

Chapter 3

Introduction

Introducing the Code of Practice

What is the Code of Practice? The Code of Practice is an agreed code of conduct between parties involved in electronic commerce. It applies only to the electronic interchange of data and not to the substance of the message transmitted. It deals with questions of security, verification and authentication of the communicating parties.

What is the purpose of the Code of Practice? The purpose of the Code of Practice is to provide a set of rules which set out minimum standards with which parties trading electronically will comply. It is intended that this tool will be used in lieu of trading partner agreements. Additional operating information will still need to be agreed upon between Trading Partners and documented by them.

Who supports this Code of Practice? NAGASA's Electronic Commerce Committee developed this code to support and advance the application of Electronic Commerce between manufacturer, dealer, and customer in the printing and imaging distribution channel. The NAGASA Board of Directors support and encourage the use of the Code.

How do I become a signatory? The form for becoming a signatory to this Code is on page 9 in Chapter 2. Fill out the information and send the form to NAGASA. The information you provide will be supplied to all other signatories to help potential trading partners find out whom they should contact.

Terms and Principles

The objective of the Code is to establish a set of principles that will:

- 1) Create an environment in which smooth operations of electronic commerce can be fulfilled through good and ethical business practices,
- 2) Set minimum agreed standards and rules of conduct when using electronic processes to trade commercially,
- 3) Minimize legal issues when preparing to trade commercially through electronic processes, and
- 4) Promote a 'safe' environment to conduct business electronically.

Definition

Electronic Data Interchange (EDI) is the transfer of structured data, by agreed message standards, from one computer system to another, using an electronic means.

A **document** is a form which trading partners agree to exchange (such as purchase orders, invoices, and advanced shipping notices). A **transaction set** is the name given a complete trading document sent electronically using EDI.

A **trading partner** is any organization with whom you establish a trading relationship.

A **mailbox** is a repository for messages in an electronic mail system. Messages should be authenticated before the message is deposited in the addressee's mailbox, as only authorized messages are allowed into mailboxes.

A **message standard** is a defined set of transaction sets, data dictionary and controls used to facilitate transactions. For EDI, we use the American National Standards Institute, Accredited Standards Committee X12 (ANSI ABC X12) standard.

Principles

1. Authentication of an EDI document:

- 1.1 An EDI document should identify the sender and intended receiver of the message as defined by the applicable NAGASA approved transaction set.
- 1.2 Each trading partner shall use computer-based methods to verify the identity of trading partners sending and receiving EDI transaction sets.
- 1.3 Higher levels of authentication may be mutually agreed between trading partners.

2. Offer and Acceptance of an EDI document:

- 2.1 An offer is made by the sender once it has been deposited in the addressee's mailbox.
- 2.2 An acceptance occurs when a receiver takes active steps to fulfill the offer, deposits a notice of acceptance in the offerer's mailbox, or otherwise communicates acceptance in a manner agreed by the trading partners (whichever is earlier).
- 2.3 If an EDI offer is not accepted by the receiver, the sender of the document should be advised in a time that is reasonable within the industry for the specific type of document transmitted.
- 2.4 Trading partners agree where such standards exist, American National Standards Institute, Accredited Standards Committee X12 (ANSI ASC X12) will be used for exchange of documents between trading partners (including transaction sets, data dictionary and transmission controls). No requirement to migrate to this standard will be assumed for preexisting documents used between trading partners (including proprietary methods) where trading partners mutually agree to continue.
- 2.5 The receiver will cause to be transmitted within 24 hours a functional acknowledgement for each document sent (except a functional acknowledgement), indicating transmission and requisite data has been received.
- 2.6 EDI documents will be considered "signed writings" under the statute of frauds.

3. EDI documents as evidence:

- 3.1 Trading partners agree a computer generated EDI document may be used as admissible evidence in a Court of Law, subject to the

acceptance of that evidence by the Court.

3.2 The retention of EDI documents is assumed to be electronically the same as the retention of paper (hard copy) documents, unless EDI specific legislative requirements apply.

3.3 Trading partners agree to maintain adequate audit trails for a reasonable period to show the movement of EDI documents within their systems.

4. Liability:

4.1 Trading partners may make supplemental or contrary agreements outside this code of practice.

4.2 Where there is any breach of the code of practice the trading partners should first try to come to an amicable solution between them. Failing this, an appropriate mediator approved by the NAGASA Executive Committee must be sought.

4.3 Subject to any contrary agreement (i.e., master purchase agreement) made between trading partners outside this code of practice, general terms published in the seller's price catalogs, product guides or other sales literature, in effect at time acceptance is transmitted, will apply.

5. Maintenance of Security and Confidentiality:

5.1 All reasonable diligence, care and all appropriate steps should be performed by a trading partner to ensure adequate security and data integrity is met.

5.2 Trading partners agree to treat EDI documents as confidential.

5.3 An EDI document should only be available to authorized persons within the trading partner's organization or to agreed third parties or agents.

6. Access to EDI Mailbox:

6.1 Trading partners should access their EDI mailbox at least once per working day during normal work hours (8:00 a.m. to 5:00 p.m. local time; also VANs provide off-peak reduced rates during 8 p.m. - 6 a.m.).

7. Fall Back Options and Notification:

7.1 When a trading partner becomes aware it is unable to send or receive EDI messages in the normal way, it will notify all relevant trading partners in a timely manner, but no later than 24 hours after becoming aware of the situation.

7.2 Each trading partner should consider the various fall back options available to them and mutually agree on the option most appropriate to maintain their day-to-day business operations.

- 7.3 The originator of the fall back notice should advise all relevant trading partners in a timely manner when it is able to resume EDI trading.

8. Terminations and Amendments:

- 8.1 Reasonable notice in writing should be given before an EDI trading relationship is to be terminated, typically at least 30 days.
- 8.2 Where any amendments to the terms of the current EDI trading relationship are to be made, due notice in writing should be given to all relevant trading partners.
- 8.3 Each trading partner reserves the right to make an emergency suspension of electronic transmission and/or computer connections in order to prevent illegal access or other damage. Such action shall not constitute termination of this agreement.

9. Application of Standards:

- 9.1 Each trading partner acknowledges that the migration of EDI Message Standards are part and parcel of using EDI.
- 9.2 The implementation of new EDI documents and/or EDI Message Standards should be carried out in a manner which does not unreasonably disadvantage or impede the conduct of normal business between trading partners.
- 9.3 A trading partner initiating a new or replacement EDI document and/or EDI message standard, should allow a reasonable time frame for implementation.

10. Costs and Expenses:

- 10.1 Each trading partner shall, at its sole cost and expense, arrange with a third party electronic clearinghouse (commonly known as a Value Added Network or VAN) for a designated electronic mailbox to which their trading partners can electronically transmit and deposit documents.
- 10.2 Trading partners shall each pay their respective costs of translation, formatting, and standards compliance checking.
- 10.3 Trading partners agree to pay their respective costs of maintaining a mailbox (including any minimum use charges), connect time, and network charges to and from their respective mailboxes.
- 10.4 A trading partner shall be solely responsible for interconnecting charges, fees, and expenses (if any), incurred by themselves and their trading partners based upon their choice of Value Added Network.

11. Modifications to this Code:

- 11.1 Any individual wishing to make a change to this Code of Practice should send a letter, detailing the desired modification, to the NAGASA president. Each request will be reviewed by the Electronic Commerce Committee and, if the committee agrees the suggestion has merit, will publish the recommended change for a 30-day comment period. After the comment period, the change must be approved by the NAGASA Board of Directors.
- 11.2 All signatories of the Code of Practice will be notified of changes once approved by the Board of Directors.
- 11.3 This Code of Practice and list of signatories will be published annually, or more frequently at the discretion of the NAGASA president.

Practices

EDI has the potential for strengthening business communications and relationships between trading partners. There are some common sense, reliable and practical steps you can take to ensure a high quality and successful EDI operation:

- ❑ Reconcile transmissions and acknowledgments for return receipt within 24 hours or as agreed with your trading partners. This will substantially improve the reliability of all aspects of your system (computer, network, personnel, etc.).
- ❑ When beginning a new transaction set, establish parallel processes (one paper, the other electronic) for about a month after start-up.
- ❑ Once you gain experience, eliminate references to paperwork that is external to the EDI transaction data, such as reference codes in lieu of text.
- ❑ Accept all transactions with errors into your EDI system for review and correction, thus salvaging some portion of the business transaction. Transmit the transaction error back to your trading partner on the Functional Acknowledgment (997) to help them resolve the problem.
- ❑ Review status reports daily and report them to appropriate parties, such as internal operators, value added network, hardware supplier, computer maintenance service provider, software vendor, or trading partners. Do the same for hardware and transmission problems.
- ❑ Protect and maintain confidentiality of passwords used for EDI access. Change passwords frequently.
- ❑ Your EDI computer should be controlled by applicable data security procedures.
- ❑ Software should provide adequate protection for password security.
- ❑ Maintain as much confidentiality, security, care, and diligence with EDI transactions as you do with their paper counterparts.

Readiness

Management

- ☐ Obtain high level consulting from major trading partner to understand issues that will be most important.
- ☐ Attend EDI seminars or training classes.
- ☐ Arrange for external consultant to facilitate your software development, integration, management readiness, and training.
- ☐ Determine whether you will develop or purchase software and what your hardware and systems requirements will be.
- ☐ Select your VAN.
- ☐ Notify NAGASA of your intent to follow this Code of Practice by completing the Signatory Letter on page 2-9.
- ☐ Make arrangement to begin EDI with your initial trading partner.
- ☐ Designate your manager for EDI implementation, establish performance expectations and success measures. Identify key personnel and back-up personnel.
- ☐ Develop your implementation time-line, including dates by trading partner, and sequence for starting new transaction sets.
- ☐ Establish adequately trained EDI operators and support personnel, including back-ups.
- ☐ Evaluate your capability (including back-up) by using a EDI operators checklist.
- ☐ Participate in NAGASA's electronic commerce user group.

Operations

Key Backup

- ☐ ☐ Install any new hardware required and conduct satisfactory testing. Obtain necessary training.
- ☐ ☐ Install software required and conduct satisfactory testing. Obtain necessary training.
- ☐ ☐ Install connection and conduct satisfactory testing of VAN. Obtain necessary training.
- ☐ ☐ Document processes and procedures to be followed to conduct business electronically. Incorporate quality practices.

Training

EDI Operators Checklist

Key Backup

- ☐ ☐ Trained in operation and process of conducting EDI. Including all aspects of hardware, software and VAN?
- ☐ ☐ Trained in basic operation of computers, especially any additional hardware and software necessary for EDI?
- ☐ ☐ Trained on using VAN?
- ☐ ☐ Knowledgeable in process of how to access your EDI mailbox?
- ☐ ☐ Trained in all interfaces to EDI (including printing incoming documents, applications interface and electronic feeds to other systems) when required?
- ☐ ☐ Understand process of reconciliation and interpretation of errors, error codes and transmission reports?
- ☐ ☐ Trained on procedures for notifying others of problems (such as internal operators, Value Added Network, hardware supplier, computer maintenance service provider, software vendor, and trading partners)?
- ☐ ☐ Knowledgeable in system creation of return documents and Functional Acknowledgments (997)?
- ☐ ☐ Competent in data archiving processes and creating backups?

Software

- ☐ Your selected software should be capable of sending EDI documents using user friendly screens. All EDI transactions should be integrated with your computer (or screen driven for PC applications).
- ☐ Your software should contain user friendly screens (if applicable), reports, error messages, and mapping capabilities.
- ☐ Your software should allow you to perform routine work processes without needing to know data element standards and conversion codes.
- ☐ Your software should provide for table drivers via screen input to meet any specific needs you have (e.g., ship to codes, systems ID, messages regularly used, etc.). Default entry is desirable.
- ☐ Your software should be capable of on-line editing in scroll mode. Avoid

multiple screens for document editing and preparation.

- ☐ Your software should be capable of separating test from production data within a single batch of transactions.
- ☐ Your software should allow you to specify values for GSO2 (Application Sender's Code) different from those in ISA header in data sent to allow identification of the source of a document (system, business unit, etc.).
- ☐ Your software should allow you to specify values for G503 (Application Receiver's Code) different from those in ISA header in data sent to allow for easy distribution of documents by the receiver.
- ☐ Your software should be able to generate the Functionally Acknowledge (997) at the group and / or document level.
- ☐ Your software should contain on-line help screens.
- ☐ Your software should include an easy to follow and understand operator's guide and quick reference materials.
- ☐ Your software supplier should provide an overview of their software, including software testing strategy.
- ☐ Your software supplier should provide an adequate period to evaluate and test, at no cost (at least 30 days).
- ☐ Your software should be capable of document modular 'add-on's.'
- ☐ Software should minimize the input EDI data required on return documents by deriving data from the original documents (e.g., POA deriving data, except changes, from the PO transaction).
- ☐ Software should map from ANSI data elements to business entry on incoming transactions, map from business entries to ANSI data elements on outgoing transactions.
- ☐ PC software should provide for generic document formatting capabilities (e.g., create a form).
- ☐ Your software should be capable of providing an interface to your internal systems (e.g., invoicing, inventory management, payables, etc.).
- ☐ Your software should be capable of both interactive and batch modes (including fast batch and hot batch), file transfer and time delay transmissions.
- ☐ Your software should have the capability of identifying the network used to exchange documents with your trading partner.
- ☐ Your software should be capable of multiple network communication links.

- Your software should perform compliance checking of data prior to being sent (your selected VAN could also perform this compliance checking).
- Your software should be multi-tasking and allow for interrupt and auto answer processing.
- Your communications software should contain checkpoint / restart capabilities.

Value Added Network

- ☐ Your selected VAN should be able to comply, on your behalf, with all requirements detailed in the NAGASA Code of Practice.
- ☐ Your VAN should provide interconnectivity capabilities to all major VAN's.
- ☐ Your VAN should have full interconnection accountability and insure that interconnections with other service providers are monitored, audited, and maintained to provide reliability. Each network must perform their own document tracking.
- ☐ Your VAN should minimize interconnect charges.
- ☐ Your VAN should be capable of accepting a complete interchange containing document types of varying standards, including multiple functional groups, which are of different standards and standard versions.
- ☐ Your VAN should provide document process time of less than one hour from your trading partner's mailbox to your own mailbox, and from your mailbox to your trading partner's mailbox.
- ☐ Transmission consistency should not vary for the various data transmission baud rates.
- ☐ Your VAN should be capable of communicating with multiple baud rates (1200 to 9600 baud at a minimum).
- ☐ Your VAN should be capable of sending transmissions at specified times and delaying or holding transmissions for a specified time increment.
- ☐ Your VAN should have hot batch capability.
- ☐ Your VAN should offer compliance checking upon request for segment sequences and data elements for transaction sets from all your trading partners.
- ☐ Your VAN should allow for on-line storage of EDI data and provide re-transmit capability for any document for a minimum of three days after initial, complete delivery.
- ☐ Your VAN should provide electronic status and exception reporting. Status reporting should provide for tracking of documents down to the GS segment level in an interchange. Reporting should provide summary, exception, and detailed status reports.
- ☐ Summary and exception reports should list error conditions first or highlight error conditions to expedite the status review process.

- ☐ Your VAN should provide auto restart capabilities. If communication errors occur an automatic restarting function should be available.
- ☐ Your VAN should insure that data transmissions are error-free and error-correcting and that error handling is transparent to you and your trading partners.
- ☐ Your VAN should constantly monitor transmission and mailbox capabilities and actively insure a quick and reliable system.
- ☐ Your VAN should insure data integrity for all transaction types.
- ☐ Your VAN should provide local (or toll-free) support and technical assistance. Problem solving should be on-line or call back within one hour.
- ☐ Network service and support should be available 24-hours per day, 7-days per week.
- ☐ Your VAN should provide training to your operators on process handling, error codes and conditions, etc.
- ☐ Your VAN should be capable of printing documents and delivering paper copies to your trading partners in the event of an extended period of down-time.
- ☐ Your VAN should provide for auxiliary power (including UPS) for re-routing of electronic transmissions in the event of failures.
- ☐ Your VAN should be capable of providing their planning and traffic forecasts.
- ☐ Your VAN should provide shadow writing capability to guard against lost EDI data due to head crashes or network failures.
- ☐ Your VAN should provide system and data security (data integrity, error free protocol ID, password protection by encrypting or other means to prevent password file liability).
- ☐ Your VAN should require a log on ID and password combination where data flow between mailboxes is controlled by an authorization database in the VAN's system.