Definitions

Electronic commerce: Electronic financial services delivered via electronic means including, but not limited to, the Internet or other electronic delivery vehicles.

Specific examples of e-commerce activities include:

1. Internet/world wide web services
    - Email inquiries and responses
    - Publishing of general information on {COMPANY-NAME} web site
    - Data entry or verification by staff on a vendor's data processing system
    - File transfers of member information for direct mail projects or statement generation
2. Web account access
    - Viewing share or loan transaction history and balances
    - Transferring funds between shares and loans, transfers to other financials, or Person to Person Transfers (PTP)
    - Requesting a check withdrawal from a share or loan
    - Applying for {COMPANY-NAME} services through applications or forms
    - E-mail statements
    - Electronic retrieval of check copies
    - E-alerts
3. Online bill paying services
4. Audio response/phone based
5. Wireless services
6. Mobile banking

Encryption: Is the conversion of data into a form, called a cipher text, which cannot be easily understood by unauthorized people.

Authentication: Is the process of determining whether someone or something is, in fact, who or what it is declared to be. Depending on the transactions, a more stringent authentication process may be required.

Firewall: Any hardware and/or software designed to examine network traffic using policy statements (ruleset) to block unauthorized access while permitting authorized communications to or from a network or electronic equipment.

Overview

{COMPANY-NAME} recognizes the importance of electronic commerce (e-commerce) activities to its present day operations.

{COMPANY-NAME} is committed to using e-commerce activities in a cost effective manner that promotes accuracy, safety, security, and efficiency. These activities bring automation and efficiencies to traditional manual tasks and allow quicker access to information resulting in improved member service.

Purpose

This e-commerce policy is to be used as both a guideline and an overview in the management of {COMPANY-NAME}'s electronic services.

Policy Detail

{COMPANY-NAME} is committed to enhancing member service through the use of many forms of e-commerce activities.

Electronic commerce activities include {COMPANY-NAME}'s web site, email, telephone access system, ACH transactions, ATM system, online bill payment, and home banking services. They also include business-to-business transactions where interaction is conducted electronically between {COMPANY-NAME} and its business partners using the Internet as the communications network.

It is the practice of {COMPANY-NAME} to safeguard member data at all times, including the processing of e-commerce transactions. Information must be protected at both the sending and receiving ends of each transaction. To accomplish this, there are several levels of protection applied to e-commerce activities.

- **Encryption**
  - Encrypting transactions provides security by ensuring that no portion of a transaction is readable except by the parties at each end of the transmission. This ensures that data can be transmitted securely without concern that another party could intercept all or part of the transaction. Encryption also makes certain that the transaction is not tampered with as it routes from point to point and data is received exactly as it was sent. {COMPANY-NAME} will use a minimum of 128b encryption. This also applies to vendors that host {COMPANY-NAME} member data.
- **Authentication**
  - After a secure connection is established, the initiating party must prove his/her identity prior to conducting the transaction. This is typically handled with user IDs or account numbers, along with password or PIN combinations. Additionally, encryption certificates are also employed to validate the authenticity of both servers and users. System administrators control system access by assigning users different levels of access for applications and data. These access levels are determined by senior management and are

specific to each job function. This ensures that access to applications and specific types of transactions are only granted as job functions require.

- **Multi-factor Authentication (MFA)**
  - For online banking, MFA offers more than one form of authentication to verify the legitimacy of a transaction. The layered defense makes it more difficult for an unauthorized person to gain access.
- **Firewalls**
  - {COMPANY-NAME} will deploy and utilize firewalls as necessary to protect internal systems from threats originating from the Internet, as well as those that might be present when connecting to vendors' networks. Firewall operating systems and configurations will be reviewed periodically to ensure maximum protection. An audit log will be maintained tracking all attempts to access un-configured (blocked) services. Firewalls and other access devices will be used, as needed, to limit access to sites or services that are deemed inappropriate or non-corporate in nature. Vendor hosted solution firewalls will be reviewed prior to implementation.
- **Network Traffic Rules and Restrictions**
  - Intra-network traffic is subject to distinct operating rules and restrictions. Through the use of firewall technology, outside parties are directed only to approved, internal resources. An example of this is web page services that allow certain types of traffic from the Internet (web page browsing) but have other types of traffic blocked (i.e. administrative tasks). This strategy dramatically reduces the risk of any party gaining unauthorized access to a protected server.
  - The internal network is also protected from virus attacks through the use of network-level anti-virus software that is updated automatically on a regular basis. These regular updates are loaded automatically to each PC, as they are available. This provides the most up to date virus protection

and security available. E-mail is also scanned prior to delivery, reducing the potential of a virus entering the network in this manner.

- **Physical Site Security**
  - The entire IT Department is protected by a card access entry system allowing only authorized personnel into the Department. Sensitive data, hardware, and software are secured in the {COMPANY-NAME} data center, which is secured with a card access entry point and is monitored throughout the day by IT staff. Access to the data center is further limited to a small number of authorized personnel. It is {COMPANY-NAME}'s practice to change administrative passwords and immediately remove card access privileges after any change in IT staff.
  - In addition to on-site storage of data, {COMPANY-NAME} stores overnight backups of critical systems data and replicated Storage Area Network (SAN) storage to a secure, off-site location. This ensures that data is available in the event of a disaster or other critical situation.
- **Staff Training and Review**
  - IT staff receives training and reviews all procedures at least annually or as major system additions or changes are implemented.
- **User Password Maintenance /R**
  - Staff passwords, on the host data processing system, expire after 45 or 90 days, forcing users to modify their passwords. This control, along with a strict {COMPANY-NAME} policy prohibiting users from sharing or disclosing their passwords, is intended to prohibit unauthorized access to systems and data. After receiving a change in status from the Human Resources Department or other management team members, IT staff immediately removes user access codes from appropriate systems.
- **Expert Assistance**
  - {COMPANY-NAME} recognizes that e-commerce security issues change daily. New threats to security, safety, and

accuracy appear daily and system vendors publish updates and patches regularly to eliminate the threat. To assist in the ongoing maintenance of key components of system security, {COMPANY-NAME} will engage, at a regularly scheduled interval, consulting and audit oversight with a nationally recognized leader in the area of e-commerce security. This vendor

  - may also provide technical assistance as new e-commerce related features are added to the system to ensure the continued safety and security of existing systems.

- **Communications Network**
  - {COMPANY-NAME} employs the use of several types of data communication lines including dial-up phone lines, direct point-to-point circuits, and other private and public network connections. Data transmissions are secured, encrypted, and/or password protected, as needed.

Response Program

In the event PURPLESEC suspects or detects unauthorized individuals have gained access to member information systems, PURPLESEC will report such actions to appropriate regulatory and law enforcement agencies according to PURPLESEC's information security response procedures.