

white

MAINTAINING
YOUR DATA:
INTERNET
SECURITY

PRESENTED BY THE
TECHNOLOGY COMMITTEE OF
THE ELECTRONIC TRANSACTIONS
ASSOCIATION
MAY 2001

paper



ABOUT THE ELECTRONIC TRANSACTIONS ASSOCIATION

The Electronic Transactions Association (ETA) is an international trade association representing companies offering electronic transaction processing products and services to merchants within the acquiring industry. Members include financial institutions, independent sales organizations and manufacturers/distributors of software, equipment, and point-of-sale devices. ETA was established in 1990 to influence policy within the industry by providing leadership through education, advocacy and the exchange of information.

For additional information, please contact:

Electronic Transactions Association
14 West Third Street, Suite 200
Kansas City, MO 64105
800.695.5509
816.472.7765 fax
www.electran.org

ACKNOWLEDGEMENTS

The Electronic Transactions Association recognizes the following committee members responsible for the development of this document.

Michael Cottrell
Vice President, Market Strategies
Vital Processing
Phoenix, AZ

James Richards
Chief Technology Officer &
Senior VP, Software Development
CardSystems
Tucson, AZ

Acknowledgement also is given to the following individual who provided additional research, input and services.

Sheila Navis
Associate Director
Electronic Transactions Association
Kansas City, MO

For other resources & additional information, visit the following Web sites

www.visa.com
www.mastercard.com

CONTENTS

A WHITE PAPER ON INTERNET SECURITY	4
The needs for security	4
Basic approach	4
Identifying the assests...What am I trying to protect?	5
Identifying the threats	6
TOP 10 LIST OF PROACTIVE SECURITY MEASURES	7
TOOLS FOR INFORMATION SECURITY	8
Firewalls	8
Encryption	10
System Audits	11
Physical Security	11
CONCLUSION	12
GLOSSARY OF INDUSTRY TERMS	13

ELECTRONIC TRANSACTIONS ASSOCIATION
COPYRIGHT © 2001
ALL RIGHTS RESERVED

DISCLAIMER

This White Paper was prepared by members of the Technology Committee of the Electronic Transaction Association (the “Committee”) and reflects the Committee’s interpretation of relevant credit card association rules and regulations. This White Paper is for general informational purposes only and the committee recommends that the ETA membership consult directly with the appropriate credit card association with specific questions regarding the interpretation of any Visa or MasterCard rule or regulation.

A WHITE PAPER ON INTERNET SECURITY

With the rapid explosion of e-commerce and the Internet as a serious business tool, a lot of attention has been given to “information security.” Helping businesses securely manage information has become a multi-billion dollar industry. Companies such as Verisign®, Microsoft®, Cisco®, Oracle® and SUN Microsystems®, to name a few, all spend a significant amount of time and money developing their services with security in mind.

With such a widerange of companies engaged in the information security business, it begs the question, “What exactly is security?” Security means different things to different people depending on their age, position within a company or access to “top secret” information.

If you were Charlie Brown and asked Linus what security was, he’d wave his blanket at you. Asking that same question to a CEO of a company might yield a response such as “Security at ACME Products revolves around protecting our patented products, source code, the lives of our personnel and the vested interest of our stockholders.” In trying to analyze this statement, Linus’ security blanket begins to look really attractive.... it covers everything.

For purposes of this document, rather than describe what security is, we’ll discuss the needs that security should fill. We’ll address the need for physical security, background checks, firewalls, access codes, tokens and other methods all designed to protect one’s information. In general, the need for security can be summed up as follows:

The needs for security

1. Keep outsiders from entering the organization and gaining access to sensitive or private information. Access can be gained physically or virtually.
2. Prevent unauthorized information from leaving the premises.
3. Monitor and control internal employees’ access to information and systems.

Basic approach

The first step in developing a security policy is recognizing the need for one. To begin designing the policy, it is important to first determine what the policy should cover. Additionally, the policy should be integrated and cohesive with existing organizational policies within the company.

In general, by asking yourself the following questions, you should be able to determine how robust your security system needs to be, as well as ensure that the security yields cost benefits.

1. What am I trying to protect?
2. From what and whom do I need to protect it?
3. How likely are the threats, and what are the consequences if they happen?
4. Can the assets be covered in a cost-effective security manner?
5. And finally, have I reviewed the process and improved any weaknesses?

Once you have the answers to these questions, you can begin designing an information security process. The process should take into consideration that information is valuable to your company and that you have exclusive right to the information. The information and systems must be protected from fraud, disclosure, and intentional misuses. Additionally, the data and software must be securely stored and guarded. The policy should define accountability for information at each employee level.

The security policy developed must conform to existing policies, rules, regulations and laws to which the organization is subject. Another important element that often is overlooked is the value of collaboration when designing policies. A security policy should be a joint effort by technical personnel who understand the full ramifications of the proposed policy and the implementation of the policy, and by the decision makers who have the power and responsibility for enforcing the policy. Without the joint development process, the organization risks implementation of a process that is neither enforceable nor useable.

Identifying the assets, what am I trying to protect?

Part of a risk analysis involves identifying all things that need to be protected. Some things are obvious, like the various pieces of hardware or cardholder data. Others are apt to be overlooked, such as people who actually have access to the systems. It is essential to list all things that could be affected by a security problem or potential threat. A list of categories should include:

1. Data. Stored online, archived off-line, backups, audit logs, databases, in

transit over a communication media, during execution, and during delivery (physical or otherwise). This can include cardholder data, merchant specific data, ACH files, contract information, rate information, contact information, etc.

- 2. Supplies.** Paper, forms ribbons, magnetic media.
- 3. Hardware.** Including CPUS, keyboards, terminals, terminal servers, routers, firewalls, disk drives, communication lines, printers, personal computers, laptops. This should include not only the hardware used for actual processing, but also the hardware used to view data and access the data. This might also include hardware systems used for access to the facilities and systems (tokens or smart cards).
- 4. Software.** Often includes source programs, utilities, backup operating systems, communication programs, object programs, source code itself, web content and e-mail systems.
- 5. People.** Users of the systems, people needed to run systems, contract personnel for hardware and software. The U.S. Department of Commerce lists insiders as the number one threat to information.
- 6. Documentation.** Documentation often is overlooked, but should include documentation of programs, hardware, systems, local and remote administrative procedures.

After identifying all of the assets, assign a value to them according to loss of business, contract obligations and legal ramifications should the assets be compromised. Sometimes it helps to assign a monetary value, however, this is not necessary for each item. Once ranked in a matrix, the next step is to identify the threats to the assets.

Identifying the threats

When examining the possible threats, a business should consider both internal and external sources. The threats should be examined with the perspective of what the potential loss might be according to the protected assets.

A common threat is disclosing information. It is necessary to determine how valuable and sensitive the information stored on the computer systems is. This could be a pricing proposal, a technical paper or perhaps guides to future product development market initiatives. Consider placing passwords and encrypting potentially valuable information. How many computers in businesses today, using only a basic password, contain access to this sort of valuable data? Unfortunately too many businesses ignore this easy-to-implement practice.

One of the most common threats is unauthorized access to computing facilities. Unauthorized access is the use of any computer resource or facility without prior permission to use those resources that can take place in a variety of ways. One way is by the use of another person's account to gain access to a system, facility or application.

Perhaps one of the greatest threats to recently emerge is the denial of service. Everyone is familiar with the recent attacks on ebay or Yahoo where repeated attacks from thousands of computers forced the sites to shut down. Another high profile example is the "I Love You" virus that affected hundreds of thousands of systems worldwide. The impact ranged from a minor inconvenience at the mail server, to absolute shut down of corporate systems. Both examples show the importance of protecting systems and businesses against these types of attacks and the potential for monetary impact. Each business has its unique needs and should determine which services are essential, and for each of the essential services, determine the effect to the service or productivity should that business portion become disabled.

TOP 10 LIST OF PROACTIVE SECURITY MEASURES

1. Security Policy

Develop a security policy. This will limit liability exposure and is the basis for applying appropriate security to the enterprise telecommunications infrastructure.

2. Security Awareness

Implement a strong security awareness, training and education program.

3. Monitor Access

Know who, when, why and how users are accessing your systems.

4. Routine Backups

Routinely back up all systems, store backups off-site and test the backups.

5. Integrity Checks

Run system integrity checks and compare using off-line encrypted checksums.

6. Check Reusable Passwords

Routinely scan for bad passwords, or better force the use of good passwords. Consider using one-time passwords or handheld tokens for authentication, especially over the Internet.

7. Audit

Don't just audit, but use the audit data for intrusion detection by audit reduction and analysis.

8. Secure Mobility

Encrypt all data on laptops leaving the premises.

9. Physical Security

Physically secure all laptops, desktops, servers and peripherals after business hours.

10. Limit Access

Limit Internet access to those with a real need.

TOOLS FOR INFORMATION SECURITY

Firewalls

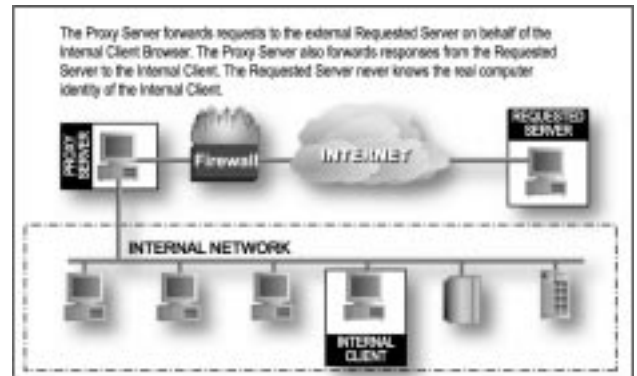
Remember the good days when a firewall was something you found in the front of your Chevy. Well, in today's high-tech world, a firewall serves the same purpose, but for a network. Much the same as a firewall is put in a car to provide a point of resistance to a burning or hot engine, a firewall on a network performs the same type of functionality for a computer system.

There are three main types of firewalls: 1) a packet filter, 2) a hybrid or 3) a proxy. A packet filter firewall examines each IP packet crossing the network, and based upon a set of rules, either lets the packet through, or denies access. A proxy firewall actually acts as a secure gateway between networks.

The proxy authenticates data and allows only specific information to enter or leave the secure side of the proxy. Often times, proxy servers are referred to as application level firewalls, protecting the network (inbound or outbound) depending on the specific application in use. Proxy firewalls are one of the most secure.

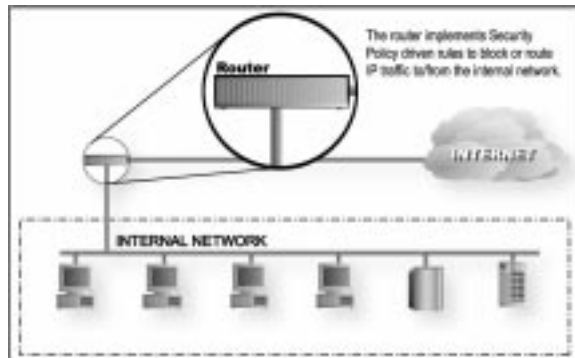
For that reason, administration of a proxy firewall can take special skills and discipline in keeping it accurate. The third type of a firewall actually is a hybrid between the two, providing the functionality of the packet filter with an increased security level found in a proxy.

A proxy firewall works much the same as a packet filter, except that a host would be in place between each of the stations desiring access to the Internet or outside services. This often is referred to as a dual-homed host architecture. The proxy server doesn't always forward users' requests to Internet services; it controls what users do because it makes decisions about the requests it processes based on the company's security policy. Additionally the proxy server can control what access comes in to the network. A proxy service sometimes is more of a software solution, and not necessarily a firewall architecture per se. Below is a diagram showing a proxy service in place with a dual-homed host.



A proxy diagram

A packet filter diagram



According to Visa's Cardholder Information Security Program, a firewall mechanism is to be put into place so that all electronic cardholder data is protected from unauthorized access during all phases of its life, from generation to destruction, and to ensure that it cannot be compromised, released to any unauthorized entity or otherwise have its confidentiality or integrity placed at risk. The firewall mechanism must be built and maintained using the model of least privilege. All access is to be on a need-to-know basis, and more importantly, all access to cardholder data will be restricted to personnel who need to access said data to perform their stated job function only.

Management of system passwords

Going back a few years, employees used secret handshakes and code words to identify their right to use facilities or enter a building. Alpha bravo five, left shake right shake four finger dribble provided access to every trade secret in the organization. This age-old tradition actually is still in place today, just in a different format. Now, systems and applications can assign, log and track an employee's access to the network or facility by use of passwords and system identification numbers.

Each employee, contractor, or vendor accessing an organizations system should have a unique user ID and a private password. In addition, personnel needing access to systems, building infrastructure, networks and applications that access data in the organization should have prior written approval from an appropriate manager or supervisor. Requests for changes to account access also should follow established written procedures. Some common guidelines for password management include:

1. Avoid dictionary words.
2. Use both numbers and letters.
3. Difficult passwords that cannot be remembered.
4. Easily guessed names, such as a street address or product name.
5. Change passwords every few weeks — don't allow users to re-select previous passwords.
6. If a user has multiple attempts to sign on with an incorrect password, block all access after a certain number of tries.

One of the simplest tools to implement with passwords is a shutdown of the application after a certain period of inactivity, say five minutes. This is critical for applications containing cardholder data. This way if a user unexpectedly steps away from the worksta-

tion, the system is not left vulnerable for a lengthy period of time. Additional measures should include training personnel to log off of the system when leaving the workstation.

Another method of authenticating users that is catching on rapidly is the use of a token or a physical device to validate the user's identity. The most popular are smart cards. When users sign into a system, they are asked for a password, in addition they are prompted to insert a smart card. The system then validates both the smart card and the password prior to allowing the user to continue the session.

Other authentication methods use the human body as a token. This is most often referred to as biometrics. Biometrics serves as a gatekeeper of confidential information where authentication and the personal security of remote users are essential. Biometrics is the ultimate password replacement. The question a password seeks to answer is, "Does this user possess the right information?" With biometrics, the fundamental question that is answered is, "Is this the right person?" Biometric authentication methods include fingerprint validation, iris scans, voice recognition and other non-invasive methods to validate unique aspects of the user. Again, as with smart cards, the user can (at the discretion of the security policy) be required to supply a password that works in conjunction with the biometric scan.

To gain the most out of passwords and token systems, establish multiple controls and levels for the passwords. With a password or smart card, it becomes easy to limit where an employee can go on the network. While many persons in the organization need cardholder information, many do not. Passwords protect or re-

quire secure authentication from users prior to allowing access to applications that provide this data.

Encryption

Encryption is an important tool in that even if other controls such as passwords or firewalls are compromised, the data is still unusable. Data Encryption Standard (DES) is perhaps the most widely used data encryption mechanism. In a nutshell, DES uses an algorithm and a key value to take plain text and encrypt the data. Another encryption method is Secure Sockets Layer (SSL) that often is used to transmit data in a secure method over the Internet.

Several types of encryption packages are available on the market today. They range from complex software solutions to external hardware encryption devices (such as Atalla or Racal encryption devices). While both serve similar purposes, hardware encryption devices typically are much faster than a software solution. Many common software packages provide encryption tools for use by the operator or author when storing data or saving files.

Perhaps one of the main advantages to encryption is that only machines or operators in possession of the key can restore the encrypted text to a readable format. When providing access to keys, the user should be instructed not to write the key down or keep it in a physical place close to the secured data.

When using cryptographic keys to store cardholder information, or to access cardholder information, it is vital that the integrity of the keys not be compromised. For this reason, whether it is Personal Identification Number encryption, or PIN pad encryption processes, key management controls should be implemented. The key management controls should be clearly

defined, written and audited on a regular basis.

A complete listing of key management requirements are available from the card associations, online debit networks and card brands. Key management processes should consider implementation of the following information gathered from both Visa and MasterCard.

1. Random Key Generation

Any keys that are generated are generated on a random basis to ensure it is not possible to predict the outcome of a certain key set. Additionally, keys should be unique between entities.

2. Access to keys

Available on a need-to-know basis. A limited number of key custodians in as few of locations as possible.

3. Key Forms

Cleartext, cleartext within a cryptographic device, cleartext with separate components and custodians using split knowledge, and cleartext asymmetric public keys.

4. Dual Control

A single custodian should not have the ability to utilize or see more than one cleartext key component. Two or more entities should operate together to protect sensitive information.

5. Audit Trails

Audit trails should exist for the life of a key or key component. These should include enough data to enable a complete reconstruction of all key management activities including when, where, why and by whom.

6. Documentation

All processes and procedures for key management and exchange should be documented.

7. PIN Pad Injection

PIN pads should be stored and injected according to the guidelines of the associations/brands for which the PIN pads will be processing transactions. PIN injection and storage processes should be part of an annual audit.

System Audits

Nearly all businesses undergo a financial audit on a regular basis. An audit of the security policy in place is just as important. During the security audit, the organization should review any policies that concern system security, as well as the processes and procedures put in place to enforce them. While it is not always necessary to have “fire” drills, it is recommended that as part of the ongoing security policy, organizations perform random testing of mission critical components.

Physical Security

Many organizations processing card information have physical security controls in place for entry into the operations building where information is kept. The typical scenario involves issuing of badges that must be swiped or presented to enter the building. Additionally, once inside the main building, administrators can determine where in the building the person can have access by requiring badges at doors to different areas of the building. For instance, an employee answering calls at a help desk probably doesn't need access to the computer operations data center. However, this employee might need access to the file room containing original merchant setup information. This access should be administered and monitored on a daily basis. Changes to access should require written approval from the employees immediate supervisor and possibly require approval from other entities (such as security or information technology).

While many organizations are good at implementing security at the head office, many neglect to implement the same types of controls at the remote sales offices or facilities beyond the main operations center. Remote sales offices tend to be a little lax in their implementation of security procedures. While it may not be necessary to require a badge system at a small office, consider other physical controls in the office. Require that items such as CDs, diskettes and laptops be secured when not in use. When sending reports to remote locations, don't include cardholder information on the reports or allow copying and printing of sensitive material at these sites.

A common mistake made with cardholder information is the improper destruction of cardholder data. Printed reports, microfiche or other media containing cardholder information should be destroyed in a secure manner prior to disposal. This could include shredding, incineration or other commercially accepted methods for secure data destruction.

CONCLUSION

After taking a look at many tools and options available for security, there are a lot of similarities between a security policy and Linus' security blanket. The fiber that makes up the blanket consists of the many tools and services used in a security policy; the firewalls, biometrics, passwords, access controls and documentation all are combined to cover the assets of the company. Along with the fiber that makes up a blanket, there also is a border that holds it all together, making it easy to unfold and use. For a security program, the border consists of common sense, a return on the security investment and diligence in implementing and operating the security program. Programs that are bound too tight or are created in a convoluted manner actually might end up being a detriment to the company. Security plans should be reviewed regularly, easy to use and enforceable throughout the organization.

GLOSSARY OF INDUSTRY TERMS

A

APPLET: A small program that can be transported across a network that can then run on the receiving computer to perform a specific function.

APPLICATION PROGRAM: The computer program that performs a data processing function rather than control function.

ASYNCHRONOUS: A data transmission that involves the generating and transmitting of characters, that have a specific start and stop sequence associated with each character. This transmission does not require a separate clock signal for the reception of data.

AUTHENTICATION: In security, ensuring that the message is genuine, that it has arrived exactly as was sent, and that it comes from the stated source.

B

BYTE: A single unit of information, such as a letter, number or other character. A byte is made up of eight bits. Through arrangement of the bits 0 and 1 values, the byte may express any of 256 characters. In addition, there may be a start bit to indicate the end of a word.

C

CYBERSPACE: Refers to any number of on-line sources: the Internet, bulletin board systems, or commercial on-line services.

D

DATA: Digitally represented information that includes voice, text, facsimile and video.

DATA ACQUISITION: The process of identifying, isolating and gathering source data to be processed in a usable form.

DATA BASE: A collection of records stored electronically.

DATA CAPTURE: A data processing term for collecting, formatting, and storing data in computer memory according to pre-defined fields, for example, customer name, account number and dollar amount of purchase.

DATA COMMUNICATIONS: The transmission, reception and validation of data; data transfer between data source (originating node) and data sink (destination node) via one or more data links according to appropriate protocols.

DATA COMPRESSION: The technique that provides for the transmission of fewer data bits without the loss of information. The receiving location expands the received data bits into the original bit sequence.

DATASET: The major unit of data storage and retrieval, consisting of a collection of data in one of several prescribed arrangements and described by control information to which the system has access.

DES—DATA ENCRYPTION STANDARD: A U.S. government encryption standard used in ATMs and POS terminals.

DIGITAL CERTIFICATE: An electronic identification or passport that authenticates the identity of a user of an Internet program. Through the automated on-line exchange of digital certificates between two parties in an electronic transaction, both can be assured of the identity of the other and that a message received has not been tampered with during transmission.

DISTRIBUTED PROCESSING: The processing of functions such as program execution, storage control, and input/output that are performed at two or more nodes or endpoints on a network.

DNS—DOMAIN NAMING SYSTEM: The Internet's means of converting a text address into a numeral IP address.

DOMAIN: The unique name of a site. Domain end in one of several designations that indicate the type of organization holding the domain: con is short for commercial sites; gov for government sites; net for Internet service providers; org for non-profit organizations; lib for libraries.

DOWNLOAD: To transfer something from another computer (generally one connected to the Internet) to your computers hard drive.

E

E-CASH—ELECTRONIC CASH: System by which consumers can transfer value over the Internet or other on-line connection to pay for goods or information. Typically, this is associated with low transaction values or between individuals where the seller is unlikely to accept credit cards.

E-MAIL—ELECTRONIC MAIL: A method of communication over the Internet by sending messages through the network as data packets.

ELECTRONIC COMMERCE: The use of the Internet or an on-line service for commercial purpose. This can include banking, shopping or purchase of financial services and products.

ENCRYPTION: A method of coding data, using an algorithm, to protect it from unauthorized access.

ENCRYPTION KEY: A data string used to encrypt or decrypt information.

F

FIREWALL: A series of hardware and software based security measures that limit outside access to a server or network.

FTP—FILE TRANSFER PROTOCOL: A standard method of transferring text, sound, and graphics files, and executable program files over the Internet.

G

GIF—GRAPHICS INTERCHANGE FORMAT: A type of graphics file.

GUI—GRAPHICAL USER INTERFACE: A software design, typically including icons, pull-down menus and a mouse, which helps users navigate applications and on-line services.

H

HOME BANKING: A program by which consumers can electronically check on bank balances, transfer funds or perform other basic banking functions from a remote location. The service may be offered via a conventional telephone or a personal computer. Some providers are considering the use of interactive television programs. Also called airchair banking, virtual banking, electronic banking, remote site banking and self-serve banking.

HOME PAGE: The welcome mat for a Web site: the introductory page that leads you to other information linked to a specific Web site.

HTTP—HYPERTEXT TRANSFER PROTOCOL: A standard for linking document on the World Wide Web.

HYPERLINK: The dynamic word or image on a World Wide Web document that, when clicked takes you to a linked document.

HYPERTEXT: Internet text that is linked dynamically to other text.

I

INFORMATION SUPERHIGHWAY: A broad term that includes the Internet, on-line services, interactive television and other types of services designed to bring information to consumers.

INTERNET: A global network of computers at various government, educational and commercial sites based on TCP/IP standards that provides file transfer, remote log-in, e-mail, news and other services.

INTERNET PUSH TECHNOLOGY: Software that enables requested information or Web pages to be delivered automatically to a consumer's PC via the Internet without the need for the consumer to search for and retrieve the information.

INTRANET: A private, internal network generally in a corporate or university setting, that is based on TCP/IP technology and uses Internet based software, but which is not directly connected to the Internet.

IP NUMBER OR ADDRESS: A set of numbers, set off by dots that indicate a machines unique Internet Protocol address. An IP number looks like this: 190.34.234.6.

IP—INTERNET PROTOCOL: The part of TCP/IP that routes information throughout the network.

IRC—INTERNET RELAY CHAT: A means for people to communicate in real time over the Internet.

ISP—INTERNET SERVICE PROVIDER: A service that provides direct Internet only access via phone lines.

ITV—INTERACTIVE TELEVISION: Programs by which consumers not only watch television, but also interact with it through use of a remote control. Some service providers also are looking to link financial services to entertainment services so that consumers can use their television screens to shop, pay bills, bank and access other financial services.

IVR—INTERACTIVE VOICE RESPONSE: Technology used in bank call centers that allows callers to interact directly with a host computer, rather than a service representative, by responding to questions either by using touch tone or speech recognition.

J

JAVA: A programming language developed by Sun Microsystems Inc. for on-line multimedia and database access applications.

L

LAG: The time between making an entry into a computer and receiving a response from the computer. On low speed Internet connections, lag can become a major problem.

LAN—LOCAL AREA NETWORK: A set of interconnected computers, generally all at one site.

LEGACY SYSTEM: A financial computing system from an earlier generation that can sometimes be interfaced only with difficulty to modern computing and networking systems.

LISTSERV: Both an electronic-mail mailing list and the software used to send the message systems.

M

MODEM: A hardware device that adapts a PC for phone line data transmission. Internet modems reside in a PC's card slot, while an external modem is plugged into a PC's serial port.

MULTIMEDIA: The transmission of information in more than one form. Includes text, audio, graphics, animation and full motion video.

N

NODE: A decision making switching point where MasterCard transmissions are routed. Refers to the packet switching centers located around the world.

O

OFX—OPEN FINANCIAL EXCHANGE: A message protocol being developed by Microsoft Corporation, Intuit Inc. and Checkfree Corporation to allow banks to use computer hardware and software from multiple vendors without communications problems.

OPERATING SYSTEM: The basic software that provides a PC's user interface and sets the architectural standards for all applications.

P

PACKETS: Smaller units of information that are broken down and transmitted over the Internet; also called IP datagrams.

PASSWORD: A unique string of characters that a user must provide in order to gain access to an on-line system or services.

PCMCIA CARD: A miniaturized, card-based peripheral used in mobile PCs that conforms to standards set by the Personal Computer Memory Card International Association. These cards—about the size of a credit card—provide expanded plug-and-play functionality such as extra memory, data/fax modem or LAN connectivity, and may be used to store digital certificates, providing certificate portability and improved security compared to hard disk certificate storage.

PCs—PERSONAL COMPUTERS: Compact computer devices found in homes or offices. A number of home banking programs require consumers to have a PC and a modem to transmit and receive information.

PDA—PERSONAL DIGIAL ASSISTANTS: Small portable computers that allow consumers to transmit and receive messages over the airwaves. Some banks have considered supporting such devices to enable consumers to bank electronically while commuting or when in other locations where phone lines are not available.

PEER TO PEER: Transmission from one endpoint on the MasterCard Banknet transaction processing network to another. Bypassing the need to bring the transmitted data into a central node before retransmitting outward.

PROTOCOL: A standard specification for how computers will communicate with each other.

PUBLIC KEY CRYPTOGRPHY: A system for securing messages sent over the Internet or other networks that is based on encryption using a matched pair of keys—one public and one private. Only parties with knowledge of both keys are able to decrypt an encrypted message.

R

RAM—RANDOM ACCESS MEMORY: The computers primary workspace, which holds all applications and documents in use.

S

SERVER: A software program, or the computer running the program, that allows other computers to share its resources.

SET—SECURE ELECTRONIC TRANSACTIONS: A protocol developed by MasterCard International, Visa International and others that spells out what is needed to protect the security of credit card transactions conducted over the Internet.

SGML—STANDARD GENERALIZED MARKUP LANGUAGE: Computer code for formatting a document. HTML is a type of SGML.

S-HTTP—SECURE HYPERTEXT TRANSFER PROTOCOL: An extension of HTTP that provides security for online transactions.

SIGNATURE: A file that appears at the end of e-mail messages or Usenet posts that contains a name, phone number, e-mail address, graphics, quotes, etc.

SPIDER: A technology used by Internet search tools that combs the Web and Collects information that can be searched by users.

SSL—SECURE SOCKET LAYER: A software encryption system developed by Netscape Communications Corporation that encodes information so that it can be read only by those to whom it is sent.

T

T1: Can refer to a service, a carrier line, a switch, or speed. T1 denotes a speed of 1.544 MBPs (megabits per second).

T3: A 44.746 megabit line.

TCP/IP—TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL: A package of standards that allow disparate machines, operating systems, computer languages, and software to communicate with each other.

TELNET: A program that allows users to log in to other computers on the Internet from remote locations.

U

UNIX: A computer operating system developed by Bell Laboratories. Much of the Internet was originally built using Unix.

UPLOAD: To transfer information from your computer to another machine or to the Internet.

URL—UNIFORM RESOURCE LOCATOR: The address for a particular Web site.

V

VRML—VIRTUAL REALITY MODELING LANGUAGE: A standard code for the Web that can be used to create three-dimensional objects online.

W

WEB PAGE/WEB SITE: A screen or series of screens created within the HTML environment and viewed with a Web browser.

WEB HOSTING SERVICE: Support services provided by an ISP to someone with a Web page. Typical services include script writing, link maintenance and audience tracking.

WEB PAGE SOFTWARE: The application software used to create a Web page. Such software usually comprises background patterns, clip art, and templates of common page designs.

WEBMASTER: A person who builds or maintains Web sites.

WEB TV: A proprietary technology from Web TV Networks Inc. commonly used to denote technology that allows consumers to use their TV sets to access the Internet.

WORLD WIDE WEB: A data network that contains sites linked by a common protocol system of hyperlinked documents that can be accessed via the Internet.



ELECTRONIC TRANSACTIONS ASSOCIATION
14 WEST THIRD STREET ■ SUITE 200 ■ KANSAS CITY, MO 64105
800.695.5509 ■ 816.472.7765 FAX
WWW.ELECTRAN.ORG WEBSITE