most cases.
b. Encrypting PIN Pad (EPP) – A new self-contained keypad for customers to enter their PIN number. The new keypad encrypts the PIN within the keypad before it gets transmitted. In legacy systems, the unencrypted PIN number traveled to another part of the ATM machine to be encrypted leaving the line vulnerable to "wiretapping." The new keypad is also outfitted with antitheft and tampering security to render it useless if removed from the ATM.
c. Voice Response – Although not part of the Triple DES issue, one probable new requirement by the Americans with Disabilities Act (ADA) is the installation of voice modules to assist blind users in the operation of the ATM.

Costs range from a low of $1,000 for upgrades to almost $35,000 for a new ATM.[2] As of the end of 2003, credit unions owned a reported 20,000+ ATMs.

On another note, the vast majority of ATMs and network controllers run IBM's old OS/2 operating system. IBM recently announced it would no longer support OS/2 past December of 2006. ATM manufacturers, while dealing with the Triple DES requirement, must also move their products to the Microsoft Windows environment. Ideally, the operating system upgrade will occur at the same time as the Triple DES upgrade.

This move towards open-architecture software (Windows) also requires changes in the ATM's traditional network communication infrastructure. The older communication languages (protocols) do not support modern functions that make ATMs interactive such as touch screens, video, and vocal instruction. TCP/IP, the protocol used by the Internet and personal computers, supports these functions and allows ATMs to be connected to local and wide-area networks.

Benefits of the new operating system include redundant communication paths and reduced costs in both management and deployment (no more leased lines or dedicated circuits). ATM owners can connect their ATMs directly to existing computer networks and manage them more effectively.

The major drawback, as with the Internet itself, is security. Firewalls, secured servers, and other measures such as virus protection are critical. In August

[2] CO-OP Network, December 2003

2003, the Nachi worm infected several Diebold ATMs.[3] Outbound traffic from the infected machines stopped, thus resulting in an inconvenience to customers. The cause of this event was determined to be that a security patch wasn't loaded on the ATMs even though it was available for over a month.

Patch management, virus pattern updates, security assessments, and firewall/router protections are now concerns that must be expanded to include the ATM system. Transaction, strategic, and reputation risks all increase exponentially for credit unions deploying these TCP/IP-based machines.

V. **CONCLUSION** – Credit unions, along with other ATM or network owners, are faced with a mandatory upgrade. If a credit union chooses not to upgrade, their legacy ATMs will eventually no longer be able to communicate with the host or network system, thereby rendering them useless.

Additionally, credit unions must ensure they review, and revise as necessary, their policies, procedures, and practices to address the added risks involved with new or existing deployments of Internet-based ATMs.

[3] "Nachi worm infected Diebold ATMs" by Kevin Poulsen, The Register, Tuesday, November 25th, 2003