National Check Network

National Check Database

Reference Manual

April 2002

Confidential and Proprietary Data

Trademark Notice

Table of Contents

1 - Introduction

2 - Transaction Details

3 - NCN Toolkit

4 - NCN Rule Set Maintenance

5 - Transaction Log Utilities

6 - Billing File Generator

7 - Transaction Activity Report Writer

8 - Compliance Report Generator

9 - CheckManager 3000 Terminals

10 - Verifone Terminals

11 - Lipman - Nurit Terminals

12 - Hypercom Terminals

13 - Dassault Terminals

14 - Support Server

15 - Troubleshooting

NCN
NATIONAL CHECK NETWORK

Section
1

Introduction

In this section...

- National Check Network (NCN) Overview
- NCN Data Base
- Transaction Overview
- Site Setup

1 - Introduction

This section contains an overview of the National Check Network (NCN) and describes the NCN database. It also provides an overview of the transaction process and the site setup.

National Check Network (NCN) Overview

NCN provides on-line check verification in a variety of configurations using either check MICR data to identify the account or any of four different identifications (ID's). The software processes personal checks, payroll checks, government checks, and third party checks differently. It accepts external negative files from a wide range of users throughout the U.S., including check collection agencies, credit card processors, and large merchant chains. The system augments this negative check data with extensive information about each MICR account and ID presented to the system as part of each check verification. This positive data base has much more value than the negative file since it can spot fraudulent check passing patterns prior to when the checks get returned by banks. The system accepts dial-in inquiries via telephone from point of sale terminals or from cash registers directly.

For each check approval transaction using checking bank and account data, the MICR information on the bottom of the check provides the necessary input data to the data base. This information includes the **transit field** (A.B.A. routing number plus bank identification number) plus the individual **account number**. Automatic check readers sense this information and transmit it through the point of sale terminal. Since the system uses the complete MICR information, there is no possibility for cases of mistaken identity.

For each check approval transaction using ID's, the system accepts driver's licenses, Social Security numbers, custom courtesy card numbers, or military ID's. The clerk typically keys in the appropriate ID, although the system also accepts input from magnetic stripes that are on driver's licenses or courtesy cards.

The NCN system has a primary goal of fraud prevention. It makes an account evaluation based on multiple criteria and using limits that each installation and each merchant can customize. It continuously accumulates positive information on repeat customers and uses this information to detect unusual check writing activity on an account.

All this flexibility and capability means that users must make numerous configuration choices at the time of installation of each merchant. This manual describes these choices individually and explains the multitude of transaction evaluation parameters available to satisfy each merchant's special requirements. Since each member of NCN can set all of these values independently, the resulting system becomes uniquely customized for each different agency and meets a wide variety of individual requirements without requiring special and expensive software alteration.

NCN Data Base

The data base is a key element to powerful check verification systems. The NCN system data base consists of information in three primary areas:

1. **Account information.** As checks are processed during normal transactions, each new account creates a record in the data base. All activity for the account accumulates entries in the record without regard to the possible existence of returned checks. Thus, the account information becomes a **positive file** with long term historical summaries and detailed data on recent transactions for all accounts active in the system. This positive information allows merchants to process checks more efficiently for the 99% of their customers who never have returned check problems. The account information also includes a summary of past and currently unpaid returned checks, so it also provides **negative information.** Access to this information uses the combined transit and account fields from the MICR line on the bottom of checks.

2. **Returned check information.** All returned checks that are still unpaid exist as entries in the data base. This information is the traditional **negative file** that many check authorization/verification systems use as the sole basis for the check evaluation. Access to this information uses the combined transit and account fields from the MICR line on the bottom of the returned checks.

3. **Identification information.** The NCN system provides the capability to accumulate individual ID's associated with each account, and to associate several accounts with one or more ID's. If a given ID is associated with an account that has unpaid returned checks, the system can give a negative evaluation of checks written by the same individual on other accounts. This feature provides a significant tool for reducing fraudulent bad check passing. The ID also plays a major role in payroll check cashing, with special velocity limits available for payroll checks cashed using each ID. The system recognizes several alternate forms of identification:

    - Driver's license
    - Social Security number
    - Courtesy Cards provided by merchants or check collection agencies
    - Military ID's

ID-based check verifications use these three data bases by linking the ID to a specific account that has unpaid checks in the returned check data base. The system creates a special “account” in the MICR data base in order to track check cashing activity and to provide the same features that the MICR-based check transactions have.

Another key element in evaluating a check is the concept of **velocity.** A common fraud pattern involves obtaining a checking account and then passing as many checks as possible as rapidly as possible before any of the checks are returned by the bank for insufficient funds. In order to detect this pattern, the system monitors the number of checks written in a specified period of time (velocity) and can return a negative evaluation of further checks on the same account when the velocity exceeds a preset limit.

Transaction Overview

Figure 1-1 shows the basic concept of a check verification conducted from a point-of-sale. The point-of-sale terminal, which normally has a check reader attached, assembles a **request packet** of information. This request packet includes both information specifying the specific transaction, such as the MICR data and check amount, and information

specifying the origin of the transaction, such as the NCN **site number,** specific merchant **location number**, and the **rule set number** for evaluating the transaction. The point-of-sale terminal sends this request packet as a single transmission to the NCN computer over conventional phone lines.

The NCN computer receives the request packet and performs several steps to evaluate the transaction:

1. Use the MICR or ID information to access data base information
    - Account history
    - Recent check writing activity
    - Unpaid returned checks
    - Use the Site Number and the Rule Set Number to retrieve the evaluation parameters
2. Evaluate the transaction
3. Create the **response packet** based on the evaluation results
4. Send the response packet and log the transaction

    The response packet sent back to the point-of-sale always includes the **idle prompt** and the **basic response** (ACCEPT/WARNING/DECLINE). In the case of warnings or declines, the system sends additional information explaining the response to aid the clerk in making a decision. All information sent back to the point-of-sale is placed in a single **response packet** of information that it transmits as a single burst of information.

It is important to note that NCN does not make any decision to accept or reject a check. It only advises the merchant of the status of the account with two different negative messages, one a warning and the other a stronger advice to decline the check. If any limit is exceeded, it advises the merchant of that fact, and furnishes additional detail to the point-of-sale. If everything is satisfactory, it tells the merchant that fact. The merchant uses this information to make the final decision regarding check acceptance. The system logs every transaction and its response, so merchants accepting checks against the advice of NCN can see the original response if the check later bounces.

The system makes its evaluation based on several possible criteria. The exact criteria used is chosen by the NCN user and may be individually tailored for a specific merchant location. Depending upon the actual options selected, the possible negative criteria include:

- **Negative file.** If an account has returned checks that have not been paid, further transactions on this account usually give a strong negative response (decline). Limits exist to set a number of unpaid returned checks or the total amount of unpaid checks. The unpaid returned checks may be counted if they have occurred at any merchant in the system, if they have occurred at any merchant in the group set, or only if they have occurred at a specific location.

- **Transaction limits.** Limits may be placed on individual transactions so that if either the amount of the transaction or the cash back exceed their respective limits, the system usually gives a milder negative response (warning). If desired, other limits on the transaction can trigger an ID verification or intervention by a manager.

- **Daily limits.** Limits exist for the total number of checks on a single account in a day, the total amount of checks on a single account in a day, and the total cash back for a single account in a day. When exceeded, the system usually gives a warning instead of a decline.

- **Velocity limits.** Limits similar to the daily limits exist for a velocity **window.** The velocity window specifies the number of days (between 1 and 14) used in velocity calculations. When exceeded, the system usually gives a warning.

- **ID status.** If activated, the system gives a negative response for checks offered by individuals who use an ID that has been associated with another account that has unpaid returned checks. ID's may also be flagged as stolen or stopped by special command by either a store or the collection agency. Flagged ID's usually result in a strong negative response (decline).

- **Federal Reserve limits.** The transit field includes a designation for the Federal Reserve district used by the bank on which the check is drawn. Fraudulent check passers sometimes alter this designation to cause the check to be sent to the most remote district for processing in order to gain more time before checks are returned by the bank. If desired, the Velocity PLUS system includes a list of acceptable Federal Reserve districts. Checks that specify districts outside this list usually give a warning.

- **Special stop.** Individual accounts may be stopped by special command by the collection agency. This may occur if the account has had returned checks that proved difficult to collect. Another example involves accounts that have been closed by a bank. Checks drawn on accounts with special stops usually give a decline.

The NCN check verification system has a large degree of flexibility, so individual users can choose to issue a warning or decline for each of the conditions described above. The list shown above indicates the most common choice for each of the possible failure conditions. These choices are described in more detail in “Transaction Details” on page 2-1 and in “Rule Set Parameter Definitions” on page 15-6, which defines each of the parameters used in evaluating transactions.

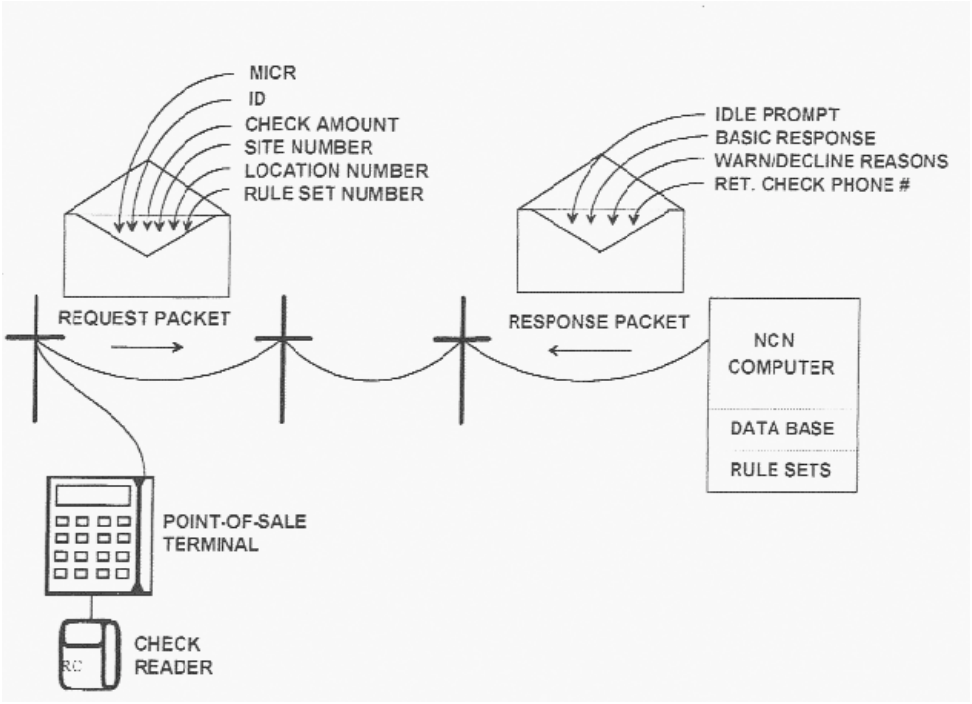


Figure 1-1. Sketch of check verification information packets

Site Setup

Each NCN site must provide certain data before using the system for check verification. These data include:

- **Agency name (16 characters).** Any decline at the point-of-sale due to unpaid checks provided by a member of NCN results in a decline message which includes the contributing member's name and phone number for the customer to call. The name must be a maximum of 16 characters including spaces.

- **Agency phone number.** As mentioned in item 1, each decline for unpaid checks provided by a member of NCN results in a response packet which includes a phone number for the customer to call to obtain information regarding the decline or arrange payment.

In return, each NCN site receives some standard information:

- **NCN site number.** This number must be used as part of the merchant ID on all transactions from a point-of-sale and associated with all returned checks provided to NCN.

- **VeriFone download ID.** This number is used for all downloads of VeriFone programs using the service provided by NCN.

NCN
NATIONAL CHECK NETWORK

Section
2

Transaction Details

In this section...

- Personal Check Transactions
- Payroll Check Transactions
- DL State Codes

2 - Transaction Details

Personal check transactions follow different strategies than payroll check transactions, and both are closely intertwined with the parameters and rules for making decisions. NCN uses a rule set combined with stored data in the data base to make an appropriate response. This chapter describes the basic transaction types in detail.

Each **Rule Set** specifies a unique set of transaction evaluation data to be used during the transaction process. This information includes the idle prompt displayed on the P.O.S. terminal, the group set to which the location belongs, and the equipment installed at the point of sale. The rule set options contain all of the limits and parameters used in making the transaction response.

Personal Check Transactions

Personal check verification transactions result in one of three outcomes: acceptance, warning, or decline.

Figure 2.1 shows the logic involved in MICR-based personal check transactions for the four possible warning conditions when using the default configuration:

D (day velocity limit)

W (window velocity limit)

T (transaction limit)

O (out of Federal Reserve set)

Complementing this diagram, Figure 2-2 on page 2-6 shows the logic involved in MICR-based personal check transactions for the three possible decline conditions in the default configuration, U (unpaid checks limit), A (account status problem), and I (ID flagged). Changing the warning set of conditions or the decline set of conditions shifts individual items between these two figures, but does not change the basic logic. If a check passes these seven tests (as most checks do), the check is authorized. The next few paragraphs explain these two figures in more detail.

MICR-based personal check transactions always use the MICR account number, the merchant ID (site number, location number, and rule set number), and the check amount as input information. Depending upon selected options, other input data include the sale amount and a customer ID. NCN uses the MICR account number to access existing information from its data base for the account status, recent transaction activity, and associated I.D's. Figure 2-1 on page 2-3 shows how all these data are processed to generate the four warning conditions.

MICR transaction activity (Figure 2-1 on page 2-3), includes all personal check transactions within the velocity window from all locations on the NCN system. Many merchants place more emphasis upon transactions actually conducted at their store (location). Therefore, the system includes a **location filter** to select only those transactions that occurred at the location identified with the current transaction.

NOTE

in this text, the word "location" refers to a specific merchant location. Specifying such a location requires both the site number and the location number.

Thus, for example, the account in question might have had seven transactions on the system within the velocity window, but only two of them were at the specific location conducting the current transaction. In this case, the output of the location filter would be only those two transactions. These two transactions, plus the current transaction, are compared against six different **thresholds**: **day** limits for the **number** of transactions conducted today, the **total amount** of transactions conducted today, and the **total cash back** for today, and **window** limits for the total **number** of transactions within the velocity window period, the **total amount** of transactions conducted within the window period,

and the **total cash back** within the window period. These six thresholds come from the **rule set** that is defined for the location. If the activity at the current location exceeds any of these six thresholds, either the "D" output or the "W" output is TRUE and the system generates an appropriate message.

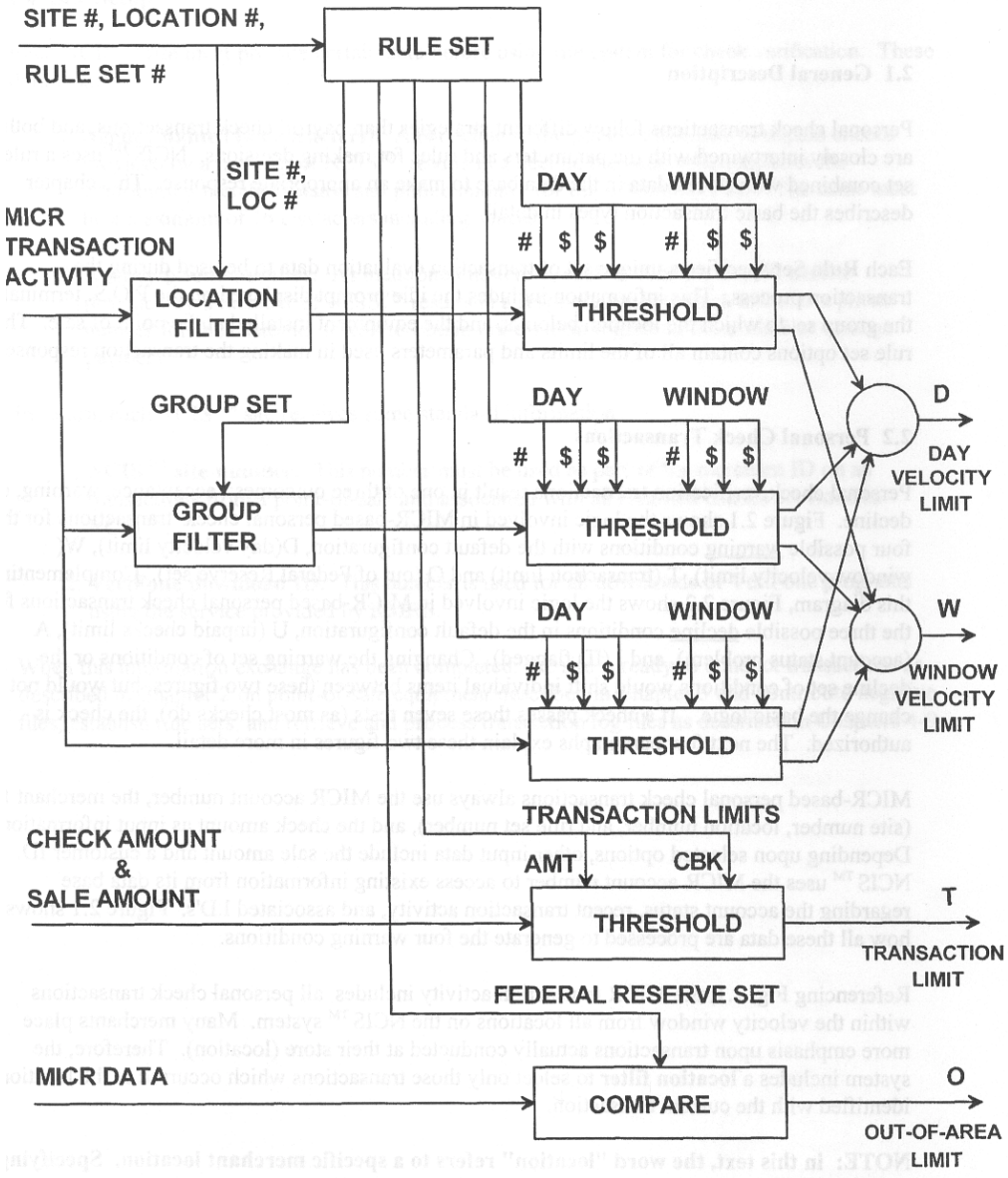


Figure 2-1. Logic for MICR-based personal check transactions to calculate warning conditions in default configuration.

Similarly, many merchants want to use data from other merchants but place more importance on data from other stores of a similar nature (e.g. only consider other convenience stores or auto parts stores) or other members of their chain of stores. NCN provides for a definition of a **group** of such stores. Each location must be part of one group. Furthermore, each location can define one or more groups to comprise a **group set** used for filtering transaction activity. The **group filter** selects only those transactions that

were conducted at any store belonging to the group set. Thus, for example, if an account had a total of seven transactions, of which two were conducted at the current location, perhaps five might have been conducted at other stores within the group set. These transactions are tested against a different set of six **thresholds** that are defined in the rule set. The six group set threshold limits are the same as was described for the six location threshold limits. If the activity within the group set exceeds any of these six thresholds, either the “D” output or the “W” output is TRUE and the system generates an appropriate message.

The system also allows testing of all transactions for the account using still a different set of six **threshold limits**. As with the location limits and the group set limits, these include **day** limits on the total number of transactions, total amount of transactions, and total cash back, and **window** limits on the total number of transactions, total amount of transactions and total cash back. If the total activity exceeds any of these six thresholds, either the “D” output or the “W” output isTRUE and the system generates an appropriate message.

The system provides for two **threshold** limits on each individual **transaction**: the **amount** of the transaction and the **cash back** for the transaction. If the transaction exceeds either of these two thresholds, the “T” output isTRUE and the system generates a CHECK TOO BIG or TOO MUCH CASH warning.

The final test shown in Figure 2-1 on page 2-3 uses the MICR data to determine if the bank on which the check is drawn is within an appropriate Federal Reserve district. Much fraudulent check passing involves altering the MICR data to cause a check to be processed at a remote Federal Reserve site. This gives additional time before the check bounces. Therefore, it is important to verify that each check is local and is processed by the appropriate local Federal Reserve bank or that the customer has previously presented a good check so is known to the system. Acceptance of out-of-area checks from repeat customers is important to some merchants who serve reliable but transient populations such as military personnel. Since some locations draw customers from more than one district, the system allows each location to specify an allowable **Federal Reserve set**. Each check is compared against this set and if it comes from a bank not in the set, the “O” output is TRUE and the system generates an appropriate warning unless the customer presents an ID that is known to the system and is good (unflagged). Note that accepting out-of-area checks from patrons with known ID's requires use of a VeriFone program that prompts for ID's on all personal checks, such as the full feature program for TRANZ terminals.

Figure 2-2 on page 2-6 shows the MICR-based processing for testing the default decline conditions for a personal check. As with the filtering used on transaction activity in Figure 2-1, the **returned check data** for the account conducting the transaction have **location** and **group set** filters. These filters serve a similar purpose on the returned check data. Many merchants have the most concern about any returned checks that were originally presented at their store. Therefore, the **location filter** selects only those returned checks that fit this criterion and the compare them with both a **number** and an **amount threshold**. Many collection agencies set the number threshold to zero and ignore the amount threshold. Some agencies, however, recognize that most returned checks occur through innocent errors and do not want to stop further checks on accounts that will pay for the check and the agency fee. They do want to stop fraud artists who have a larger numbers of unpaid returned checks. Therefore, they set the limit on the number of unpaid checks to a small, non-zero value. If the returned check data from the location exceed either limit, the system generates a “U” output and declines the check (assuming the default configuration).

Just as some merchants care most about returned checks from their own store, they also care about returned checks from other stores in their **group set**. Therefore, the system provides a **group filter** that selects only those returned checks that were originally presented at a store within their group set. Two different group **threshold limits** test this selected returned check data and generate a "U" output if the data exceed either limit.

Figure 2-2 also shows that the MICR data access the **account information** contained in the data base. It is possible to stop an account manually with an **agency stop** (collection agency wants to stop an account even after all returned checks have been paid)**, store stop** (store decides that there have been too many bad checks on a specific account)**, bank stop** (bank notifies agency that an account is closed)**,** or **customer stop** (customer notifies agency that someone is using his checking account without authorization). Any such stops affect the **account status** and generate an "A" output and decline check message in the

default configuration. NCN also provides the ability to stop a specific range of check sequence numbers. Customers can request this when their checkbook has been stolen and they don't want to close their account. Checks that have a sequence number within a specified stop range also generate an “A” output and decline check message.

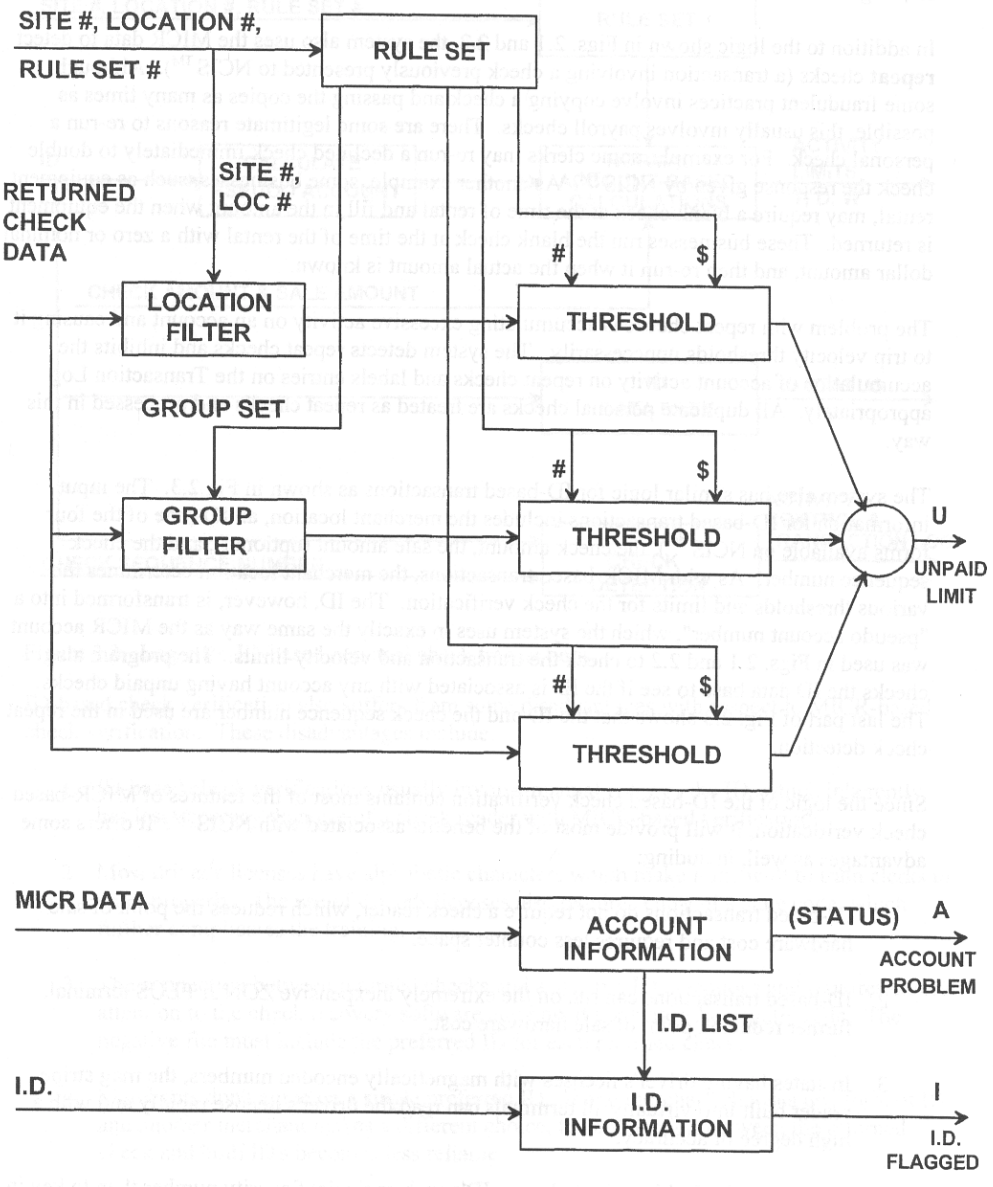


Figure 2-2. Logic for processing personal check transactions to calculate decline conditions.

The final decline condition for personal checks involves the status of any ID's associated with the account. Each account in the system accumulates a list of I.D's known to have been used to cash checks with the account. The **ID information** includes a status, that can be flagged if the ID is associated with a different account that has problems. This feature

provides valuable additional protection against fraud, as it identifies “runners” who can use multiple accounts but have only a single identification such as a driver's license. If the system detects such a **flagged ID**, it generates an “I” output and declines the check in the default configuration.

In addition to the logic shown in Figure 2-1 and Figure 2-2, the system also uses the MICR data to detect **repeat** checks (a transaction involving a check previously presented to NCN). Although some fraudulent practices involve copying a check and passing the copies as many times as possible, this usually involves payroll checks. There are some legitimate reasons to re-run a personal check. For example, some clerks may re-run a declined check immediately to double check the response given by NCN. As another example, some businesses, such as equipment rental, may require a blank check at the time of rental and fill in the amount when the equipment is returned. These businesses run the blank check at the time of the rental with a zero or nominal dollar amount, and then re-run it when the actual amount is known.

The problem with repeat checks is accumulating excessive activity on an account and causing it to trip velocity thresholds unnecessarily. The system detects repeat checks and inhibits the accumulation of account activity on repeat checks and labels entries on the Transaction Log appropriately. All duplicate personal checks are treated as repeat checks and processed in this way.

The system also has similar logic for ID-based transactions as shown in Figure 2-3 on page 2-8. The input information for ID-based transactions includes the merchant location, an ID (one of the four forms available on NCN), the check amount, the sale amount (optional), and the check sequence number. As with MICR-based transactions, the merchant location determines the various thresholds and limits for the check verification. The ID, however, is transformed into a “pseudo account number”, that the system uses in exactly the same way as the MICR account was used in Figure 2-1 and Figure 2-2 to check the transaction and velocity limits. The program also checks the ID data base to see if the ID is associated with any account having unpaid checks. The last part of Figure 2-3 shows that the ID and the check sequence number are used in the repeat check detection.

Since the logic of the ID-based check verification contains most of the features of MICR-based check verification, it provides most of the benefits associated with NCN. It offers some advantages as well, including:

- ID-based transactions do not require a check reader, which reduces the point of sale hardware cost and requires less counter space.

- ID-based transactions can run on the extremely inexpensive ZON Jr PLUS terminal, further reducing point of sale hardware cost.

- In states having driver's licenses with magnetically encoded numbers, the mag stripe reader built into virtually all terminals can read the driver's license rapidly and with a high degree of accuracy.

- Clerks usually find it easier to key in ID's such as Social Security number than to key in MICR data, and they do it more accurately.

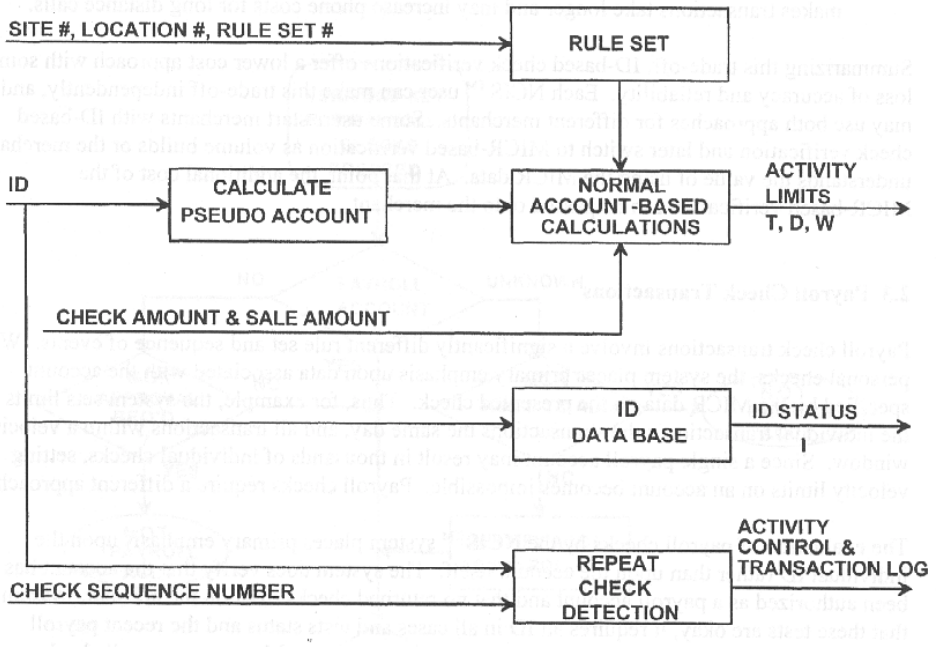


Figure 2-3. Logic for ID-based personal check transactions.

ID-based check verification also suffers from some disadvantages with respect to MICR-based check verification. These disadvantages include:

- ID-based check verifications usually involve manual entry of the ID, which inherently has less accuracy than use of a check reader with MICR-based verification.

- Most driver's licenses have alphabetic characters which make it difficult to train clerks to enter properly. The use of driver's licenses also requires entry of a state code, which further complicates the training.

- The connection between returned checks and a specific ID is tenuous and requires careful attention to the check recovery software and how it generates the negative file. The negative file must include the preferred ID for each returned check.

- Merchants don't agree on a single preferred ID. If one merchant chooses one form of ID and another merchant makes a different choice, the connection between the returned check and both ID's becomes less reliable.

- Less expensive terminals such as the ZON Jr PLUS and the ZON Jr XL communicate at 300 Baud instead of the 1200 Baud communications used by the TRANZ terminals. This makes transactions take longer and can increase phone costs for long distance calls.

Summarizing this trade-off, ID-based check verifications offer a lower cost approach with some loss of accuracy and reliability. Each NCN user can make this trade-off independently, and can use both approaches for different merchants. Some users start merchants with ID-based check verification and later switch to MICR-based verification as volume builds or the merchant understands the value of using the MICR data. At that point, the additional cost of the MICR-based verification can be passed onto the merchant.

Payroll Check Transactions

Payroll check transactions involve a significantly different rule set and sequence of events. With personal checks, the system places primary emphasis upon data associated with the account specified by the MICR data on the presented check. Thus, for example, the system sets limits on the individual transaction, other transactions the same day, and all transactions within a velocity window. Since a single payroll account can result in thousands of individual checks, setting velocity limits on an account becomes impossible. Payroll checks require a different approach.

The evaluation of payroll checks by the NCN system places primary emphasis upon the individual ID rather than upon the account itself. The system does verify that the account has been authorized as a payroll account and that no returned checks exist on the account. Assuming that these tests are okay, it requires an ID in all cases and tests status and the recent payroll check cashing by the ID. Thus the data base contains a record of the recent payroll check cashing transactions for each ID, plus a list of locations authorizing the ID to cash payroll checks. This approach places more emphasis upon the individual than on the account itself.

Figure 2-4 on page 2-10 shows the first stage of the logic followed by the system when a clerk initiates a payroll check transaction. On the VeriFone program, the clerk initiates the transaction by pushing a different key on the VeriFone terminal (the exact key depends upon the program in use). The terminal prompts for the MICR data, which can be read by a check reader or keyed in manually. The terminal automatically prompts for the amount of the check and usually the amount of the sale (which frequently is zero).

Using these data, the system first checks the account type. If the account is known to be a personal checking account or if the account is unknown, the next action depends upon the rule set used for this transaction. If the rule set does not require manager approval for payroll accounts, the system identifies an unknown account automatically as a payroll account or process a personal check as a payroll account. If the rule set requires manager approval for new payroll accounts, the system displays a message “NOT PAYROLL ACCT” and refuses to process the transaction. For these cases requiring manager approval, the manager must run a special transaction using a different key on the VeriFone terminal to register approval of the account as a payroll account.

The system checks its data base to find out if the ID is known and authorized to cash payroll checks at this location. If it is not known or authorized, the system adds it automatically if the location has authorized this option to occur without manager approval. If manager approval is required to add the location to the ID list of approved payroll check cashing locations, the system declines the check with the message "ID-NO PAYROLL AUTH".

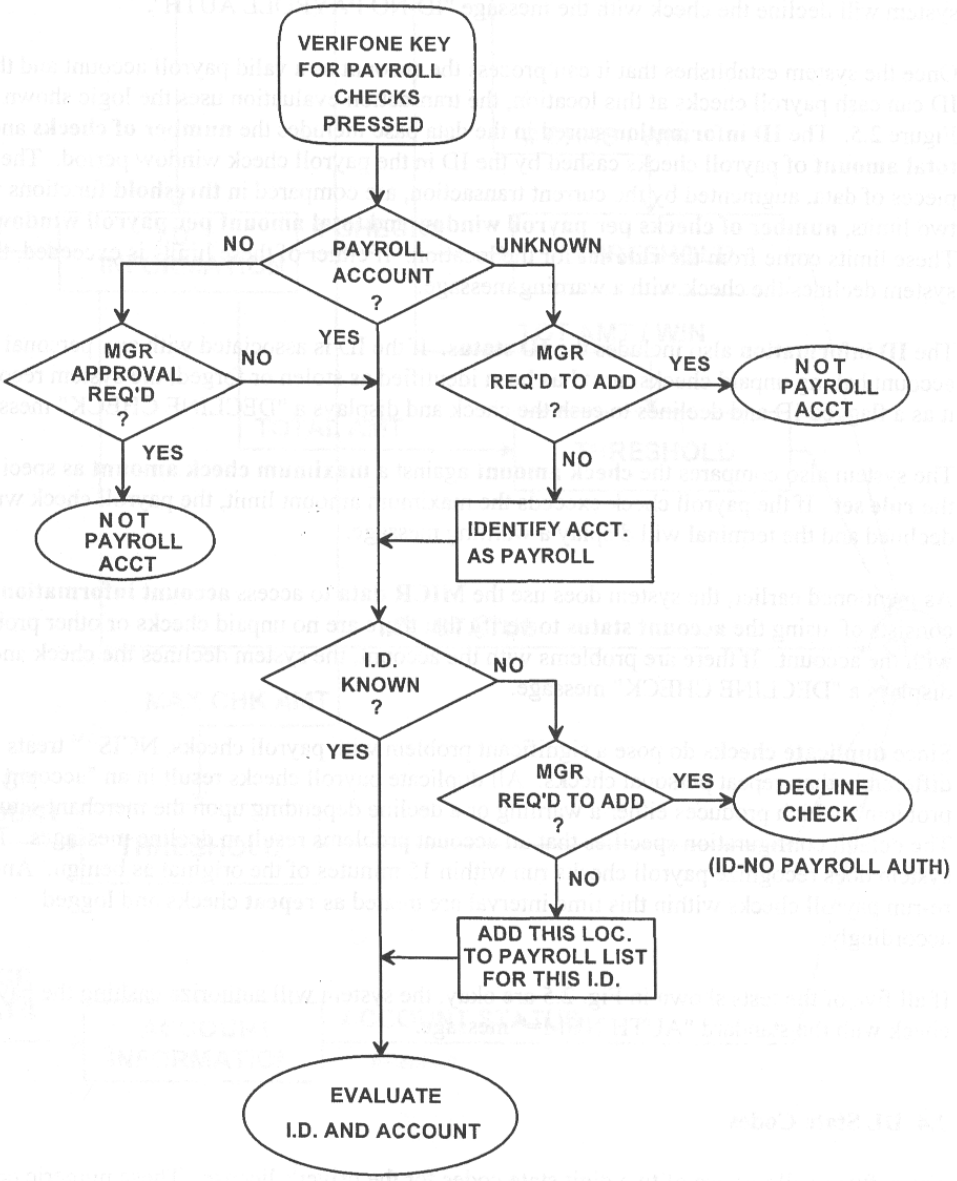


Figure 2-4. First stage logic for payroll check transactions.

Once the system establishes that it can process the account as a valid payroll account and that the ID can cash payroll checks at this location, the transaction evaluation uses the logic shown in Figure 2-5 on page 2-12. The **ID information** stored in the data base includes the **number of checks** and the **total amount** of payroll checks cashed by the ID

in the payroll check window period. These two pieces of data, augmented by the current transaction, are compared in **threshold** functions with two limits, **number of checks per payroll window** and **total amount per payroll window**. These limits come from the **rule set** for the location. If either of these limits is exceeded, the system declines the check with a warning message.

The **ID information** also includes the **ID status**. If the ID is associated with any personal account having unpaid checks, or it has been identified as stolen or forged, the system recognizes it as a flagged ID and declines to cash the check and displays a "DECLINE CHECK" message.

The system also compares the **check amount** against a **maximum check amount** as specified in the **rule set**. If the payroll check exceeds the maximum amount limit, the payroll check is declined and the terminal displays a warning message.

As mentioned earlier, the system does use the **MICR data** to access **account information**. This consists of using the **account status** to verify that there are no unpaid checks or other problems with the account. If there are problems with the account, the system declines the check and displays a "DECLINE CHECK" message.

Since **duplicate checks** do pose a significant problem with payroll checks, NCN treats them differently than repeat personal checks. All duplicate payroll checks result in an "account problem", that produces either a warning or a decline depending upon the merchant setup. The default configuration specifies that all account problems result in decline messages. The system does recognize payroll checks run within 15 minutes of the original as benign. Any re-run payroll checks within this time interval are treated as **repeat** checks and logged accordingly.

If all five of the tests shown in Figure 2-5 are okay, the system authorizes cashing the payroll check with the standard "AUTH NUM=" message.

DL State Codes

The software allows use of two digit state codes for the driver's license. These numeric codes are translated into the appropriate alphabetical codes, so the data entry in the check recovery software should continue to use the letter code. NCN uses the standard code substitution table established by ANSI and published as a standard for Information Interchange.

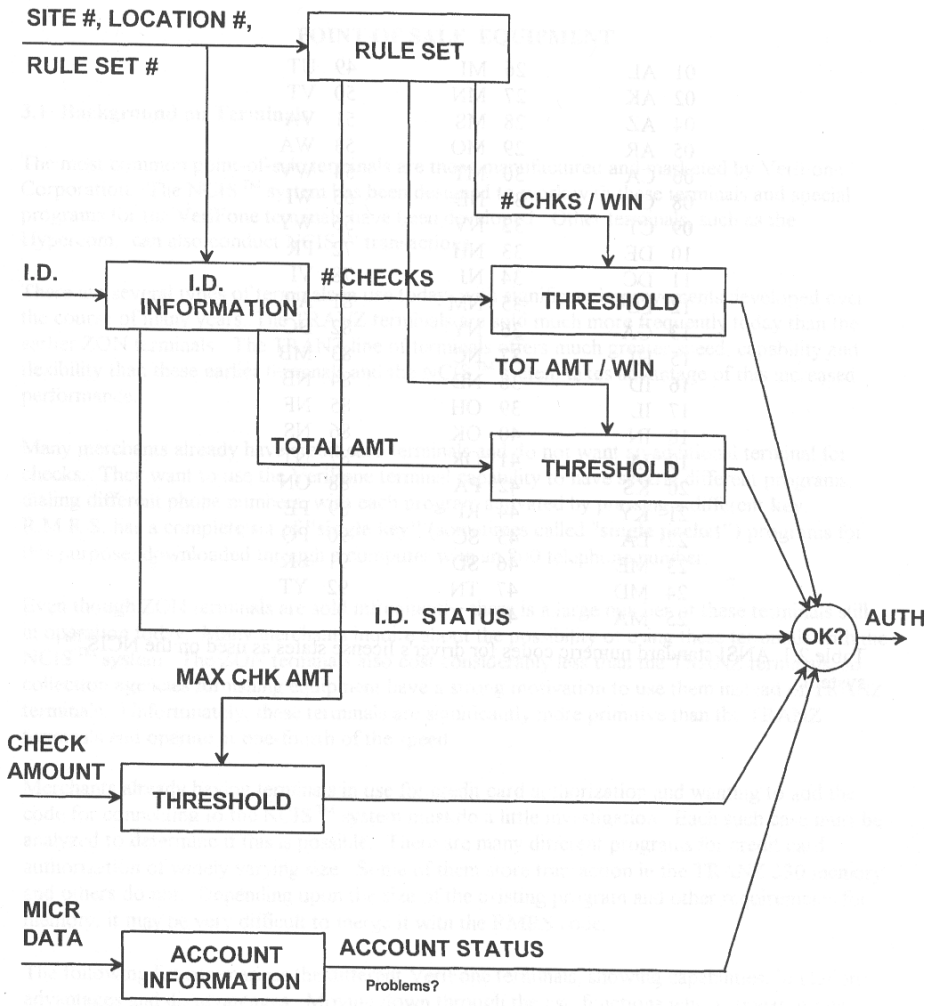


Figure 2-5. Logic for processing payroll check transactions.

Using this table will give compatibility with NCN, enable use of NCN for backup of Velocity PLUS® systems, and provide standardization with the most common convention in use today. The ANSI standard used on NCN is given in Table 2-1

Table 2-1. ANSI standard numeric codes for driver's license states as used on the NCN system.

01 AL	26 MI	49 UT
02 AK	27 MN	50 VT
04 AZ	28 MS	51 VA
05 AR	29 MO	53 WA
06 CA	30 MT	54 WV
08 CO	31 NE	55 WI
09 CT	32 NV	56 WY
10 DE	33 NH	72 PR
11 DC	34 NJ	78 VI
12 FL	35 NM	81 AB
13 GA	36 NY	82 BC
15 HI	37 NC	83 MB
16 ID	38 ND	84 NB
17 IL	39 OH	85 NF
18 IN	40 OK	86 NS
19 IA	41 OR	87 NT
20 KS	42 PA	88 ON
21 KY	44 RI	89 PE
22 LA	45 SC	90 PQ
23 ME	46 SD	91 SK
24 MD	47 TN	92 YT
25 MA	48 TX	

NCN
NATIONAL CHECK NETWORK

Section
3

NCN Toolkit

In this section...

3 - NCN Tool Kit

All members of NCN need to transfer daily negative file updates to the NCN computer.

The NCN Communication Toolkit is provided to satisfy this requirement and provide other capabilities as well. This chapter explains how to install and use the basic Toolkit.

“Toolkit Installation” covers installation of the Toolkit. “Concise Overview – Toolkit Use for File Communication” provides a concise overview of the use of this Toolkit. “Exception Files” gives important information regarding “exception files”. **It is critical that NCN users understand this section!** “Frequently Asked Questions” gives miscellaneous information in a “question and answer” format. “Rule Set Functions” and beyond must be consulted if rule sets, transactions logs, billing files, and compliance reports are to be manipulated.

The Toolkit performs the following functions:

Send negative files to NCN and retrieve any resulting exception files. “General File Transmission” for the basic commands see “Exception Files” on page 3-4 for more information on the exception files.

Create, retrieve, modify, and send rule sets into NCN. “General File Transmission” for the basic commands and “Rule Set Functions” for details on all aspects of rule set maintenance.

Retrieve and process transaction log files created by NCN. Using the SFTP program over the internet to retrieve files and use the DOS based toolkit to translate the files downloaded from the SFTP server only into ASCII format if desired, and import them into a special data base for further processing. “Transaction Log Utilities” on page 5-1 describes how to create special billing files from the data base that contains transaction log file information.

“Printing a Transaction Activity Report” on page 7-1 gives the steps for creating printed reports based on the billing files. “Building the Compliance Report Database” on page 8-1 describes several different compliance reports that use the transaction log file data base and the incremental negative files sent to NCN.

“““summarizes the flow of transaction log file information as the Toolkit creates the various files and reports described in item 3 above. It shows the sequence of processing steps and the various intermediate results, and it gives the references to specific chapters that describe the different steps in detail.” on page 3-2 summarizes the flow of transaction log file information as the Toolkit creates the various files and reports described in item 3 above. It shows the sequence of processing steps and the various intermediate results, and it gives the references to specific chapters that describe the different steps in detail.” on page 3-2 summarizes the flow of transaction log file information as the Toolkit creates the various files and reports described in item 3 above. It shows the sequence of processing steps and the various intermediate results, and it gives the references to specific chapters

that describe the different steps in detail." on page 3-2 summarizes the flow of transaction log file information as the Toolkit creates the various files and reports described in item 3 above. It shows the sequence of processing steps and the various intermediate results, and it gives the references to specific chapters that describe the different steps in detail.

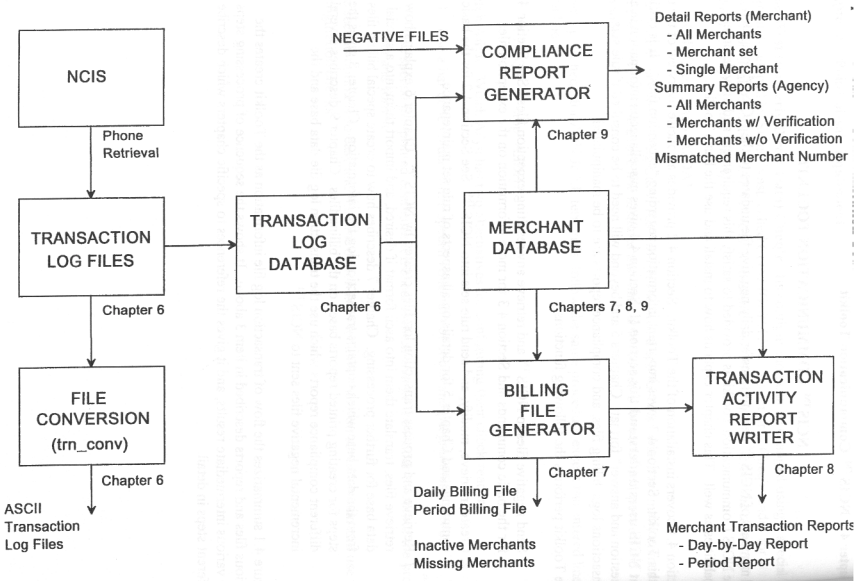


Figure 3-1. Diagram showing sequence of steps in processing transaction log files.

Toolkit Installation

Install the programs in the order given below. The instructions assume that the programs are being installed to hard drive **c:** from floppy drive **a:** The Toolkit software requires Windows 95, 98, ME or Windows NT in order to operate. All of the "Windows" programs are 32 bit programs and does not run under Windows 3.x.

To install the Toolkit:

1. Insert the **DISK 1** into the a: drive

2. Click on **START**, then **RUN**, and enter "**a:setup**" in the dialog box

3. Insert additional diskettes when prompted.

4. At the end of the installation, you must apply the **CONFIG** disk. Insert the fourth disk into the floppy drive and from the **RUN** dialog box, type **a:config a: c:** It copies a single file (**fcomparm.dat**) that is necessary for making connections to the NCN system.

NOTE

The disk set has been customized with site-specific data already set properly for your site in the file, **fcomparm.dat**. In unusual cases, it may be necessary to modify this file by typing "edit **c:\NCIS\fcomparm.dat"** (to change com port, phone number, etc) .

The file **fcomparm.dat** contains parameter information used for making and controlling a modem connection and a couple of other parameters that control printing. The typical contents of that file are shown below; only the first two fields are read with the remainder treated as a free form comment:

comport 2 Set serial port for modem to use

baudrate 38400 Set serial port send/receive rate

phonenbr 13034424596 Set phone number to dial to reach NCN

sitenbr ??? NCN site number

password ???????? NCN password for this site

linkstats no Diagnostic use only with US Robotics 28.8

lmargin 15 Left margin for rule set display/printing (0...40)

nendlines 0 # lines between rule sets (0 = form feed) (0...10)

The installation also sets up icons for Windows 95, 98, ME, 2000 shortcuts and supply an entry on the **START** menu.

Concise Overview – Toolkit Use for File Communication

The file communications programs run from a DOS window under "Windows 95".

..... switch to the c:\NCIS subdirectory, then.....

Negative File Functions

To send a negfile use the SFTP software over the internet.

General File Transmission

To fetch files (normally used only to retrieve report files or program updates) type:

getfile <filelist> <ENTER>

NOTE
path info ignored in above <filelist>.

To send regular files type:

sendfile <filelist with optional paths> <ENTER>

Rule Set Functions

To edit or create a rule set for submission to NCN (See “Creating and Editing Rules Set Files on the Local Computer” on page 4-1 type:

rulemain <ENTER>

To send or fetch or delete a rule set to/from NCN (see Chapter 5 NCN Rule Set Maintenance for further information) type:

NCISrule send 789 <ENTER>

or

NCISrule fetch 789 <ENTER>

or

NCISrule delete 789 <ENTER>

Review Results of any Communications Action

To view "session log file" (the "session log file" contains a step-by-step report of the progress and results of each Toolkit communication session) type:

showlog <ENTER>

To erase "session log file" (the "session log file" continues to grow with each session so it should be erased periodically). To do this, type:

eraselog <ENTER>

Exception Files

One of the key features of NCN is its database integrity. Toward that end, all negfiles that are received at NCN are extensively examined, record by record, to detect errors. When an error is detected in a record, that record is written to a file. We call such files "exception files".

There are two kinds of exception files: "format exception" files, and "purge exception" files. When NCN processes a received negfile, either one or both of the above files may be generated.

A "format exception" file contains records from the negfile that have some form of format error. For example: a field may be missing; a required field may present but empty; a numbers only field may contain letters; a field may contain too many characters; a driver's license form may be invalid for the specified state; etc.

A “purge exception” file contains records from the negfile that specified a payment of a specific unpaid item, but that unpaid item could not be found in the database. Such records can arise for a number of reasons: the unpaid item record was never received; the record was received but a format error caused it to be rejected; the payment record was typed wrong at data entry; etc.

Because negfiles need to applied in strict order, NCN enforces the following rule:

> *A new negfile is not be accepted by NCN if a previous negfile had any errors. Instead of accepting the negfile, NCN returns the error file (or files) (the exception files). It is required that those error files be corrected, and submitted with name unchanged to ensure that negfiles are applied in correct order.*

Frequently Asked Questions

The Frequently Asked Questions section provides additional detail on the use of the Toolkit in a “question and answer” format. The most important material is enclosed in boxes for emphasis.

Question: What does NCN stand for?

Answer: NCN is an acronym for “National Check Network”, a state-of-the-art, highly cost effective, centralized check verification system operated by Rocky Mountain Retail Systems in Boulder, Colorado.

Question: Is there anything else I need?

Answer: Yes. A US Robotics Sportster V.34 56K data/fax modem and an available serial port on your computer. An alternate modem that is supported by the Toolkit is the SupraFaxModem 14.4

Question: What's so great about the US Robotics Sportster 56K?

Answer: It's the modem used at NCN to receive your calls and it's always best to use matching modem types for hassle free calls.

- It lets the file transfers go FAST!
- Two independent modem testing organizations evaluated major brands of 28,800 baud modems and found the US Robotics modem to be measurably superior.

Question: What's in that fcomparm.dat file that I need to edit?

Answer: fcomparm.dat (file communications parameter data file) contains information that tells the Toolkit utilities what serial port the modem is connected to, what speed to use with the serial port, your NCN site number, your NCN password, and the digits to dial to reach NCN.

Question: Why do I need an NCN site number?

Answer: NCN “tags” information received from you with this number for your protection and for the protection of others. It is an integral part of the system for insuring database integrity for check verification.

Question: Why do I need to set a baud rate to use with the serial port? Why don't you just let it go as fast as possible?

Answer: Normally we recommend that the serial port baud rate be set at 57,600 (or at 115,200 if your serial port uses a 16550 UART and your computer is fast enough). The modems then connect at their highest supported speed. But if the phone connections that you can establish from your location won't support this speed, then by setting the serial port baud rate to 9600, the modems does not try to connect at more than 9600 baud.

Question: Why do I need to send files to NCN?

Answer: This is how your “returned check” and “check paid” information gets to NCN for incorporation in the database. We call the files that contain these records “negfiles” (a concatenation of “negative files”). It’s also the way that “rule sets” are added and changed.

Question: How do I send a “negfile” to NCN?

Answer: Switch to the Toolkit subdirectory (type: cd \NCN)

- Type: negfile a:\negs\myname.net

Question: I notice that when I send a negfile to NCN that it does some kind of compression and also renames the file from the one I provided on the command line to some other name. What's going on here?

Answer: Negfiles are always compressed for speed of transmission and because NCN expects them to be compressed. The name is changed to include your NCN site number and an extension that is incremented for each negfile transmission so that negfiles aren't accidentally overwritten.

Question: I tried to send a negfile to NCN and it refused to accept it with a message that some file or other had to cleared. What's that mean?

Answer: A previous negfile contained one or more errors. The erroneous records are put in?????.nfx or?????.pgx where????? is your NCN site number. Until such errors are dealt with, NCN continues to refuse new negfiles. This is done to ensure that adds and deletes are performed in the correct order. The offending files were automatically sent back to your computer when the new negfile was refused. You must correct these files and resubmit. Format exception corrections should be submitted before purge exception corrections when both are present.

- edit the error file to fix the offending records

- type negfile ?????.nfx to send the "format" corrections or type negfile ?????.pgx to send the "purge" exceptions

Question: Why would I need to fetch files from NCN?

Answer: This provides a way to retrieve activity reports, accounting reports, new releases of the Toolkit, new documentation, etc.

Question: If you're making sensitive and proprietary information retrievable as files, what's to keep some other NCN site from looking at my data?

Answer: Private files are given a name that includes the site number of the NCN site that "owns" the files (such as rep01012.dat). They can only be fetched by the matching NCN site. Other sites receive an "access denied" response if they attempt to fetch another site's file.

Question: How do I "fetch" files from NCN?

Answer: Use this procedure:

a. Switch to the Toolkit subdirectory (type: cd \NCIS)

b. Type: **getfile rep01012.dat,document.zip**

NOTE
path information should not be included. It is ignored if present

Question: Where do files "fetched" from NCN end up in my computer?

Answer: They are always placed in the subdirectory from which the getfile command was typed (usually \NCIS).

Question: How do I send a regular files (not a negfile) to NCN?

Answer: Use this procedure:

a. Switch to the Toolkit subdirectory (type: cd \NCIS).

b. Type: sendfile d:\rawdata\trash.zip,\report\00109.dat

Question: Why are there two file sending utilities?

Answer: NCN treats negfiles differently than regular files and expects them to be compressed a certain way and named a certain way. Rather than bothering you with these details, we provided a special utility for sending negfiles that takes care of these details for you. In addition, negfiles must be submitted singly and in correct sequence and sometimes result in the return of error files instead of acceptance of the negfile.

Question: Is there some kind of log that's kept on my computer of the file transfers that I have done?

Answer: Yes. Each file transfer session is recorded in file.log in the subdirectory from which the utility was invoked.

NOTE

This file could grow large if many file transfers are done, so occasionally it should be deleted. It is recreated by the next file transfer session.

Question: How can I look at the file transfer log file?

Answer: Type: showlog

Question: How can I erase the file transfer log file?

Answer: Type: eraselog

Question: What do I do if I cannot get the US Robotics modem that you recommend and my boss insists that we use one that we already have?

Answer: A: 1) Try it. It might work. However, it doesn't work, examine the file NCISmodm.sup This file is used as the source of setup strings that are sent to the modem to configure it for use. Read that file. It contains comments that tell what modem configuration is needed. Grab the manual for the modem you want to use and have at it.

Question: Would NCN prepare a custom modem setup for our favorite modem?

Answer: Yes, but reluctantly, and only if:

a. You send a modem manual, and

b. a check for $250 is included with the manual.

Question: What if I need to send or receive lots of small files?

Answer: You following methods are used:

a. Use pkzip to “zip” a bunch of files for sending. This has the beneficial side effect of compressing them at the same time.

b. If NCN is sending a bunch of files at once, the file extension is .zip and you need to use pkunzip to process it.

c. PKZIP and PKUNZIP are included in the Toolkit but please note that they are “shareware” and if you use them regularly, the authors deserve a payment. Read the order.doc and sharewar.doc files for details.

Question: When I do a file transfer with one of the Toolkit utilities, it says “press ESC at anytime to abort this program”. What does this do and what happens to the file being transferred?

Answer: The file transfer utility programs periodically look for characters from the keyboard. If an ESC (escape) key is found to have been pressed during a file transfer, that transfer is terminated and any partially received file is deleted.

Question: What happens to a file being transferred if the phone connection is lost or the modem turned off?

Answer: Only files that are received in their entirety are preserved. Any partially received file, for whatever reason, is deleted.

Question: Can I compress and decompress individual files without using pkzip and pkunzip?

Answer: Yes. Use rmrscomp to compress a single file and rmrsdcmp to decompress an individual file.

Question: One time I invoked a Toolkit utility and got a “help” screen. How did that happen?

Answer: Some Toolkit utilities require one or more command line argument. If they are invoked with the wrong number of arguments, all utilities retaliate by displaying a “help” message.

Question: What do the files on the Toolkit disks do?

Answer: fcomparm.dat = holds comport assignment, site number, password, etc.

The file descriptions follow:

Table 3-1. Toolkit Disk File Descriptions

File Name	Description
list.com	utility to “view” text files.
getfile.exe	utility to “fetch” files from NCN
negfile.exe	utility to send a “negfile” to NCN
sendfile.exe	utility to send general files to NCN
pkunzip.exe	PKWare program to “unzip” “zipped” files.
pkzip.exe	PKWare program to “zip” files.
rmrscomp.exe	RMRS utility to compress a single file.
rmrsdcmp.exe	RMRS utility to decompress a single file.
rulemain.exe	utility for creating, editing, printing rule sets.

Table 3-1. Toolkit Disk File Descriptions

File Name	Description
NCISrule.exe	utility send, fetch, and delete rule sets at NCN
NCIStget.exe	utility to retrieve transaction logs from NCN
showtlog.exe	Windows program for building and viewing a transaction log database.
billing.exe	Windows program for generating ASCII detail billing files, summary billing files, and maintaining merchant info.
sn.bat	batch file negfile send with errorlevel reporting
showlog.bat	batch file used to simplify display of file.log
eraselog.bat	batch file used to simplify deletion of file.log
errlevel.bat	batch file for interpreting DOS errorlevel returns from getfile.exe,negfile.exe, and sendfile.exe
NCISmodm.sup	modem setup file (to configure attached modem)
usr28800.mdm	US Robotics 28,800 setup file
supra144.mdm	SupraFaxModem 14.4 setup file
NCISfget.hlp	“help” file used by getfile.exe
NCISfsnd.hlp	“help” file used by sendfile.exe
NCISnsnd.hlp	“help” file used by negfile.exe
NCISrule.hlp	“help” file used by NCNrule.exe
NCIStget.hlp	“help” file used by NCNtget.exe
order.doc	PKWare instructions for registering their shareware
sharewar.doc	PKWare discussion of shareware
seqnbr.dat	used to add advancing numeric ext to negfiles
rule_hdr.txt	header information used when printing rule sets
file.log	maintains a running log of file transfer sessions
dlog.*	database tables for transaction log database
tlog.*	database tables for transaction log database
idapi.cfg *	Borland Database Engine configuration file

Table 3-1. Toolkit Disk File Descriptions

File Name	Description
* Borland Database Engine disks. These are to be installed ONLY if: Transaction log files are to be retrieved and manipulated using the Windows programs showtlog.exe and billing.exe	

NCN
NATIONAL CHECK NETWORK

Section
4

NCN Rule Set Maintenance

In this section...

- Creating and Editing Rules Set Files on the Local Computer
- Communicating Rule Set Information to NCN
- List of Rules that can be Edited

4 - NCN Rule Set Maintenance

NCN rule sets control the way that verification requests from point-of-sale utilize information contained in the NCN database to arrive at a recommendation to be returned to the point-of-sale terminal display. The "NCN Communication Toolkit" provides a way to maintain these rule sets on a computer at your site and to submit them electronically to NCN. This gives you total control over the way the NCN system conducts verifications on behalf of your clients. An electronically submitted rule set takes effect immediately so you can be extremely responsive to client requests to modify the way their verifications are conducted.

Creating and Editing Rules Set Files on the Local Computer

1. Switch to the subdirectory that contains the NCN Communication Toolkit. (**c:\NCN**)

2. Invoke the rule set maintenance utility by typing **rulemain <enter>**
   The system displays:

   Starting rule set maintenance program for NCN site?????

   @ The**?????** represents your site number and is filled in automatically. The information about your site is maintained in **\NCIS\fcomparm.dat**.

   The @ symbol indicates that the program is waiting for a command. All commands are single character. A list of these commands can be obtained at any time by pressing the space bar. (Actually, pressing any key that is not a valid command key displays a list of valid commands. The following list appears:

   press r to Read in new rule set
   press d to Display current rule set
   press p to Print current rule set
   press e to Edit current rule set
   press s to Save current rule set
   press x to eXit program

3. Always start by reading in the rule set that is be created or modified. It becomes the "current rule set" referred to above and all subsequent operations are conducted on that rule set. Do this by typing an "r" after the @ prompt. You are prompted to enter the number of the rule set to be read. If the rule set specified does not yet exist, it is created by reading rule set 0 instead. Thus, rule set 0 serves as a "master" that you can customize.

   This is a useful time-saver because most rule sets contain similar or identical values. When the rule set is read, an automatic display of all rules defined in the rule set is sent to the screen. At this point, you are ready to edit the rules.

4. To edit rules in a rule set, type **e** at the **@** prompt. You are prompted to specify the rule you want to edit. (All rules are specified by either a number or a number-letter combination. All list of all such rules is included at the end of this chapter. As mentioned earlier, detailed information about the rules is available in Appendix B of the Instruction Manual.) Type the rule to be edited and press enter. If the rule specified exists, a prompt appears that further identifies the rule. At this point, you may type the new value. All values are checked for being in a legitimate range and are automatically converted to proper values if found invalid.

5. Use the **d** command (Display) to display on the screen the current rule set values.

6. Use the **p** command (Print) to print the rule set to an attached printer (assumed connected to LPT1:).

NOTE

The header that is printed should be edited to reflect your agency name and address and site number.

The file that contains this information is: **rule_hdr.txt** In addition, there are two other parameters that affect the appearance of printed output. These parameters are set in the file **\NCIS\fcomparm.dat** The first parameter is **lmargin**; it controls the left margin of the rule set. The default setting is 15, which centers the output. It may be set to any value between 0 and 40 inclusive. The other parameter is **nendlines**; it controls the number of blank lines that are output to separate rule sets when more than one is printed in a session. Legitimate values are from 0 to 10 inclusive. The value 0 is the default and has special meaning: at this setting, each rule set is printed starting on a new page with a new header as well; this is the default. If **nendlines** is non-zero, the header is printed only for the first rule set with subsequent rule sets separated from the previous rule set by **nendlines** blank lines.

7. At any point, the rule set file can be "saved" by typing the **s** command (Save).

8. When finished, exit the program by giving the **x** command (eXit). If a rule set has been modified but not saved, a prompt appears giving the option of saving the file before the program shuts down.

NOTE

Edit rule set 0 at an early stage and put in it the "base" rule set for your agency. Rule set 0 then serves as a template from which subsequent new rule sets can be derived any time you "read" a rule set that is not yet defined.

Rule set files are kept in the same subdirectory as the NCN Communications Toolkit (usually **c:\NCN**). The naming convention is: **rulennnn.dat** where **nnnn** is the rule set number with leading zeroes as required to give a 4 digit number. **Do not attempt to edit or delete these files directly!** They should be modified using the rulemain and NCNrule program.

You may want to find out what rule set files exist on your system. This can be done by typing: **dir rule????.dat <enter>**. This produces a listing of all files that match the naming convention given above.

Communicating Rule Set Information to NCN

To communicate rule set information to the NCN application, switch to the subdirectory that contains the NCN Communication Toolkit and enter one of the following:

- To send rule set 789 to NCN type: **NCISrule send 789 <enter>**
- To delete rule set 110 at NCN type: **NCISrule delete 110 <enter>**
- To fetch rule set 102 from NCN type: **NCISrule fetch 102 <enter>**

TIPS:

a. If **NCISrule send** is performed after each rule set modification by **rulemain**, then the local copy of the rule sets match what is contained by NCN.

b. Deleting a rule set is an infrequent occurrence, but if it must be done, always use **NCISrule delete** to perform the function. If NCN reports that it successfully performed the deletion, then, and only then, is the local copy deleted. This ensures that NCN has the same collection of rule sets as those on the local computer.

List of Rules that can be Edited

The following table list the rules that can be edited.

Table 4-1. List of Rules that can be Edited

#	Definition
2	Rule set number
3	Terminal prompt (1 to 16 chars)
4	Group number
5	**Tender sequence options**:
5a	Return reason list to terminal
5b	Require ID if account has none
6	**Transaction limits:**
6a	Check amount requiring ID
6b	Maximum check amount allowed
6c	Cash back amount requiring ID
6d	Maximum cash back allowed
7	**Day velocity limits:**
7a	Number of checks from anywhere

Table 4-1. List of Rules that can be Edited (Cont.)

#	Definition
7b	Number of checks from site/group
7c	Number of checks from site/location
7d	Cum amt - checks from anywhere
7e	Cum amt - checks from site/group
7f	Cum amt - checks from site/location
7g	Cum cbk - checks from anywhere
7h	Cum cbk - checks from site/group
7i	Cum cbk - checks from site/location
8	Personal check activity window.
9	**Window velocity limits:**
9a	Number of checks from anywhere in window
9b	Number of checks from site/group in window
9c	Number of checks from site/location in window
9d	Cum amt - checks from anywhere in window
9e	Cum amt - checks from site/group in window
9f	Cum amt - checks from site/location in window
9g	Cum cbk - checks from anywhere in window
9h	Cum cbk - checks from site/group in window
9i	Cum cbk - checks from site/location in window
10	Maximum payroll check amount allowed
11	Payroll check activity window
12	**Payroll check velocity limits:**
12a	Number of payroll checks in window
12b	Cum amt - payroll checks in window
13	**Payroll ID approval requirements:**
13a	Payroll ID must be approved somewhere
13b	Payroll ID must be approved for site/group

Table 4-1. List of Rules that can be Edited (Cont.)

#	Definition
13c	Payroll ID must be approved for site/location
13d	Manager approval reqd for payroll IDs
13e	Manager approval reqd for payroll accounts
14	**Unpaid check limits:**
14a	Number of unpaid items from anywhere
14b	Number of unpaid items from site/group
14c	Number of unpaid items from site/location
14d	Cum amount of unpaids from anywhere
14e	Cum amount of unpaids from site/group
14f	Cum amount of unpaids from site/location
15	Federal Reserve Districts deemed local
16	**Young account time periods:**
16a	Num days a 'local' account is 'young'
16b	Num days an 'out-of-area' account is 'young'
17	**Transaction limits for young accounts:**
17a	Check amount requiring ID.....(young account)
17b	Maximum check amount allowed...(young account)
17c	Cash back amount requiring ID..(young account)
17d	Maximum cash back allowed.....(young account)
18	**Day velocity limits for young accounts:**
18a	Num checks from anywhere.....(young acct)
18b	Num checks from site/group.....(young acct)
18c	Num checks from site/location....(young acct)
18d	Cum amt - from anywhere.....(young acct)
18e	Cum amt - from site/group.....(young acct)
18f	Cum amt - from site/location.....(young acct)
18g	Cum cbk - from anywhere.....(young acct)

Table 4-1. List of Rules that can be Edited (Cont.)

#	Definition
18h	Cum cbk - from site/group.....(young acct)
18i	Cum cbk - from site/location.....(young acct)
19	**Window velocity limits for young accounts:**
19a	Num checks from anywhere in win..(young acct)
19b	Num checks from site/grp in win..(young acct)
19c	Num checks from site/loc in win..(young acct)
19d	Cum amt - from anywhere in win...(young acct)
19e	Cum amt - from site/gro in win...(young acct)
19f	Cum amt - from site/loc in win...(young acct)
19g	Cum cbk - from anywhere in win...(young acct)
19h	Cum cbk - from site/gro in win...(young acct)
19i	Cum cbk - from site/loc in win...(young acct)
20	**Response messages:**
20a	Approval msg (1 to 9 chars)
20b	Warning msg (1 to 16 chars)
20c	Decline msg (1 to 16 chars)
21	**ID flagged options:**
21a	ID flagged for: assoc acct has problem
21b	ID flagged for: marked 'stopped'
21c	ID flagged for: marked 'stolen/forged'
21d	ID flagged for: special purpose #1 marked
21e	ID flagged for: special purpose #2 marked
21f	ID flagged for: special purpose #3 marked
21g	ID flagged for: special purpose #4 marked
21h	ID flagged for: special purpose #5 marked
22	**Decline/Warning choices:**
22a	Msg for: account is stopped.....(D/W)

Table 4-1. List of Rules that can be Edited (Cont.)

#	Definition
22b	Msg for: over unpaid item limit.....(D/W)
22c	Msg for: over single transaction limit....(D/W)
22d	Msg for: over activity limit for day.....(D/W)
22e	Msg for: over activity limit for window...(D/W)
22f	Msg for: account is not 'local'.....(D/W)
22g	Msg for: ID with regular acct flagged...(D/W/I)
22h	Msg for: ID with payroll acct flagged...(D/W/I)
23	Group set
24	Canadian checks accepted
25	Manager password for payroll auths

Rule Set Parameter Definitions

This section explains the items used in specifying a rule set. Each item is referenced by number or number-letter.

- **NCN site number**. This number was assigned to your agency by Rocky Mountain Retail Systems when you became a member of NCN. It is used to “tag” your contributions to the database and must also be placed in the VeriFone terminals at your customer locations so that verification transactions can be “tagged” with your site number (see note following item 2 for additional information).

- **Rule set number**. This must be a number between 1 and 9999. This number must be placed in the VeriFone terminals at your customer locations and causes verification transactions from that terminal to be evaluated using that set of “rules”. The “rules” are primarily limits placed on such things as check-passing activity and the face amount of the checks.

The rule set number is made up of the following:

The first field of any verification request packet sent to NCN must contain a terminal ID (sometimes called merchant ID) that includes an NCN site number, a merchant number, and a rule set number.

Following is a valid terminal ID:

3718-812759-22

Where: 3718 is the NCN site number, 812759 is the merchant number, and 22 is the rule set that is applied to transactions from this terminal. The merchant number may be freely assigned by an NCN site and can contain from 1 to 6 digits.

NOTE

Terminal idle prompt. This field of 16 characters is displayed by VeriFone terminals (except the ZON Jr PLUS) when a terminal begins a check verification transaction. Any word or phrase may be used, but it is preferable to choose a name that includes some reference to the rule set number and to your agency. This practice provides a way to easily determine which rule set is being invoked by transactions from a particular terminal. This is a required rule set item and may not be left blank.

NOTE

The NCN software sends a response packet back to the point-of-sale terminal that includes the above mentioned "terminal idle prompt" as the first 16 characters. Most VeriFone terminals can strip this idle prompt off and then display the remainder of the message for the clerk. ZON Jr PLUS terminals lack the capability to separate this idle prompt from the rest of the message, so such terminals display the received idle prompt upon completion of the transaction. On ZON Jr PLUS terminals, the clerk must then press the "9" key to scroll the display to the right in order to see the response to the verification request. This is easier for clerks to remember if the idle prompt is more descriptive, e.g. "PRESS 9 FOR ANS" for those locations using ZON Jr PLUS terminals.

- **Group number**. This field allows selection of data from a group of merchants (usually a specific store chain or merchants with similar characteristics). Its use is for excluding NCN database information that is not "tagged" with the matching site and group number during the evaluation of a transaction. When specified, it should be a number between 1 and 99 inclusive and rule set item 23 (Group set) must be specified as well.

- **Point-of-sale options** affect what is shown on the terminal display at the completion of a verification transaction.

- **5a Return reason list.** Selecting this option makes detailed information available at the point of sale terminal whenever a check is not authorized. Thus, in addition to either a warning or a decline message, "scrolling" the terminal reveals more detail such as which limits are exceeded, the break down of unpaid checks by site/location, site/group, and total system, the name and telephone number of the agency (or agencies) that holds any unpaid check items, etc.

- **5b Require ID if none.** Selecting this option causes the NCN system to examine whether the micr account specified in the verification request packet has at least one ID associated with it. If it does not, and the verification request packet from the POS terminal did not include an ID, then the transaction is refused with a message returned to the terminal stating ID IS NEEDED. At this point, the transaction must be repeated using a "key" that allows an ID to be entered as part of the transaction. This option should ONLY be used when the point-of-sale terminal has the capability of prompting for an ID and including this in the verification request packet.

- **Single transaction limits** apply to amounts involved in an individual verification request.

- **6a Amount requiring ID.** This sets the limit on the amount of a check that requires an ID to be included in the verification request packet.

NOTE

For this particular limit (6a) 0 is treated as special case. If 0 is used for this limit, it is always considered to be exceeded. This in turn forces an ID to be required for all checks, a feature that is used by agencies that are offering a check guarantee service through NCN.

- **6b Maximum check amount.** This sets the maximum amount of a check that is approved.

- **6c Cash back requiring ID.** This sets the maximum cash that can be returned without supplying an ID in the verification request packet. This option is only usable when the point-of-sale terminal prompts the clerk for both the check amount and the sale amount. Only then can "cash returned" be calculated.

- **6d Maximum cash back.** This sets the maximum cash that can be returned. This option is only usable when the point-of-sale terminal prompts the clerk for both the check amount and the sale amount. Only then can "cash returned" be calculated

- **Single day activity limits** are used to set limits on the cumulative number or amount of transactions for a specific account for the current day. Which transactions are added together can be: unrestricted (from anywhere); restricted to transactions from a particular site/group set; tightly restricted to transactions from a particular site/location.

- The **personal check activity window** option sets the number of days of information that are to be included in measuring the activity (often this is referred to as "velocity") of an account. This can be set from 1 to 14 days. A setting of 1 includes only today's activity. A setting of 2 includes today and yesterday.

  Personal check "window" limits are applied against the cumulative activity that has occurred on an account during the activity ("velocity") window specified by rule set item 8.

  Maximum payroll check amount. Sets the maximum face amount of a payroll check that is accepted.

  Payroll activity window. Set the activity "window" for payroll checks.

  Sets **limits on payroll check cashing activity** accumulated within the activity "window" set by item 11.

NOTE

Payroll check cashing activity is accumulated against the ID that is presented as a required part of the transaction.

12a **Number payroll checks per window.** Sets limit on the number of payroll checks cashed using a particular ID within the "window" period of days.

12b **Amount payroll checks per window.** Sets limit on the cumulative dollar amount of payroll checks cashed using a particular ID within the "window" period of days.

- **ID approval required.** IDs must be presented when a payroll check verification is conducted. Options 13a through 13d specify the level of approval required to make an ID acceptable for use in conjunction with payroll check cashing. Either 13a, 13b, or 13c must be “YES” to set the scope of approval required. Note that you cannot change 13a, 13b, or 13c to “NO”---you must set the desired option to “YES” and the others are automatically change to “NO”. Use 13d to determine whether such approval is automatic or requires a manager.

- **13d Manager required to approve payroll ID.** This option selects whether manager approval is required before an ID can be used for payroll check cashing. If such approval is required, the manager must use a specially programmed VeriFone terminal to communicate an ID approval packet to NCN. If manager approval is NOT required, then any ID submitted in conjunction with a payroll check transaction is automatically approved at the level specified by option 13a through 13c.

- **13e Manager required to approve payroll account.** This option selects whether manager approval is required before an account can be used as a payroll check. If such approval is required, the manager must use a specially programmed VeriFone terminal to communicate a payroll account approval packet to NCN. If manager approval is NOT required, then any account is accepted as a payroll account.

- **Unpaid check limits.** This group of options sets limits on the number of outstanding unpaid checks that are tolerated. Only in very unusual circumstances would a number other than 0 be used here. In fact, these options may be left blank, in which case the default is 0.

- **Federal Reserve list.** The first 2 digits of the transit/routing number indicate the Federal Reserve district where the bank is located that holds the checking account. The Federal Reserve districts are numbered 01 through 12. If a bank is a savings and loan institution rather than a full service bank, 20 is added to the Federal Reserve number where the savings and loan institution is located. In addition, 00 is reserved to indicate a US Government check and 80 indicates a traveller's check. NCN allows the use of the first 2 digits of the transit/routing number to indicate whether the check is to be considered “local” or “out-of-area”. If no entries are made for this option, all checks are treated as “local”. If one or more entries are made for this option, those banks and saving and loans that are in the listed Federal Reserve districts are treated as “local”.

NOTE

If 10 is entered, 30 is assumed, so there is no need to make an entry for a regular bank and another one for a savings and loan in the same district.

"Out-of-area" checks receive a message (usually a warning message, but a decline message may be sent if desired) indicating that the check is "out-of-area" unless there is one or more IDs associated with that account. Allowing the presence of an ID to override an "out-of-area" condition accommodates "naturally out-of-area" accounts such as those from college students or military personnel. Once an ID has been accepted by a local merchant, the account is treated as local, even though the Federal Reserve district may be far away.

- **Special limits for "young" accounts.** A new account is one that has never been "seen" by NCN. There are two ways an account becomes known to NCN: a verification transaction is conducted involving the account; a returned check drawn on the account has been entered in the NCN database. If an account becomes "known" through a verification transaction, there is no information, positive or negative, on which to base an authorization. In this case, many merchants want to use a different set of criteria (limits) in evaluating the verification request until enough time has passed for a check to clear and thus generate positive information. NCN allows for this by putting an account in the "new" category for a number of days specified by rule set items 16a (for "local" checks) and 16b (for "out-of-area"). Verification requests for accounts that are in the "new" state use the limits given in rule set items 17, 18, and 19.

CAUTION

Setting the new account hold period for either local checks or out of area checks to a non-zero value requires setting alternate limits (items 17-19) as well. Otherwise, any new account has NO limits until the end of the new account hold period.

- **16a New local account window.** This sets the number of days a never-before-seen "local" checking account is to be considered "new". Setting this number to 0 inhibits the use of an alternate rule set (limits 17, 18, and 19) for "local" checks. 0 to 14 days can be specified.

- **16b New out-of-area account window.** This sets the number of days a never-before-seen "out-of-area" checking account is to be considered "new". Setting this number to 0 inhibits the use of an alternate rule set (limits 17, 18, and 19) for "out-of-area" checks. 0 to 14 days can be specified.

- **New account transaction limits.** These are the same as rule set item 6 except that they are only applied to accounts that are in the "new" state.

- **New account single day velocity limits.** These are the same as rule set item 7 except that they are only applied to accounts that are in the "new" state.

- **New account window velocity limits.** These are the same as rule set item 9 except that they are only applied to accounts that are in the "new" state.

- **Point-of-sale messages.** NCN allows the authorization/warning/decline messages that are returned to the point-of-sale terminal to be customized. An example where this capability might be useful is if your agency wants all verification transactions other than authorizations to result in a message on the terminal requesting a call be made to a "help desk" to get an authorization. If no entries are made for rule set items 20a...c, the following defaults are used:

  Approval message: AUTH NUM 021-815

Warning message: MANAGER NEEDED

Decline message: DECLINE CHECK

For approval messages, a 6 digit (plus dash) transaction number is always appended, so only the first 9 characters are available for modification. In the default approval message shown above, 021-815 was the transaction number.

- **Bad ID criteria.** When an ID is included in a verification request packet, the NCN system looks to see if any negative information is connected to that ID. If any are found, the transaction is given an authorization. Because there are multiple sources of such negative information and there may be cases where a merchant does not want some of those reasons to cause an authorization failure, NCN provides a "mask" that permits each merchant to select which of the negative items are to be used in determining the goodness of the ID. Rule set items 21a through 21h allow the selection of such items. By default, if none of these items are marked as selected, NCN assumes that 21a, 21b, and 21c are "selected". 21d through 21h are not "selected".

NOTE

The use of special purpose ID "flags" 1 through 5 must be coordinated through NCN management.

- **Warning and Decline conditions.** This option determines which type of result message is returned to the terminal when particular conditions are detected during the verification request evaluation. If more than one condition is detected, the more "serious" message is returned to the terminal. Thus, if a condition was detected that would return a warning message together with another condition that would return a decline message, only the decline message is sent to the terminal, along with (if enabled by item 5a) the reason (or reasons) for all detected conditions. The defaults for this item are:

  2a= D Account Problem

  22b= D Unpaid Items

  22c= W Transaction Limit

  22d= W Day Velocity Limit

  22e= W Window Velocity Limit

  22f= W Out of Area

  22g= D ID Flagged (personal check)

  22h=D ID Flagged (payroll check)

- **Group set list.** This set of ten 2-digit numbers specifies the groups to be used for transaction activity and returned check limit tests for this rule set (see discussion of rule set item 4). If no groups are specified, all groups defined in the system are used, which is the same as accepting data from anywhere. There is no need to specify a group set unless a limit such as 7b, 7e, 7h, 9b, 9e, 9h, 18b, 18e, 18h, 19b, 19e, or 19h as been specified.

- **Canadian checks accepted.** When a check is used for micr input at point-of-sale, Canadian checks can be detected by the presence of a dash in the sixth position of the transit/routing field (ABA number). Some agencies may want to refuse verification for such checks due to collection difficulties. This option allows them to indicate to NCN whether or not to refuse Canadian checks. If this field is left blank, then Canadian checks are NOT accepted.

NOTE

If manual input of micr numbers is permitted at the point-of-sale terminal, it is not possible to detect Canadian checks unless the clerks can be trained to include a dash in the proper place.

- **Manager password for payroll authorizations.** The manager password is used for authenticating payroll ID and account authorization packets. It consists of three alphanumeric characters that must be keyed at the point-of-sale to be included with packets sent to NCN for authorizing IDs for use with payroll checks and authorizing specific micr accounts for use as payroll checks. This option is only relevant when either 13d and/or 13e have been set to Y (which is the default). The default password here is YES which, on a VeriFone terminal requires 11 keypushes to enter because of the alpha characters. The manager, to key YES, must press:

  9 <ALPHA> <ALPHA> <ALPHA> 3 <ALPHA> <ALPHA> 7 <ALPHA> <ALPHA> <ALPHA>

If the password contains leading, trailing, or imbedded spaces, these must also be keyed

NCN
NATIONAL CHECK NETWORK

Section
5

Transaction Log Utilities

In this section...

5 - Transaction Log Utilities

NCN records all verification transactions in a log file for each day. These daily logs are maintained for 10 days by the NCN system and can be downloaded to your site for use in answering customer inquiries and preparing billing files. This chapter describes how to download the transaction records for your site and how to add them to a database using a "Windows" program that allows specific records to be found and sorted in various ways.

It also explains how to use a utility that converts the binary transaction log records to a comma-delimited ASCII file for those cases where subsequent processing of transaction log files are done with programs developed in-house. Use the following steps:

1. Use the Toolkit utility NCIS **tget** to retrieve transactions for a specific day.

2. Use the "Windows" program **Import Tlogs** to import the raw log file retrieved in step 1 into a composite database that holds as many days of transaction records as you want to keep available.

   or

1. Use the Toolkit utility NCIS **tget** to retrieve transactions for a specific day.

2. Use the Toolkit utility **trn_conv** to produce a comma-delimited transaction log file for subsequent in-house processing.

Retrieving Transaction Records for your Site

Transaction files are given a date that is in the form **yyyymmdd** For example, April 15, 1996 would be specified as **19960415** Note that this format requires an 8 digit date. Use leading zeroes if either the month or the day are single digit. Thus January 8, 1996 would be specified as **19960108**

From a DOS prompt in the \NCN subdirectory, type **NCIS tget <date>** where the date is composed as described in the previous paragraph. For example:

c:\NCIS> NCIStget 19960327

retrieves the transaction log file for your site for March 27, 1996.

Alternately, the date of the file to retrieve can come from a file, TLOGDATE.DAT, in the C:\NCIS directory. (This option allows automation and automatic retrieval of the transaction log file in some systems.) When using this option, omit the date following "NCIStget" as shown above.

The log file retrieved by the above command is a binary file. The “Windows” program **showtlog** has been provided for use in viewing this “raw” transaction log.

NOTE

You are billed for connect time while retrieving transaction log files. The first minute or fraction thereof is billed at $2.00/minute. Subsequent minutes or fractions thereof are billed at $1.00/minute. Assuming the use of a 28.8 kbaud modem, until the transaction record exceeds 5000, the connect time is less than a minute.

Add Raw Transaction Log to Composite Database

Use the following steps to add a raw transaction log to a composite database:

1. Start up the "Windows" program **Import Tlogs** by clicking on the "shortcut" in the Windows 95/98/ME desktop screen.

2. Import the transaction log. Use DatabaseOps|Import Raw Log to accomplish this. If you have a number of consecutively dated transaction log files in a subdirectory, you may use DatabaseOps|Import Range Of Logs to process multiple transaction logs at once.

NOTE

Pressing CTRL-I invokes the import dialog directly.

To learn the **showlog** function, explore the various menu options.

The composite database is stored in the **\NCIS** subdirectory. You should be aware that a transaction record in raw form is 86 bytes in size. Importing that record to the composite database and the generation of 3 indices consumes approximately 232 additional bytes. After the raw file has been imported, it may be deleted to save disk space. In addition, when the composite database contains records that are older than some number of days, they should be removed from the database by using **DatabaseOps|Erase Entries By Date** (or typing **CTRL-E**). To erase a range of dates, use **DatabaseOps|Erase Date Range Of Logs**. To see what dates are in the composite database use **DatabaseOps|Show Contents** (or type **CTRL-C**).

NOTE

The composite transaction database is used as the source for producing billing records and so take care before removing transactions of a given date that they have been included in the billing database.

The Transaction Log View program also prepares intermediate information required by other programs. For example, the Compliance Report Generator uses a “by account” index as prepared by the Transaction Log View routine.To make this happen, select **Database Ops** and mark the “by account” index option.

CAUTION

ALWAYS MAKE THIS SELECTION IF YOU PREPARE COMPLIANCE REPORTS! This should cause a check mark to appear beside the option. Note that clicking a second time causes the routine to erase the “by account” index and remove the check mark.

Converting Transaction Logs to Comma-delimited ASCII Files

This utility is to be used whenever there is a need to import the log files into a database program of your own. Use the following steps:

1. From a DOS prompt in the **\NCIS** subdirectory, type:

   c:\NCIS> trn_conv 19960815.lgt d:\tlogs\19960815.asc

   The utility requires two command line parameters:

   - A path to the NCIS binary transaction log (the input file), and
   - A path to where the ASCII conversion is placed (the output file).

   To facilitate the use of “batch” files for automating the conversion process, **trn_conv** returns the following error codes that may be tested by the **IF ERRORLEVEL** “batch” command:

   0 Conversion successful...no errors found.

   1 Wrong number of arguments supplied on the command line.

   2 Could not find the input file (first filepath on command line).

   3 Could not open the output file (second filepath on command line).

   4 Input file was not a valid NCIS binary transaction log file.

   5 Error encountered while reading input file.

   6 Error encountered while writing output file.

Format of comma-delimited ASCII file

The output file is a comma-delimited ASCII file with each line (including the last line) terminated by a CR (carriage return: hex 0D) and a LF (line feed: hex 0A) character.

The following fields may sometimes be empty: check amt; cash back; check num; id; lane num; raw MICR. In particular, the raw MICR field only appears in transaction log files for sites conducting ACH transactions.

Num	Field Description	Example	Field Size and Limits
1	date	08/20/96	Fixed: 8 chars (Month/Day/Year)
2	time	13:29:31	Fixed: 8 chars (military time Hr:Min:Sec)
3	trn number	886076	Var: 1 to 6 digits (1...999999)
4	site number	353	Var: 1 to 5 digits (1...65535)
5	merchant #	76075	Var: 1 to 6 digits (0...999999)
6	rule number	1002	Var: 1 to 4 digits (1...9999)
7	group num	22	Var: 1 to 2 digits (0...99)
8	check amt	52	Var: 0 to 7 chars (empty... 9999.99)
9	cash back	10.00	Var: 0 to 7 chars (empty... 9999.99)
10	**ver result**	**DEC itw**	**Var: 4 to 12 chars (see explanation below)**
11	account	10288197812345	Var: 1 to 28 characters
12	trn code	R	Fixed: 2 chars (see explanation below)
13	check num	3510	Var: 0 to 10 digits (empty... 3999999999)
14	id	DL=CA-1897	Var: 0 to 23 characters
15	lane num	21	Var: 0 to 3 digits (empty... 255)
16	raw MICR	(see below)	Var: 0 to 40 characters (only ACH sites)

Examples:

08/20/96,13:29:31,886076,353,76075,1002,22,357.52,10.00,DEC itw,

10288197812345,iR,3510,DL=CA-1897,21,t123123123t 1234567o 101

08/20/96,15:33:02,876076,353,78,23,22,20.00,,AUTH,10288197812345,NU,,,

08/21/96,00:02:16,34,353,12,25,,,AUTH,10788197812345,NF,678,DL=CA-1897,

NCN returns one or more, single letter **reason codes** with every warning or decline. These correspond to the letters shown in Figs. 2.1 and 2.2. Table 5-1 lists the possible codes.

Table 5-1. Reason Codes Returned with Warning or Declines

Reason Code	Explanation
t	Transaction limit exceeded
d	Day velocity limit exceeded
w	Window velocity limit exceeded
o	Out of area check
u	Unpaid items exist on the account
i	ID flagged
a	Account problem
r	Re-presented check
y	Young account

NCN also provides a two-letter **transaction code** on every log entry. The first letter gives the **transaction type** and the second letter gives the **transaction condition.** The transaction type also shows if the data in the request were read automatically by a check reader or mag stripe reader, or manually entered. A capital letter implies automatic data entry while a lower case letter implies manual entry. Table 5-2 on page 5-6 lists the transaction type codes and Table 5-3 on page 5-6 lists the transaction condition codes.

Table 5-2. List of Transaction Type codes

Transaction Type	Explanation
"N" or "n"	Normal personal check
"P" or "p"	Payroll check
"T" or "t"	Third party check
"I" or "i"	ID based transaction
"B" or "b"	Blocked for ACH
"V" or "v"	Void of previous ACH entry
"L"	Log entry for information
"G" or "g"	Guaranteed check
"A"	Activation record for special transaction card
"C"	Card transaction

Table 5-3. List of the Transaction Condition Codes

Transaction Condition	Explanation
F	First presentation of a check
R	Repeat presentation of a check (personal)
D	Duplicate check (payroll)
U	Untestable presentation (no check number)
O	Override of prior warning for ACH
G	General purpose log entry
M	Mandatory accept (no verification)
Q	Query only

NCN
NATIONAL CHECK NETWORK

Section
6

Billing File Generator

In this section...

- The Day-by-Day File
- The Period Summary File
- Generating the Day-by-Day Billing File (rptxxxxx.blg)
- Generating the Period Summary File (rptxxxxx.bgs)

6 - Billing File Generator

Transaction logs can be downloaded from NCN and processed into simple ASCII text files that can be subsequently used for preparing statements or invoices to be sent to your merchants. The Billing File Generator is a Windows program that provides a means of building and maintaining a database that contains information about all the merchants that are using NCN through your company. That database, in conjunction with the transaction logs, can be used to prepare two basic types of ASCII billing files: a day-by-day file that contains one line per merchant per day summarizing activity for that day, and a period summary file that contains one line per merchant that summarizes the verification activity for a given date range (typically one month).

There are three possible verification messages returned to the point-of-sale terminal:

- AUTH
- WARNING
- DECLINE

In addition, NCN is able to distinguish “repeat” verifications of the same check from “first” verifications of that check. This is done by examining the check number supplied in the verification request packet. Thus, there are 6 possible verification results: “first” AUTH, “repeat” AUTH, “first” WARNING, “repeat” WARNING, “first” DECLINE, and “repeat” DECLINE. In addition, the transaction log can contain a variety of **other** entries, such as log entries from errors. As a consequence, there are 13 statistics that can be extracted from a transaction log file: the number of verifications results of each type (6), the dollar amount of each verification type (6), and the number of “other” entries (1).

The Day-by-Day File

There are two formats available for the day-by-day file. An example of each form is shown below utilizing the same source data so that the differences can be clearly shown. The examples are shown on two lines for clarity; in the actual file, each record is contiguous and terminated by a carriage return and line feed character.

The "original format" is identical to that used in older Velocity PLUS systems and is retained for use by programs written earlier (so-called "legacy" programs). It summarizes the 12 statistics in a convenient form: the first two data values sum verifications and amounts and this is usually all that is required for billing purposes. However, it drops the cents portion of amounts and adds all "repeats" together so that it is not possible to determine the "repeats" that were AUTHs versus WARNINGs versus DECLINEs. If this

level of detail is required, then the "enhanced format" must be used. The "enhanced format" includes each of the 12 possible statistics with no commingling of values. Thus it contains the most information, but imposes a heavier requirement on invoicing and statement generation programs to properly sum results

NOTE

In order to use the **Transaction Activity Report Writer** program, it is necessary to use the "enhanced" format. That is the only format accepted by that program.

Original format:

3,359,000010,Joes Flower Shop,19960424,

33,685,1,1,6,294,10,189

The interpretation of each field in the above record is as follows:

3,	Record type (fixed)
359,	NCN Site number
000010	Merchant number (zero padded to 6 digits)
Joes Flower Shop	Merchant name (always 16 characters or 6 digits)
19960424,	Date of activity (always 8 digits)
33,	Number of verifications performed of all types
685,	Total dollar amount of all verifications
1,	Number of “first” warnings given.
1,	Dollar amount of “first” warnings.
6,	Number of “first” declines given.
294,	Dollar amount of “first” declines given.
10,	Number of “repeat” verifications given (of all types).
189	Dollar amount of “repeat” verifications given

Enhanced format:

3,359,000010,Joes Flower Shop,19960424,

16,201.05,6,136.63,1,1.23,2,2.46,6,294.12,2,50.12,7

The interpretation of each field in the above record is as follows:

3,	Record type (fixed)
359,	NCN Site number
000010,	Merchant number (zero padded 6 digits)

Joes Flower Shop,	Merchant name (always 16 characters or 6 digits)
19960424,	Date of activity (always 8 digits)
16,201.05,	Number and dollar amount of “first” AUTHs
6,136.63,	Number and dollar amount of “repeat” AUTHs
1,1.23,	Number and dollar amount of “first” WARNINGs
2,2.46,	Number and dollar amount of “repeat” WARNINGs
6,294.12,	Number and dollar amount of “first” DECLINEs
2,50.12,	Number and dollar amount of “repeat” DECLINEs
7	Number of “other” entries

The Period Summary File

As in the case of the day-by-day file, there are two formats available: the "original format" and the "enhanced format". An example of each format is shown below.

Original format:

3,359,000010,Joes Flower Shop,19960401,19960430,

330,6841,10,10,60,2940,100,1881

The interpretation of each field in the above record is as follows:

3,	Record type (fixed)
359,	NCN Site number
000010,	Merchant number (zero padded 6 digits)
Joes Flower Shop,	Merchant name (always 16 characters or 6 digits)
19960401,19960430	Period covered by record
330,	Number of verifications performed of all types
6841,	Total dollar amount of all verifications
10,	Number of “first” warnings given.
10,	Dollar amount of “first” warnings.
60,	Number of “first” declines given.
2940,	Dollar amount of “first” declines given.
100,	Number of “repeat” verifications given (of all types).
1881	Dollar amount of “repeat” verifications given

Enhanced format:

3,359,000010,Joes Flower Shop,19960401,19960430,

160,2010.05,60,1360.63,10,10.23,20,20.46,

60,2940.12,20,500.12,29

The interpretation of each field in the above record is as follows:

3,	Record type (fixed)
359,	NCN Site number
000010,	Merchant number (zero padded 6 digits)
Joes Flower Shop,	Merchant name (always 16 characters or 6 digits)
19960401,19960430,	Period covered by record
160,2010.05,	Number and dollar amount of "first" AUTHs
60,1360.63,	Number and dollar amount of "repeat" AUTHs
10,10.23,	Number and dollar amount of "first" WARNINGs
20,20.46,	Number and dollar amount of "repeat" WARNINGs
60,2940.12,	Number and dollar amount of "first" DECLINEs
20,500.12,	Number and dollar amount of "repeat" DECLINEs
29	Number of "other" entries

General Information – Merchant Database and Billing File Generation

The Billing File Generator can prepare a list of "inactive merchants" and a list of "missing merchants" as it creates the billing files. An "inactive merchant" is one that is present in the Merchant Database but has no transactions in the selected date range. A "missing merchant" is one that has conducted transactions in the selected date range, but there is no entry in the Merchant Database. In addition, if a Merchant Database exists, the fourth field in the billing file is filled from the Accounting ID field of that database. If no merchant entry is found, the fourth field is defaulted to the 6 digit (zero padded) merchant number. If any of these features are to be used, it is necessary to build and maintain the Merchant Database. The steps required to do this are:

1. From Windows, run the Billing File Generator program. If you have not set up a program group or "shortcuts" during installation (see sections 4.4.1 and 4.1.2), select **Program Manager|File|Run** and type **\NCIS\billing** in the dialog box (for Windows 3.1) or select **Start|Run** and type **\NCIS\billing** in the dialog box (for Windows 95).

2. Select **Other|Edit/View Merchant Table** Use the navigation/control bar near the bottom of the dialog box to navigate from record to record and to put the database into add, delete, or edit mode. A hint appears above the buttons in the navigation/control

bar if the mouse pointer is allowed to linger over a button to help explain what each button does.

3. Only 3 fields are required in each merchant record: Site Number, Merchant Number, and Accounting ID. The other fields are used in other modules.

Tips:

After entering the first Site Number, click on the Use fixed site number box. Then it automatically fills in Site Number on each new entry.

Use the Search button to order the database in various way and to navigate quickly to specific merchants.

Generating the Day-by-Day Billing File (rptxxxxx.blg)

1. Use the procedures described in Section 5: "Transaction Log Utilities" to build the transaction log database so that it includes the transactions for the date range required for the billing cycle.

2. From Windows, run the **Billing File Generator** program. For Windows 3.1, this can be done by selecting **Program Manager|File|Run** and typing **\NCIS\billing** in the dialog box. For Windows 95/98/ME, this can be done by selecting **Start|Run|Open** and typing **\NCIS\billing** in the dialog box (or use the program group or "shortcuts" created during software installation -(see "Toolkit Installation" on page 3-2).

3. Build the Daily Summary Table by selecting
Daily Summary Table Ops|Add Entries For Selected Date and adding transactions for the desired dates.

4. Create the day-by-day billing file by selecting **Make|Per Merchant Per Day File** This causes a dialog box to appear. Fill in the dialog entries as follows:

   a. Enter the date range desired for the billing. If the database does not contain information for some of the days in the date range, you are warned. At this point, you can either abort or continue.

      You **MUST** type your site number.

      Leave the **All "Marked" Sites** box unchecked!

      The **Include Days With No Transactions** box can be checked if you want "zero" entries in the billing file for days that the merchant conducted no verifications.

      The **Include Merchants With No Activity** box can be checked if you are maintaining a Merchant Database and you want to include entries in the billing file for merchants that had no transactions on any day in the billing period. This also enables the creation of a list of "inactive merchants".

      The **Generate Missing Merchants List** box can be checked if you are maintaining

a Merchant Database and you want to know about merchants that are conducting transactions that have no entry in the Merchant Table.

b. Choose the desired file format by checking either **Original Format** or **Enhanced Format**. (Note: always choose **Enhanced** if you are planning on using the Transaction Activity Report Writer).

c. Click on **OK** to start the file generation. When this process is complete, the following tips should be useful.

Tips: select **Show Table|Missing Merchants Table** to view the list of "missing merchants". To invoke the Merchant Table Database editor, highlight one of the "missing merchant" entries and type **CTRL-A** (think... **A**dd missing merchant).

Select **Show Table|Inactive Merchants Table** to view the list of "inactive merchants". To delete the merchant, highlight one of the "inactive merchant" entries and type **CTRL-D** (think... **D**elete inactive merchants.

5. The billing file is written to **\NCIS\rptxxxxx.blg** where **xxxxx** is your zero padded site number.

Generating the Period Summary File (rptxxxxx.bgs)

1. Use the procedures described in Chapter 6 to build the transaction log database so that it includes the transactions for the date range required for the billing cycle.

2. From Windows, run the Billing File Generator program. For Windows 3.1, this can be done by selecting **Program Manager|File|Run** and typing **\NCIS\billing** in the dialog box. For Windows 95, this can be done by selecting **Start|Run|Open** and typing **\NCIS\billing** in the dialog box.

3. Build the **Period Summary Table** by selecting **Make|Period Summary Table** and entering the desired date range. If the database does not contain information for some of the days in the date range, you are warned. At this point, you can either abort or continue.

4. Create the period summary billing file by selecting **Make|Per Merchant Per Period File** This causes a dialog box to appear. Use that to select among the following options:

   - You **MUST** type your site number.
   - Leave the **All "Marked" Sites** box unchecked!
   - The **Include Merchants With No Activity** box can be checked if you are maintaining a Merchant Database and you want to include entries in the billing file for merchants that had no transactions on any day in the billing period. This also enables the creation of a list of "inactive merchants".
   - The **Generate Missing Merchants List** box can be checked if you are maintaining a Merchant Database and you want to know about merchants that are conducting transactions that have no entry in the Merchant Table.

- Choose the desired file format by checking either **Original Format** or **Enhanced Format**. (Note: always choose **Enhanced** if you are planning on using the Transaction Activity Report Writer).

5. Click on **OK** to start the file generation. When this process is complete, the following tips should be useful.

   Tips: select **Show Table|Missing Merchants Table** to view the list of "missing merchants". To invoke the Merchant Table Database editor, highlight one of the "missing merchant" entries and type **CTRL-A** (think... **A**dd missing merchant).

   Select **Show Table|Inactive Merchants Table** to view the list of "inactive merchants". To delete the merchant, highlight one of the "inactive merchant" entries and type **CTRL-D** (think... **D**elete inactive merchant).

6. The billing file is written to **\NCIS\rptxxxxx.bgs** where **xxxxx** is your zero padded site number.

Other Tips

- Most menu items that reference Site should be ignored. These items are only useful when data from multiple sites is included in your database (which is normally not possible). (Such menu commands are used by NCN personnel when preparing billing files for sites that are not doing their own.) The only exception to this rule are those menu items that reference Site Totals Table These are useful and show the sum of all verification transactions by all of your merchants.

- Use the menu items **Goto** and **Next** to navigate quickly to desired positions in displayed tables. The exact action of these menu items depends on which table is currently being displayed.

- Don't let the **Daily Summary Table** grow to contain many more days than are actually needed to prepare the billing files. They take up valuable disk space and make the adding of additional days take longer and longer (because of index files that the database routines must maintain). To keep this table in check, use either **DailySummaryTableOps|Remove Entries For Selected Date** menu selection or the **DailySummaryTableOps|Empty The Daily Summary Table** menu selection.

NCN
NATIONAL CHECK NETWORK

Section
7

TRANSACTION Activity Report Writer

In this section...

- Printing a Transaction Activity Report
- Merchant Table Management
- Miscellaneous

7 - Transaction Activity Report Writer

This utility uses the ASCII billing files prepared by the Billing File Generator to print transaction activity reports for merchants. It **requires** that these files have been produced in the "enhanced format" and detects and refuses to process "original format" files. It produces two different reports: the daily activity report and the period summary report, derived from **rpt?????.blg** and **rpt?????.bgs** respectively, where**?????** is your zero-padded site number.

Initial Steps

Start up the **Transaction Activity Report Writer** program by clicking on the **Report Writer** icon or Win95 shortcut.

When the program runs for the first time, it prepares a list of fonts supported by your default printer that can be used by the Report Writer (it can only use non-proportional variable pitch fonts). If that list is empty, you must use a different printer. If the list is non-empty, select a font by clicking on it and then clicking on the OK button. This selection can be changed later by using the **Printer...|SelectFont** menu item. There are three usable fonts that the program looks for and lists for selection: Courier New, Letter Gothic, and Line Printer. Allow its a matter of taste, we believe that Line Printer produces the most attractive reports, followed by Courier New, with Letter Gothic in last place.

Test your printer and font selection by clicking on **Printer...|PrintTestPage** If that produces an acceptable report, the next step is to edit the "header" that is printed at the top of each report. Usually, this is the name, address, etc. of your agency, but the choice is yours. To edit the "header", click on **Header...|Open For Edit** and modify the default until it suits your taste. Save the results by clicking on **Header...|Save** If the editing goes badly awry, you can click on **Header...|Cancel** to cancel the edit. Test the results by printing test pages until you are totally satisfied (click on **Printer...|PrintTestPage** to do this).

Printing a Transaction Activity Report

Click on **BillingFileOps...|Select Billing File** to bring up the open file dialog box. Chose the file type using the drop down list box at the bottom left, then select the desired file and click on then **OK** button.

If a billing file was opened, various print options appear under the **BillFileOps...** menu.

1. Select **Print All Merchants** to print a report for all entries in the billing file.

2. Select **Print Merchant Set** to print reports only for merchants that have an entry in the Merchant Table with a matching Set Number.

3. Select **Print Next Merchant** to print all merchants, one at a time. This is a test mode not meant to be used for "production" printing.

Merchant Table Management

Click on **MerchantTable** to bring up the **Merchant Information View/Edit** dialog box. “Merchant Table Maintenance” on page 8-5 for additional help in utilizing this feature.

Miscellaneous

Under the **Options...** menu there are two selections.

1. **Print Zero Amounts** controls the treatment of zeroes in the detail lines of the transaction activity reports. If this is checked, then zeroes are printed. If it is not checked, then such entries are left blank.

2. **Show Diagnostics**, when checked, causes the display of all printer fonts and the selected printer fonts after **Printer...|SetupPrinter** has been executed. It is not likely that this option is ever needed. Its there only to show why a given printer has no suitable font for use.

   Although it is unlikely that it is ever needed, it is possible to view and edit the ASCII billing files. Click on **BillingFileOps...|Edit Billing File** to bring up an edit menu. Return to this menu list to save or rename or cancel the edit session.

NCN
NATIONAL CHECK NETWORK

Section
8

Compliance Report Generator

In this section...

- Building the Compliance Report Database
- Merchant Table Maintenance
- Report Templates
- Printing Reports
- Miscellaneous

8 - Compliance Report Generator

This utility utilizes data extracted from incremental negfiles and transaction log files covering the appropriate date range to generate a "compliance report" database that contains an entry for each returned check and shows what the verification response (or possibly the lack thereof) was at the time of check presentation. From this database, a number of different reports can be printed.

First Steps Following Software Installation

Upon first use of this utility, you should set up a template as “Report Templates” on page 8-6. These templates initialize the header information that is printed in the upper left corner of reports. Normally, this is the name and address of your agency. To do this, select ReportTemplates and create a new one. When you have filled in the appropriate information, click on the “X” in the upper right hand corner of the screen to exit. The information gets saved automatically.

Next, click on **Print|Select Printer Font** and choose a printer font. You probably have several to choose from. If present, we recommend that you choose **Courier New.** The other likely fonts are **Letter Gothic** and **Line Printer.** The program interrogates your printer driver and asks for a list of all fixed pitch fonts. Only fixed pitch fonts are used because of the need to have columns line up on the reports. This font selection only need be done once.

Finally, to test your header, the font selection, and your printer connection, click on **Print|Print Test Page.** This should produce a sample one page compliance report.

Building the Compliance Report Database

The compliance report database is built by scanning incremental negfiles, finding the "returned item" records there, and performing a search of the transaction log database to find the verification transaction that most closely matches the "returned item" information. It is from this database that all reports are printed.

NOTE

The contents of the compliance report database can be viewed on-screen by clicking on **Options|Show Compliance Table**). Before examining the operational steps required to build this database, it is useful to understand the search strategies employed and the "partial match" feature that gives the compliance reports unexpected power.

Search Strategies

The "returned item" record provides the following information that can be matched against corresponding data fields in the verification records:

1. MICR number (Bank Routing Number + Account Number) when doing a MICR lookup

2. Date of check

3. Merchant number

4. Site number

5. Amount of check

6. Check sequence number (the check number)

7. ID when doing an ID lookup

In attempting to find a matching verification transaction in the transaction log database, the MICR number is used first as a search "key". All transactions involving that MICR number are examined and "scored" as to the number of data fields that match. The score must be equal to or greater than a specified minimum score (more on this in the next section). If multiple verification transactions are found to "match", the one with the highest score is taken.

If no verifications records were found in the MICR number search, and an ID was included in the “returned item” record, then a new search is conducted using the ID as a search “key”. This finds verification transactions that were done using only an ID. Transactions found this way are “scored” in the same manner as described in the previous paragraph.

Finally, if the above search has failed to find a satisfactory match, a search is made for all verification transactions that a particular Site/Merchant has conducted. Once again, transactions found this way are "scored" as previously described.

If all of the above searches fail to find a satisfactory match to a verification transaction, then the compliance report database entry shows “no matching verification found”.

Partial Matching

In searching for the verification transaction that corresponds to a particular "returned item" record, requiring an exact match to all data fields in the two records is too strict and hides useful information. Errors are common and it is useful to know that errors are occurring and what kind they are. The Compliance Report Generator therefore permits unmatched data fields under conditions that can specified by the user. For each type of search described in section 9.2.1, it is possible to specify which data fields to test for matches and the minimum match score that is to be considered acceptable. To specify

these conditions, click on **Options|Select Match Items** and then either **MICR Lookup** or **ID Lookup** or **Site/Merchant Lookup**. This brings up a panel with "check boxes" for the various data fields, and a "spinner" that allows the minimum match score to be set. Changes made here are retained from session to session.

When doing a MICR Lookup, the matched information includes the MICR number by default. Similarly, for an ID Lookup, the matched information includes the ID but not the MICR number. When doing a Site/Merchant Lookup, neither the MICR nor the ID gets included in the matched fields.

This "partial match" capability has much more power than might appear at first glance. We have found it useful in the following areas:

- It discloses keyboarding errors by clerks during manual entry of MICR number or IDs.
- It discloses assignment of “returned items” to the wrong merchant. This one is so valuable that a special report of mismatched merchant numbers has been provided.
- It discloses terminals in the field that have been programmed with the wrong merchant number.

We make the following recommendations regarding the "match" settings:

- Set the Minimum Match Count to two less than the number of “Match” items for MICR lookup and for ID lookup. Typically most users select everything in the list except the site number and set the number of match items at “2”. For Site\Merchant lookup, set the Minimum Match Count at one less than the number of “Match” items. Most users select everything in this list and set the number of match items equal to 4.
- Uncheck the “Match Check Amount” box if none of your POS transactions input a check amount. If some of your merchants use POS transactions that include a check amount while others do not, you should leave the “Match Check Amount” box “checked”. The “match scorer” detects the lack of a POS check amount and scores that as a match to any amount in the “returned item” record.
- Set the Minimum Match Count to zero to completely disable a particular "search" (this is a time saving device that should be used to disable the ID search if none of your POS verification transactions are conducted using ID only).

Operational Steps in Building the Compliance Report Database

The following steps must be taken to build up a compliance report database:

1. Save your incremental negfiles. These need to be uniquely named (so that they don't write over each other and so that you can tell what they contain). We suggest that you create a subdirectory called **negfiles** and save them there.

2. Use the Transaction Log Database Manager to build a verification transaction database that contains data covering the likely date of presentation of the "returned items". 60 days should be sufficient.

CAUTION

"Returned items" that have check dates that are not included in the current transaction log database is discarded!

3. Decide whether you want an entry in the compliance report database for every returned item from every merchant found in the negfiles or whether you want to restrict entries to merchants that have been entered in the **Merchant Table** database (recommended). If you want to restrict entries to selected merchants only, there are two things you must do: 1) make entries in the **Merchant Table** for each merchant you want to include in the compliance report database (see "Building the Compliance Report Database" on page 8-1 for additional help with this procedure) and 2) click on **Options|Constrain Report...** (if it is not already "checked") then click on **Options|Select Merchant Set Constraint** and choose the set number for the merchants to be included (note: if you select 0, then all merchants found in the **Merchant Table** are included regardless of their set number. This is the recommended setting).

4. Create a Report Template, if one doesn't exist, as explained in "Report Templates" on page 8-6. This controls which sites get included in the report and it establishes one or more lines of header information that appear at the top of each report.

5. Process each incremental file by clicking on **Process Negfile**. This causes a file selection panel to appear. Use this to select one or more files for processing. The procedure for selecting multiple files is: click on the first file desired; scroll to the last file desired, press the **SHIFT** key and then click on that file; to select (or deselect) a collection of files that are not consecutive in the file list, press **CTRL** and then click on the file.

6. Once the desired files have been selected, select the appropriate Report Template to use in preparing the report.

NOTE

If OPTIONS|Diagnostic Mode is selected, the program pauses on every record in the negative that is not type "10". This is usually highly annoying and unnecessary.

7. After selecting the negative file or files, and selecting the Report Template, click on **OK** to start the processing. Note that as these negfiles are processed, certain errors can

be detected. These errors are recorded and can be viewed later. “The ErrorLog” on page 8-8 describes this activity in more detail

CAUTION

This utility does not protect against the processing of a negfile multiple times. If this is done accidentally, the compliance database is then have duplicate entries. It is important to ensure that each incremental negfile is processed once and once only.

8. It is also up to you to decide which negfiles are processed in order to produce a report. We recommend that you consider producing a monthly report by processing all negfiles created during that month against all verifications performed in the last 2 months. Other strategies are possible, but this is a good place to start.

Merchant Table Maintenance

In order to print reports for your merchants that contains their company name and address as well as to control which merchants have reports printed, and possibly to control which merchants have entries in the compliance report table, a database called the **Merchant Table** has been included. It is not essential that this database be built and maintained, but it is highly desirable as some features of the report printing process depend on data that is held here. Without this database, those features would be inoperative.

To add a merchant to the Merchant Table, click on **MerchantTable.** This brings up a window that can be used to examine, change, find, and create entries in the database. Do not be alarmed if the data entry panel seems overwhelming. This database is used by other utilities, so there are fields shown that do not have to be filled in for use by the Compliance Report Generator. More specifically, the only fields that **must** be filled in are in the top portion of the panel.

The nine button VCR-like array at the bottom of the panel is used for navigating (the leftmost 4 buttons are used for this) and editing entries (the rightmost 5 buttons are used for this). These buttons are somewhat cryptically marked, but a useful “hint/reminder” pops up if you pause the cursor over a button for a second.

To add a new entry to the database, click on the button that has the + icon on it (Insert Record). Use the mouse or tab key to move to fields that you want to fill in and enter the desired information. When done, click on the button that has the “check mark” icon (Post Edit). If a required field has not been set, you cannot “Post” (write) the record. It highlights the missing field for you.

If you begin editing a record and don't want to make the changes, click on the button with the **X** icon (Cancel Edit).

If, in adding a new record, you get a "Key Violation Error", it means that an entry for that merchant already exists. Press the button with the **X** icon (Cancel Edit), then navigate to the existing record and press the Edit button to allow changes to be made to the record.

If you are managing a single “Site”, after you have made the first entry of a record, click on the “Use fixed site number” check box. This speeds up subsequent data entry by automatically filling in the Site Number field for you.

If you are trying to find a specific entry in the database and clicking the navigation buttons is ineffective, click on **Search** instead. This pops up a dialog box that enables you to specify search criteria for finding the desired entry.

Report Templates

Report templates contain two important pieces of information:

1. A list of site numbers to include in a report.

2. Header information to appear at the top of each report.

The system can have multiple templates with different data. Most users, however, have only a single template that they use for every report. Agencies serving multiple retail chains, each with a unique site number, can use the templates to control the data used in preparing reports for the different chains. Every user should define at least one template.

To define a new template or edit an existing one, click on **Report Templates** at the top of the main screen for the Compliance Report Generator. This results in a new screen that contains four boxes of information. The "**Report Templates...**" box shows a list of defined templates. Data for the highlighted template appear in the "**Site Numbers to Include in Report**" box and the "**Header to print on Report**" box. These data can be edited whenever they are displayed.

To create a new template, follow these steps:

1. Enter the name of the new template in the "**Name and create new report templates here**" box. Leaving this box causes the new name to appear in the list of Report Templates and the data in the other two boxes get erased.

2. Enter one or more site numbers in the "**Site Numbers to Include in Report**" box. The template cannot be used without at least one number in this box.

3. Enter header information in the "**Header to print on Report**" box. This accommodates multiple lines that appear at the top of each report prepared using the template.

4. Exit by clicking on the "X" in the upper right corner of the screen. The new data get saved automatically.

NOTE

It is important to enter the name first. If, for example, there are no defined templates, and data get entered for the site number list and the header, and then try to enter the name of the template, the system does not allow completion of the name. Forcing the cursor to move to another box erases the data in all boxes, forcing re-entry of the data.

Printing Reports

Reports are grouped in two categories:

- **detail reports.** Are prepared on a merchant-by-merchant basis and intended for distribution to your merchants
- **summary reports.** Show overall merchant activity and are intended for use by your agency.

Detail Reports

To print compliance reports for your merchants, click on **Print|Print Detail Report**. This pops up a menu that enables you to specify which merchants to print reports for. The choices are:

- **...for all Merchants.** Choosing this menu item causes a report to be printed for every merchant that has an entry in the Compliance Report database. Address information in the Merchant Table is utilized if it is available. This prints everything and is usually more than desired. More typically, one of the more selective printing options would be used as described below.
- **...for Merchant Set.** Choosing this menu item restricts reports to those merchants that have an entry in the Merchant Table database **and** that have a specific "set number" assigned. A box pops up to allow the "set number" to be specified. The "merchant set" concept allows you to predetermine which merchants have compliance reports generated. This takes care of the very common situation in which only some of your merchants need or subscribe to this service.
- **...for specific Merchant.** Choosing this menu item lets you generate one report for one explicitly specified merchant. It requires no entry in the Merchant Table database but uses address information found there if present. A box pops up to allow the merchant number to be specified.

Summary Reports

To print reports to be used by your agency, click on **Print|Print Summary Report**. This pops up a menu that enables you to select the particular report wanted. The choices are:

- **...for Merchants With No Verifications.** Choosing this menu item prints a report summarizing the compliance statistics for all merchants with entries in the compliance report database but no entries at all in the verification transaction log database. This lets you learn about merchants that are not using your verification service.
- **...for Merchants With Verifications.** Choosing this menu item prints a report summarizing the compliance statistics for all merchants with entries in the compliance report database and that had at least one of their "returned items" verified.
- **...for All Merchants.** Choosing this menu item prints a report summarizing the compliance statistics for all merchants with entries in the compliance report database regardless of whether they are using your verification service or not.

- **Merchant Number Mismatch List.** Choosing this menu item prints a list of all merchants in the compliance report database that had one or more verifications matched to them but the merchant number in the verification transaction did not match the merchant number in the "returned item" record. This could be because the "returned item" was assigned to the wrong merchant or that the verification terminal at the merchant site contains the wrong merchant number.

The ErrorLog

Incremental negfiles are produced by the software package that is used by an agency for monitoring and controlling the collection/recovery activity. It is frequently the case that data entry errors are made and subsequently show up in the incremental negfiles. While the Compliance Report Generator is processing these files, it is also testing for data errors in the "returned item" records. It is able to test for and log for subsequent viewing the following errors:

- Transit Number error.
- Account Number error.
- Date format error.
- Merchant Number error.
- Check Amount error.
- Check Sequence Number error.
- ID Type error.
- Check Date too old.
- Merchant not in **Merchant Table**.
- Merchant not doing verifications.

It is likely that you will not want to see all possible errors. To select which errors are to be detected and logged, click on **Options|Select Errors To Be Logged**. This pops up a panel with "check" boxes that permit you to turn on and off the various error detections. We recommend that items 1 through 7 be left "checked". Item 8 (Check Date too old) occurs when a "returned item" is found that is older than the oldest date contained in the transaction log database. It is not uncommon for agencies to process "old" checks, so this box probably need not be "checked". Items 9 and 10, if "checked", typically generate an excessive number of errors and so should be used sparingly.

To view the error log file that results from processing a negfile (or a group of negfiles), click on **ErrorLog**. This pops up a dual view panel. The top panel shows a line for each negfile processed followed by lines detailing the type and location of the errors found. The bottom panel shows a view of a negfile. To navigate quickly to a detected error, click on the file name line in the upper panel. This opens that file for viewing in the bottom panel. Then, click on an error line and the bottom panel re-position to that line in the negfile and highlight the line containing the error.

Miscellaneous

The following describes the miscellaneous options when using the Compliance Report Generator with the NCN toolkit.

Erasing the Compliance Database

After each report cycle has been completed and all desired reports have been printed, the compliance database can be deleted in preparation for the next set of reports by clicking on **Options|Erase Compliance Table**. A confirmation window pops up to help prevent inadvertent erasures.

Diagnostic Mode Option

Under the **Options** menu there is an item called **Diagnostic Mode On/Off**. This is used by the program developers to examine step-by-step operation of the program. It won't hurt anything to activate this feature, but it wastes a lot of time. We recommend that you do not use this feature.

Changing Compliance Table Appearance

You may want to rearrange the order of columns displayed when viewing the compliance table. This can be accomplished by a click-and-drag of the column headings.

You can also resize a column by performing a click-and-drag operation at the boundary of two column headings.

Note that any of the above changes persist for the duration of a session but are lost when the program is terminated.

Sample Reports

Examples of each type of report available are included in the next few pages, along with some descriptive material to aid in their interpretation.

The text in the upper left corner is controlled by the header file. This can be changed by clicking on **Header|Open for Edit** and making appropriate changes. changes can then be saved by clicking on **Header|Save**.

The next text block is controlled by the **Merchant Table** database. Any merchant information, including address information, placed there is printed in this block.

The data portion of the report is composed of line pairs. The top line shows the “returned item” information extracted from the incremental negfiles. The bottom line shows the matching verification transaction. Any items from the verification transaction that do not match the corresponding “returned item” field are printed in bold to highlight the discrepancies.

The field labeled “Reference” for the “returned item” line is the reference number assigned by the recovery software to that check. Some recovery software packages do not include this reference number when they produce incremental negfiles; in such cases the field is blank. On the verification line, the reference field is composed of the verification number and the time of the verification.

The field labeled “File Date” is only filled in for the “returned item” line. It gives the date of preparation of the file that contained the returned check. This can be compared to the next field, that gives the date of the check, to get some idea of the delay involved in adding a returned item to the verification database.

The field labeled “Chk Date” for the “returned item” line gives the date of the check as recorded by the data entry clerk. This field on the verification gives the date of the verification transaction.

The field labeled “Chk account/Verified account” gives the MICR number of the returned check on the “returned item” line. The MICR number is the concatenation of the bank Routing number and the Account number.

The fields labeled “Check #”, “amount”, “Merch#”, and “Site” are self-explanatory and identical for the two lines.

The field labeled “Verif Ans” is only filled in for the verification line. It displays in coded form the verification response that was returned to the point-of-sale. It has two sections encoded as follows:

1. The first section contains one of the following three values: Auth, Warn, or Decl. The corresponding meanings are: Authorization given, Warning message given, and Decline Check message given.

2. The second section gives a two character code. The first letter is P, N, T, or I, and can be in lower case. If it is lower case, it indicates that account or ID information was manually keyed. If it is upper case, then the information came from a check reader or a magnetically encoded card. The meaning of the letter codes is as follows: P=payroll check verification; N=normal personal check verification; T=two party check; I=ID verification. The second letter tells whether the verification is a first time verification, a repeat verification, a duplicate check (only applies to payroll checks), or untestable (because no check number was available). The letter codes are: F=first verification; R=repeat verification; D=duplicate check (repeat presentation of a payroll check more than 15 minutes after the first presentation); U=untestable.

Agency Reports

The following three reports are summary reports intended for agency use. They are self-explanatory except possibly for the somewhat cryptic column headings. The heading have the following meanings:

Heading	Meaning
Site	Site number
Merch#	Merchant number

Heading	Meaning
#Ret	total number of “returned items”
#Unv	number of “returned items” that were not verified
#Wrn	number of “returned items” that were given Warning POS messages
#Dec	number of “returned items” that were given Decline POS messages
#Ath	number of “returned items” that were Authorized at POS.
$Returned	total dollar amount of “returned items”
$Unverif	dollar amount of unverified “returned items”
$Warned	dollar amount of “returned items” that received Warning messages
$Decline	dollar amount of “returned items” that received Decline messages
$Authed	dollar amount of “returned items” that were Authorized at POS

Sample Report 2. Summary of all merchants serviced by agency.

Sample Report 3. Summary of merchants using verification serviced by agency.

Sample Report 4. Summary of merchants not using verification

Mismatched Merchant Number Report The mismatched merchant number report shows all “returned items” that were assigned to a particular merchant number that matched up with a verification transaction that had a different merchant number. This can occur for two principal reasons:

1. The “returned item” was inadvertently assigned to the wrong merchant. This causes the wrong merchant to receive payment for the check when it is paid.

2. The merchant number has been improperly entered in the terminal at that merchant location. This could cause the wrong merchant to get charged for the verification or even check guarantee.

Either of these situations is sufficiently serious to warrant a special report.

The format of this report is identical to the merchant compliance report (Sample Report 1). Refer to that description for further details. The report is shown below.

Sample Report 5. Mismatched Merchant Number.

NCN
NATIONAL CHECK NETWORK

Section
9

CheckManager 3000 Terminals

In this section...

9 - CheckManager 3000 Terminals

The IVI CheckMate eN Check 3000 allows a SINGLE TERMINAL/CHECK READER DEVICE to offer a high degree of check verification software flexibility. This means you can offer your merchant base one terminal system that is capable of performing a check verification transaction in virtually any desired manner.

NCN has developed a program that offers:

1. Four (4) different transaction types, plus several options within a specific transaction.

2. A special **Configuration Mode** to select which transaction types operate in a specific installation.

3. The unique NCN Configuration Mode also allows numerous other options: Skipping check amount; Choosing the ID type whenever the transaction requests one; and enabling or disabling of printing the warning and decline messages.

4. Password protection for the Configuration Mode, different from that of the Set Up mode

5. **Setup mode** that allows changing of the phone number for verification, the merchant ID, and the default state for driver's licenses. This mode is also password protected, but differently from the Configuration Mode.

This document explains the various options available with the NCN program on this terminal, and describes how to set them up and then use the terminal.

Downloading Programs (Using Unit Config Mode)

The CM 3000 can download a program using a telephone connection in the same manner used for VeriFone terminals. It also has a couple of maintenance settings that may need occasional adjustment. To access the download/maintenance mode, use the following steps:

Press the Clear key and hold it down for 5 to 10 seconds until the terminal displays the Message " UNIT CONFIG MODE" and then proceed to the next section.

If the "UNIT CONFIG MODE" does NOT appear - follow these steps:

1. Remove power from the unit.

2. Place a check in the unit and slide it as far forward while the power remains off.

3. Apply power to the unit.

4. Wait for the unit to start up. It eventually displays the message, “REMOVE CHECK”.

5. Without removing the check, press the CLEAR key. The motor starts up and usually feeds the check through the reader. If the motor starts but does not feed the check, manually remove the check. In either case, the display changes to “CHECKMANAGER”.

   At this point, the unit is in the UNIT CONFIG mode. To select a specific function, first press ENTER and then the FUNC key and one of the following digits you choose to edit. The specific functions available include:

   1-Telephone download. See further details below.

   2- Set time and date.

   3- Direct download. Used only at the factory to load a program.

   4- Not used.

   5- Contrast. Use the “#” key to increase the contrast and the “*” key to decrease the contrast. Normally, the best contrast is between 50 and 60.

   6- Backlight. Use the “#” key to increase the brightness and the “*” key to decrease the brightness. Normally, the best backlight levels are between 50 and 70.

   7-Not used.

   8-Not used.

   9-Not used.

Perform a Program Download from The NCN Terminal Program System

Performing a telephone download (FUNC - 1) results in further prompts as outlined below:

1. Once the unit is in “UNIT CONFIG MODE” Select the Enter Key in which the display reflects FUNC

2. Press the 1 key (FUNC-1)

3. **PASSWORD?** Key in “246135” as the password followed by ENTER

4. **Dwnld Phone Num?** Enter the phone number of the download computer followed by ENTER.

5. **Serial Num?** Enter the serial number, sometimes called the “download ID”, followed by ENTER.

6. **Application ID?** Enter the name of the application to be loaded, using the ALPHA key as required to create letters, followed by ENTER.

Once all the necessary information has been entered, the download proceeds automatically, with the display showing the progress. When complete, the terminal displays "DOWNLOAD COMPLETE". Remove and reapply power to resume normal operation. Use the Setup mode and the Configuration mode to set up the terminal as desired.

Setup Mode

The Setup Mode allows you to key in commonly changed parameters such as the verification phone number and the merchant ID for verification once a verification program is downloaded. It also allows you to view the most recent transmit buffer and receive buffer as an aid to troubleshooting.

To enter Setup mode:

1. To enter the Setup Mode, press the **ENTER** key in the startup menu.

   The terminal briefly displays the phrase "Setup Mode" and then shows the current phone number.

2. Press **ENTER** again to move to the next parameter, the merchant ID. To move back to a previous parameter, press **ALPHA**.

3. Continue to press **ENTER** to step through all of the available parameters and data. At the end, the terminal reverts to the standard Startup Menu.

NOTE
The Default Password for the Set-Up Mode is: IVINEW
(Numerical equivalents only! - Or "484639")

To change setup mode parameters:

1. While the parameter is displayed, press the **Backspace** key.

NOTE
It is not possible to edit the transmit or receive buffers.

   The terminal then prompts for a password.

2. Key in the Setup Mode password.

   While entering this password, the display shows an asterisk for each entered character. If the password is invalid, the terminal displays the Startup Menu.

   After successful entry of the Startup Mode password, the terminal displays a prompt for the parameter you want to change.

3. Key in the new value, followed by **ENTER**.

The terminal tests the new data for reasonableness (e.g. a phone number must have at least 7 digits), and set the parameter to the new value if it passes the test. If it fails the test, or if the user just presses the **ENTER** key, the terminal leaves the current value unchanged, and moves to the next parameter in the Setup Mode.

At any point in the Setup Mode, if you press **BACKSPACE**, the display moves backward to the previously displayed item.

NOTE
Once you have entered the Setup Mode password for one parameter, the terminal does not prompt for it again until you start a new transaction or press the **CLEAR** key.

Setup Mode Data Fields

- Phone number for verification
- Merchant ID for verification
- Default state for driver's license entry
- Transmit buffer
- Receive buffer

NOTE
The terminal must have defined data for the phone number, merchant ID, and default DL state before it runs a transaction. ALL three parameters must have data. This applies to the default DL state, even if you do not plan to use a driver's license ID.

After viewing and possibly changing the phone number, merchant ID, and default DL state, the terminal displays the transmit buffer and then the receive buffer. The transmit and receive buffers normally are used only when investigating problems.

These are read-only buffers. The buffer display uses manual scrolling with the pound key, "#", scrolling to the right and the asterisk, "*", scrolling to the left. The terminal beeps if you attempt to scroll past either end of these buffers. After pressing **ENTER** when displaying the default DL state, the display shows:

Transmit Buffr->

Press the "#" key to see the contents of this buffer, with each key press displaying the next 16 characters of the buffer. Pressing "*" moves back to the left in 16 character steps.

When finished viewing the transmit buffer, press the **ENTER** key and the display shows:

Receive Buffer->

Use the "#" or "*" keys to view this buffer in exactly the same way as the transmit buffer. When finished, press the **ENTER** key one last time and the terminal returns to its normal operation.

Configuration Mode

The Configuration Mode requires a different password than the Setup Mode and a more complicated sequence of keystrokes to enter. This process is to "Fine Tune" the setup and configuration of the terminal program that was downloaded from the NCN Terminal Download System. Just as in the case of setup mode, start at the initial menu and perform these steps:

1. Press **ENTER**.

   The terminal displays "Setup Mode"

2. As soon as the "Setup Mode" appears, press **ALPHA**. This must be done before the first parameter appears in setup mode, a period of about one second.

   The terminal prompts for a password.

3. Key in the **configuration mode** password followed by **ENTER**.

NOTE
The Default Password for the Configuration Mode is: RMRSCFG

Numerical equivalents only! - Or "7677234"

NOTE
The configuration mode has a sequence of options, using a set of scrolling menus.

4. Select the desired option by pressing the key designated in the menu.

   The available options choices include:

   - Transaction type (four choices)
     Enable/disable check amount
   - Enable/disable sale amount
     ID type (three choices)
   - Enable/disable printing of warnings and declines
   - Default agency name and phone number printed on receipts (if printing enabled)
   - Scroll dwell time, in 100 msec intervals

For the ***Transaction type*** above, one of the three possible transaction types must be enabled. If you attempt to disable all three, the terminal displays an error message briefly and then returns to the beginning of transaction type selection. If this happens, the previously enabled transaction types still remain in effect.

Since configuration mode prompts for a password upon entry to the mode, it never prompts for it again until an exit from the mode occurs. Press **ENTER** to change to the next configuration option without altering the one currently displayed. Similarly, to move back to a previous option, press **ALPHA**. Making a selection for the final option (printer enable/disable), or pressing **ENTER** at this option, or pressing **CLEAR** at any point returns the terminal to the startup menu. The configuration options take effect immediately, as soon as you exit configuration mode.

For the ***Default agency name and phone number printed on receipts*** above, if the printing of warnings and declines is enabled, the terminal displays the prompt, "Print Name (V+)", concatenated with any previously entered name. THIS NAME SHOULD ONLY BE USED WITH Velocity PLUS® SYSTEMS. To enter a name or change an existing name, press the **BKSPC** key. The terminal responds with a prompt, "Enter new name". Key in the name (16 characters maximum) followed by **ENTER**. To eliminate a default name, press the **ENTER** key without keying any data when the "Enter new name" prompt appears.

After entry of the default name for use with Velocity PLUS® systems, the terminal displays the prompt, "Print Phone (V+)", concatenated with any previously entered phone number. To enter a phone number or change an existing phone number, press the **BKSPC** key. The terminal responds with a prompt, "Enter new phone". Key in the phone number (16 characters maximum) followed by **ENTER**. To eliminate a phone number, press the **ENTER** key without keying any data when the "Enter new phone" prompt appears.

After entry of the default name and phone number, if used, or selection of print/no print option, the terminal displays the current scroll dwell time as a count of 100 msec intervals. Thus a time display of "Scroll Time= 8" results in a dwell time of 800 msec. (This is the default time.) To change this time, press the **BKSPC** key. The terminal responds with a prompt, "Enter New Time". Key in the desired new time, followed by **ENTER**. Note that this time cannot be less than 3 (300 msec) nor greater than 20 (2 sec).

The scroll time configuration option also permits input of negative numbers. Entering a negative number eliminates the Idle Prompt from the initial scrolling menu. The scroll time takes the absolute value of the input data and uses it in the same manner as described above. Therefore, negative input data must be in the range of -3 to -20.

Equivalence To Other NCN Programs

The IVI CM 3000 terminal running this NCN program can be set-up to behave like most of the existing NCN programs for the TRANZ 330 terminal. The following list explains how to set up the terminal to run like several of the commonly used programs on the TRANZ 330. (Refer to Appendix A of either the Velocity PLUS® or the NCIS™ manual for an explanation of these programs.) Unless otherwise noted, the sale amount option should always be disabled.

The following list shows that the single program for the CM 3000 can appear like any of several programs for the TRANZ 330 without downloading anything additional. Simply change the configuration to achieve the desired transaction. While these configurations prompt for the same information as the corresponding TRANZ 330 programs, they have considerably increased ease of use due to several of the automatic features in the CM 3000 program.

- **MFxPNTR.** Enable all three transaction types, check amount, and the printer.
- **SPxPYRL.** Enable all three transaction types and check amount. Disable the printer.
- **SK33x.** Enable only the first transaction type (personal check without ID) and check amount. Disable the other transaction types and the printer.
- **SKS33x**. Enable only the first transaction type, check amount and sale amount. Disable the printer.
- **FK33x** Enable only the first transaction type. Disable the check amount and the printer.
- **SPMDLx.** Enable only the second transaction type (personal check with ID) and check amount. Disable the other transaction types and the printer.
- **33IDDx.** Enable only the fourth transaction type (ID-based verification) and select driver's license as the ID.
- **33IDSx.** Enable only the fourth transaction type (ID-based verification) and select Social Security as the ID.
- **33IDCx.** Enable only the fourth transaction type (ID-based verification) and select Courtesy Card as the ID.

Terminal Error Messages

The eN Check 3000 has several different error messages that can appear. Some of them are **run time errors** that relate to problems occurring as a program encounters an unusual state. The terminal also has a set of **syntax errors** that indicate a problem with the syntax of the program (these should rarely appear since programs get thoroughly debugged before making them available for download.

The following run time errors can appear (listed in order of increasing severity):

Table 9-1. Run Time Errors

Error Number on Terminal	Interpretation
1	ERR_NUMBER_TOO_BIG
2	ERR_DIVIDE_BY_ZERO
3	ERR_MOD_BY_ZERO
4	ERR_EXTRA_CHARS_IN_NUMBER
5	ERR_STRING_OVERFLOW
6	ERR_EMPTY_ORD_ARGUMENT
7	ERR_PROGRAM_NOT_FOUND
8	ERR_LINE_NOT_FOUND

Table 9-1. Run Time Errors

Error Number on Terminal	Interpretation
9	ERR_OUT_OF_DATA
10	ERR_BAD_FILE_WRITE
11	ERR_BAD_SEEK
12	ERR_BAD_REMOVE
32	ERR_FOR_WITHOUT_NEXT
33	ERR_NEXT_WITHOUT_FOR
34	ERR_GOSUB_TOO_DEEP
35	ERR_RETURN_WITHOUT_GOSUB
36	ERR_INDEX_OUT_OF_BOUNDS
37	ERR_ARRAY_WRONG_DIMENSION
38	ERR_DIMENSION_TOO_LARGE
39	ERR_FILE_NOT_OPENED
40	ERR_FILE_NOT_OPEN
41	ERR_BAD_FILE_NUMBER
42	ERR_BAD_LINE_NUMBER
64	ERR_OUT_OF_MEMORY
65	ERR_BAD_VERSION
66	ERR_PROGRAM_CORRUPT

The following table gives the same information for syntax errors (listed in order of increasing severity).

Table 9-2. Syntax Errors

Error Number on Terminal	Interpretation
128	ERR_CONSTANT_OVERFLOW
129	ERR_EXTRA_CHARS
130	ERR_LINE_NUM_TOO_BIG
131	ERR_MISSING_LINE_NUM
132	ERR_MISSING_ASSIGNMENT
133	ERR_MISSING_COLON

Table 9-2. Syntax Errors (Cont.)

134	ERR_MISSING_GOTO
135	ERR_MISSING_THEN
136	ERR_MISSING_TO
137	ERR_MISSING_QUOTE
138	ERR_MISSING_PAREN
139	ERR_WRONG_ARG_TYPE
140	ERR_WRONG_EXP_TYPE
141	ERR_NOT_STRING_VAR
142	ERR_NOT_NUMERIC_VAR
143	ERR_EXP_TOO_COMPLEX
144	ERR_BAD_FOR_VAR
145	ERR_BAD_VARIABLE
146	ERR_BAD_OPERAND
147	ERR_BAD_SUBSCRIPT
148	ERR_BAD_STATEMENT
149	ERR_UNEXPECTED_EOS
150	ERR_SYNTAX_ERROR
151	ERR_STATEMENT_TOO_LONG
192	ERR_NO_OPEN_PROGRAM
193	ERR_PROGRAM_TOO_BIG
194	ERR_BAD_PROGRAM_FILE

Terminal Features

The specific features included in the NCN program include:

- **Multiple Transaction Types.** Four basic transaction types have been implemented:
  - Personal check - Without ID
  - Personal check - With an ID
  - Payroll check - Which always requires an ID.

- ID-based check verification

NOTE

The first three transaction types are identical with those offered in current NCN programs SPxPYRL or MFxPNTR for the TRANZ 330 terminal.

- **Selective Enabling Of Transaction Types.** Rather than requiring loading of an alternate program, a SINGLE NCN program for the CheckManager 3000 allows selective enabling or disabling of ANY of the three transaction types listed above. This saves the time and costs associated with required loading of an alternate program. Thus, for example, if a merchant never accepts payroll checks, that transaction type can be disabled so that it never appears in the startup menu as an option. This simplifies clerk training and reduces confusion.

- **Auto-scrolling Of Menus.** Whenever the user has choices to make, the various alternatives appear in sequence on the 16 character display of the CM 3000. As an example, the initial startup of the terminal displays the **Idle Prompt** (as set in the Velocity PLUS® or NCIS ™) followed by a prompt for each of the enabled transaction types. These scroll from one option to the next at a set interval, and then keep repeating until the clerk makes a selection. The configuration mode allows adjustment of the dwell time for each scroll message, plus elimination of the Idle Prompt if desired.

- **Automatic Transaction Start With Check Insertion.** When the terminal is scrolling the initial menu, the clerk can start the transaction by pressing the appropriate key. Or, the clerk can simply insert the check into the CM3000. The terminal reads the check and starts the transaction, automatically choosing the first transaction type that appears in the scrolling menu. Again, this saves training time, reduces the number of keystrokes required by the clerk, and simplifies terminal operation.

- **Menu SimplificatioN.** If a specific merchant only conducts one type of transaction, the startup sequence simply displays the Idle Prompt and an “Insert Check” message in alternation. This simplifies terminal operation.

- **Multiple Id Types.** The configuration mode allows selection of one of three available ID types: * Driver’s license; * Social Security number; *Courtesy card. Once configured, the terminal always asks for the specified ID whenever the transaction type requires ID.

- **Option to Omit Check Amount.** Some merchants want the simplest possible transaction, only using the MICR information. This accelerates the process at the point of sale and simplifies clerk training. The configuration mode provides an option to skip the prompt for check amount and substitute “0.00” as the amount for all checks. The merchant can still enjoy the protection of velocity limits on numbers of checks with this option, even though he cannot set limits on dollar amounts.

- **Option to Omit Sale Amount.** Sale amount, as distinct from check amount, must be present only if the merchant allows for checks written in excess of the purchase amount, and he wishes to have limits on the amount of cash back. Since few merchants outside of the grocery business extend this privilege, the CM 3000 makes this optional.

- **ID-Based Check Verification.** Some merchants need the CM 3000 to run a check verification using only an ID such as a driver's license. For example, a pizza delivery merchant may want to run an ID transaction when an order is phoned in, and then later verify the check itself when the delivery person returns with it

- **MICR Validity Checking and Easy Re-scan.** The CM3000 program tests the MICR results after each reading of a check and detects some of the obvious problems. If it detects an error, it displays a suitable message momentarily and then prompts the clerk to re-scan. The clerk can simply reinsert the check without having to reset the terminal and start over. If the clerk continues to have problems with a specific check, he can simply start keying in the MICR data manually (see next item below).

- **Manual MICR Entry Always Available.** Whenever the terminal displays a prompt to insert the check for automatic reading, the clerk can start keying the data manually. The terminal detects the start of manual entry and switches to the mode to accept the data by this mode. This eliminates the need to wait for a time-out or a bad MICR read to switch to manual input.

- **Unique NCN Re-send Option.** Sometimes check verification requests fail to complete due to phone line problems. In such cases, the clerk can simply re-send the most recent check verification request by pressing the **BACKSPACE** key at the initial startup menu. This avoids the tedious task of re-entering all the data.

- **Print/No Print Option.** The CM3000 program has the capability to print a short summary on the P-250 roll printer whenever the verification returns either a warning or a decline. This printout includes the name and phone number of the agency that has one or more returned checks. Giving this printout to the check writer helps defuse a bad situation that can be intimidating to the clerk, and at the same time, gives the check writer all the information he needs to resolve the situation. The configuration mode allows enabling or disabling of this printout according to the desires of the agency or merchant and reflecting the presence or absence of a printer. When used with Velocity PLUS® (which does not return a name and phone number), each agency can store its name and number to print on all such receipts.

- **Easy Recall of Transmit and Receive Packets.** Sometimes troubleshooting of an installation difficulty requires examining either the transmit packet or the receive packet. The Setup Mode provides this information quickly, to make it easier to diagnose the problem - even over the telephone.

Troubleshooting the CM3000 Terminal

Table 9-3. CM3000 Troubleshooting

Problem	Solution
No Carrier	• Check connection of phone line to terminal • Verify phone line dialtone with analog telephone • Place an 'F' in front of the phone number (F for forced dialing)

Table 9-3. CM3000 Troubleshooting

Problem	Solution
No Dialtone	• Check connection of phone line to terminal • Verify phone line dialtone with analog telephone • Place an 'F' in front of the phone number (F for forced dialing)

NCN
NATIONAL CHECK NETWORK

Section
10

Verifone Terminals

In this section...

- Basic Operation of VeriFone Terminals
- Downloading of Single Key Programs to the Terminal
- Verifone Terminal - Check Reader Configuration
- Verifone Terminal - Other Setup Parameters
- Terminal Troubleshooting

10 - Verifone Terminals

The most common point-of-sale terminals are those manufactured and marketed by VeriFone Corporation. The NCN system has been designed to work with these terminals and special programs for the VeriFone terminals have been developed. Other terminals, such as the Hypercom, can also conduct NCN transactions.

There are several types of terminals in use today, with significant improvements developed over the course of many years. The TRANZ terminals are sold much more frequently today than the earlier ZON terminals. The TRANZ line of terminals offers much greater speed, capability and flexibility than these earlier terminals and the NCN system takes advantage of this increased performance.

Many merchants already have credit card terminals and do not want an additional terminal for checks. They want to use the VeriFone terminal capability to have several different programs, dialing different phone numbers, with each program activated by pressing a different **key**. NCN has a complete set of **"single key"** (sometimes called "**single packet")** programs for this purpose, downloaded through a computer with an 800 telephone number.

Even though ZON terminals are sold infrequently, there is a large number of these terminals still in operation today. Many merchants inquire about the possibility of using these terminals with the NCN system. The ZON terminals also cost considerably less than the TRANZ terminals, so collection agencies furnishing equipment have a strong motivation to use them instead of TRANZ terminals. Unfortunately, these terminals are significantly more primitive than the TRANZ terminals and operate at one-fourth of the speed.

Merchants already having terminals in use for credit card authorization and wanting to add the code for connecting to the NCN system must do a little investigation. Each such case must be analyzed to determine if this is possible. There are many different programs for credit card authorization of widely varying size. Some of them store transaction in the TRANZ 330 memory and others do not. Depending upon the size of the existing program and other requirements for memory, it can be very difficult to merge it with the RMRS code.

The following list summarizes the different VeriFone terminals, showing capabilities, limitations, advantages and disadvantages. Moving down through the list, functions that appear at one stage are not re-listed for more advanced terminals, even though they exist. In general, assume that each terminal has the functions of earlier terminals plus the items specifically listed for the terminal.

Verifone Terminals Models:

Four terminals are available in the Verifone models. The following paragraphs describe each model.

ZON Jr PLUS

- No check reader input
- ID-based transactions or manually keyed MICR transactions only
- Manual entry of alphabetic characters very awkward
- Communicates at 300 Baud
- Cannot combine credit card and check verification (no partial download)
- Credit card transactions more costly due to lack of draft capture capability
- Very inexpensive and widely available on used market

ZON Jr XL

- Handles check reader and printer
- Can perform MICR-based or ID-based single packet transactions
- Communicates at 300 Baud
- Can combine credit cards and check verification with partial download
- Credit card draft capture available
- Extremely common for credit card transactions, especially in some parts of the country
- Inexpensive and widely available on used market

XL-300

Very similar to ZON Jr XL

TRANZ 330

- Supports more sophisticated programs for both checks and credit cards
- Communicates at 1200 Baud
- Many merchants upgrading to this terminal due to changes in credit card pricing

TRANZ 340

- LAN version of the TRANZ 330
- Communicates only through TRANZiT 1200 or equivalent device
- Combined credit card and check verification program available through NCN.

TRANZ 380

- Same features as TRANZ 330 with larger memory
- “Split key” version operates (almost) like two independent TRANZ 330's

OMNI 380/480/490

- Much more capability than TRANZ family
- Programmed in “C”
- Cannot combine programs from two different sources
- Significantly more expensive than TRANZ terminals

Basic Operation of VeriFone Terminals

The VeriFone terminals operate in a straight forward manner. Some basic topics and terminology require some explanation.

The terminals consist of a keyboard, display, connections to other devices such as a check reader and printer, and an internal memory. The memory holds configuration data such as merchant location and dial up phone number, one or more programs that control the operation of the terminal, and special batch capture of credit card transactions. Individual memory locations have a 2-4 digit number, called a “**location**”. Some locations can serve multiple, general purpose functions (e.g. data storage, program storage), while others can only serve a single, specific function.

Transactions using these terminals start with the clerk either pressing a numbered key or performing some other action such as swiping a credit card. The initiation action causes the terminal to execute a program stored in a specific location. Each numbered key has a group of locations associated with it, called "**key locations**". These groups of locations are numbered with the specific key determining the first digit. Thus, for example, the key locations used for transactions initiated by pressing key "7" have addresses 700 - 712. Pressing key "7" momentarily displays a prompt stored in location 708 and then starts a program stored in location 707 to build up a data packet using the merchant location stored in location 704 and other data as entered using the program. It dials the phone number stored in location 700, sends the packet and processes the reply packet using a program stored in locations 710 and 711.

Transactions initiated using other keys work exactly the same way using locations x00 - x12, where "x" is any key in the range of 1 - 9. As transaction complexity increases, the programs grow too large to fit in a single location, so instructions exist to transfer control to other locations in general purpose memory that contain further program instructions. Early terminals such as the ZON Jr PLUS have only very limited memory with a two digit address and only permit programs started by keys 1 - 5. Later terminals, such as the TRANZ 380 have much more memory with a four digit address. The basic concepts carry though the entire line however, with increased memory and program capability in later terminals.

Setting up a terminal for a download usually requires examination of the contents of specific locations and storage of new data in these locations. The following paragraphs explain these basic operations.

Verifone Terminal EPROM Versions

Table 10-1. Verifone EPROM Versions

Version	Details
EPROM Version Release Numbers	Important things to be aware of concerning the Verifone terminals is the EPROM version and release numbers. The EPROM version is displayed briefly when the unit is powered on. Version and release numbers resemble the following: ZON Jr XL-Jr XL **XE2AU**2.8 XL 300-XL 300 **LE2AU**1.25 TRANZ 330-TZ 330 **3E2EU**2.1 TRANZ 380-TZ 380 **9E2EU**1.23 Where the **bold** letters represent the version and the underlined

Table 10-2. Verifone EPROM Minimum Requirements

Verifone Terminal Type	EPROM Minimum Requirements
ZON Jr XL	The Verifone ZON Jr XL in order to work with a checkreader, must be EPROM **release number 2.8 or higher.**
	When using a Printer and Checkreader, you must employ a "Y" cable Password access to Functions 7 and 8 is [1] [6] [6] [8] [3] [1] [FUNC/ENTER].
XL 300	The Verifone XL 300, in order to work with a checkreader, must be EPROM **release number 1.25 or higher.**
	When using a Printer and Checkreader, you must employ a "Y" cable. Password access to Functions 7 and 8 is [1] [6] [6] [8] [3] [1] [FUNC/ENTER].

Table 10-2. Verifone EPROM Minimum Requirements

Verifone Terminal Type	EPROM Minimum Requirements
TRANZ 330	The Verifone TRANZ 330, in order to work with a checkreader, must be EPROM **release number 2.1 or higher.**
	When using a Printer and Checkreader, you have the option of employing the 6 Pin PIN Pad port for checkreader use. Password access to Functions 7 and 8 is [1] [ALPHA] [ALPHA] [6] [6] [8] [3] [1] [FUNC/ENTER].
TRANZ 380	The Verifone TRANZ 380, in order to work with a checkreader, can be **any EPROM release number.**
	When using a Printer and Checkreader, you have the option of employing the 6 Pin PIN Pad port for checkreader use. Password access to Functions 7 and 8 is [1] [ALPHA] [ALPHA] [6] [6] [8] [3] [1] [FUNC/ENTER]. All memory locations in the TRANZ 380 contain 4 digits instead of 3 (as on the other terminals). Therefore, you need to add a leading 0 (zero) in front of all address locations. Example: 200 would be 0200, 019 would be 0019, etc.
TRANZ 380 X2	The Verifone TRANZ 380 X2 has the same features as the regular TRANZ 380, but with twice the chip capacity. It has a dual chip, hence the name X2. The only additional information you need to remember is the extra download step explained on page .
TRANZ 420/460	Use the same programs as are compatible with the TRANZ 330/380. Checkreader connections are mini-DIN, instead of the full DIN normally found on XL and TRANZ terminals.

Examine a memory location

VeriFone terminals have a built in function to examine a specific memory location.

To examine a memory location:

1. Press the <CLEAR> key on the terminal.
2. Press the <FUNC/ENTER> key.

   The terminal responds with:

   FUNCTION?

3. Press “7” to use the examine function.

   The terminal then responds with:

RECALL WHAT?

4. Enter the location address. Key in the location number of interest. If you key the required number of digits for the address, e.g. 000, the terminal displays the contents of the specified location. Alternately, you can omit leading zeroes and push the <FUNC/ENTER> key when the non-zero part is complete. The display is similar to the one shown below:

   000=18007573583

> **NOTE**
> If the location contains more than 12 characters, use the "#" key to move **(scroll)** to the right (the display actually shifts to the left to show characters off the screen to the right) and the "*" key to move back to the left.

   To examine the next location in numerical sequence, press <FUNC/ENTER>.

   To examine the previous location in numerical sequence, press <ALPHA>.

   To examine a totally different location, just key in the digits of the new address.

5. When finished examining locations, press <CLEAR>.

Store data in a location

VeriFone terminals also have a built in function to store new data in a location.

To store data in a location:

1. Press <CLEAR> followed by <FUNC/ENTER>.

2. When the “FUNCTION?” prompt appears, press “8”.

   The terminal responds with the password prompt:

   ENTER PASSWORD

3. Key in the password (166831 for ZON Jr terminals and 1<ALPHA><ALPHA>66831 for TRANZ terminals).

   As you key in the password, an asterisk “*” appears for each entered character. If you make a mistake, use the <BACKSPACE> key to eliminate the erroneous character.

4. After entering the password, press the <FUNC/ENTER> key.

   The terminal displays:

   STORE WHAT?

This prompt is somewhat misleading and might be better if it displayed “STORE WHERE?”. It wants you to enter the location number.

1. Key in the location in exactly the same manner as for examining locations.

2. When you have keyed all required digits or pressed the <FUNC/ENTER> key.

3. The address (location) appears followed by an equal sign “=”.

4. Key in the new data for that location, using the <ALPHA> key as required (and described below) for any non-numeric keys.

5. Press <FUNC/ENTER>.

   The “STORE WHAT?” prompt appears.

To enter alphabetic characters

Sometimes it is necessary to key in alphabetic characters instead of numbers, such as when entering ID's that include letters. The terminal keyboard has the alphabetic characters written above the numbers. Thus, the “1” key also has “Q” and “Z” and “.” written on it, the “2” key has “A”, “B”, and “C” written on it, etc.

On most VeriFone terminals, to obtain one of these characters, press the corresponding number followed by the <ALPHA> key.

Each time the <ALPHA> key is depressed, the character changes to the next character shown on the key.

For example, to obtain the character “B”, push:

<2> <ALPHA> <ALPHA>

To obtain a decimal point, push:

<1> <ALPHA> <ALPHA> <ALPHA>

While this can seem awkward at first, it rapidly becomes routine.

The **ZON Jr PLUS** has a much more rudimentary scheme since it lacks the <ALPHA> key. In place of this key, the <ENTER> function, obtained by pressing the “#” key, performs multiple different tasks, depending upon the context.

1. To obtain alphabetical characters, press the “#” (<ENTER>) key, and then press the number key that has the desired letter multiple times until the letter appears. You must do this for each character. When the character is correct, press the “#” key again to terminate entry of that character.

2. When the terminal expects a new character, pressing the “#” key adds an underscore character to the right of the last entered character. This gets replaced by the next entered character, that appears as an alphabetical character.

3. When completing entry of data into the ZON Jr PLUS, press the "#" (<ENTER>) key twice or even three times if terminal is accepting number keys interpreted as letters. If the terminal is accepting numbers as letters, the first press of "#" terminates the alphabetical entry mode and puts it in the numerical character input mode. Pressing "#" when in numerical input mode places the underscore character after the last

entered character in anticipation of a possible alphabetical character. The final "#" erases this underscore character and terminates data entry.

NOTE

NCN has an option to substitute numerical equivalent state codes for the alphabetical driver's license codes described above. This can eliminate much of the awkward steps required to enter alphabetical codes. Contact RMRS for more information on this option.

Downloading of Single Key Programs to the Terminal

Most programs for VeriFone terminals use at least some memory locations outside the "key locations". This causes enormous problems with partial downloads due to the lack of automatic techniques to avoid conflicts with locations used by other programs. To avoid these problems, NCN. has developed a complete set of programs that are small enough to fit in "key memory" for a single key without using any additional locations. These programs have limited flexibility and very concise user prompts, but they avoid a very large difficulty by fitting in the limited number of locations. The download service offered by NCN. to all NCN users makes all of these programs available.

Appendix A gives a complete list of "single key" programs and complete function programs available through the download service. Counting all of the possible key combinations, this list includes over 300 different programs for a wide variety of terminals and verification requirements. NCN. continually maintains and improves these programs to reflect changes and enhancements made to NCN. This section describes the steps to download these programs.

The capability of having several different programs in a single terminal allows such a terminal to conduct both credit card and check verification transactions. Furthermore, the ZON Jr XL and TRANZ terminals support a **partial download** to add new programs to existing terminals without affecting the original program. For this to work, you must abide by some restrictions:

1. **Partial downloads require a special key stroke sequence to avoid erasing existing programs**.

2. **New programs must not use any locations used by earlier programs**. Since there are no standards or guidelines for identifying and avoiding locations already in use, this is very tricky. The only safe approach to avoiding these problems is to only use the key locations for a single, unused key.

3. **The download process requires entering data in three special locations** that specify the phone number for the download computer, the download ID, and the name of the program to download. Some credit card programs use these data, especially the download ID, so you should restore them after the download.

To download a VeriFone terminal:

The general steps for downloading a VeriFone terminal are given below and then explained in more detail in the succeeding paragraphs. This procedure assumes that the programs are being loaded on an existing terminal that already has an operating credit card program and is installed at the merchant location.

1. Determine the “single key” available for check verification. Find an unused set of “single key” locations by talking to the credit card processor, talking to the merchant, and examining the terminal. No single approach works in all cases, so various approaches are explained below.

2. Verify availability of general purpose locations, if required. If the program you want to use requires general purpose locations, verify that the ones specified in Appendix A for your application are empty (i.e. not used by the credit card program).

CAUTION

Failure to perform this step is the primary cause of problems with credit card programs!

Finding unused key locations:

The following approaches have been used to find a set of unused key locations. None of these approaches works in all cases, and usually it is necessary to try a combination of these techniques.

1. Call the credit card processor and ask them which keys are available. This is the most reliable approach, but it requires some perseverance to reach someone who actually knows the correct answer. It also carries some risk since some credit card processors adamantly don't want anyone else adding code to “their” terminal and can attempt to prevent you from doing so. Sometimes your merchant can assist you by placing pressure on the processor to cooperate.

   Examine location x07 where x = 2, 3, 4,. . . 9.
   If x07 = <empty>, the key is available.
   If x07 = *G*K (beep, then abort), the key is available

2. Ask the merchant which keys he uses for credit card transactions, voids, credits, and batch functions. Focus on unmentioned keys and ask if he ever uses them. This approach is not completely reliable as there can be functions available that the merchant never uses or that someone else uses (e.g. an accountant).

   Try pressing a key that you suspect is unused and see what it prompts you for. If the terminal displays “UNUSED KEY”, then you have located an available key. This technique can be used in conjunction with talking to the merchant and may help him recall a rarely used but important function.

   Look at the plastic template on the keyboard or the terminal guide furnished by the credit card processor to see what keys are obviously used. Many times, the template has a key designated for checks (commonly using one of the large national verification/guarantee services). If such a designation exists, it is logical to overwrite the existing code on that key.

3. Record the existing terminal data for the download phone number in location 000, the terminal ID in location 001, and the application name in location 019. Use the **examine memory** procedure described in Section 3.2 and be careful to distinguish zero from “oh” (zeroes have a diagonal slash through them), one from “I” (“I” has top and bottom bars), and six from “G” (must use context).

4. Enter the download phone number (18007573583) for NCN programs in location 000, your specific 9-digit identification code in location 001, and the program name from the list in Appendix A in location 019 using the **store data** procedure "Store data in a location" on page 10-6. NCN. assigns each user a unique identification code and uses it to make sure the program includes the correct phone number for verifications.

5. Perform a partial download by pressing the following sequence of keys:

   a. <CLEAR> <FUNC/ENTER> 0 *

      Sometimes the TRANZ terminal responds with an additional prompt:

      DNLD SPEED?

   b. If this happens, press "2".

      The download process proceeds automatically with a sequence of messages

      DIALING – terminal dials download computer

      WAITING FOR ANSWER – terminal waits for computer to answer

      COMMUNICATING – terminal sends its request to computer

      *** - - - - - - - download proceeding, with dashes replaced by asterisks, each representing 10% completion

      DOWNLOAD COMPLETE – download completed---terminal ready to use

6. Enter the NCN verification ID in address x04, where x refers to the specific single key program downloaded. This ID includes three pieces of information separated by dashes:

   - The site number assigned by RMRS
   - The merchant location number assigned by each NCN member to each of its merchants
   - The rule set number to be used for the transaction.

     It has the format:

     <site number>-<merchant location number>-<rule set number>

     The verification ID is used to access the specific rule set as described earlier. Follow the store data procedure described "Store data in a location" on page 10-6.

7. Restore the credit card data in locations 000, 001, and 019 that were recorded in step 3 on page 10-10. Use the standard store data procedure and be careful to key in alphabetic characters as necessary.

The most difficult part of this procedure is ascertaining a set of unused single key locations. This is more difficult than necessary due to widely varying degrees of cooperation by credit card processors. They frequently do not want anyone else adding code to the terminal, since it potentially could change their code and even possibly perpetrate credit card fraud. Sometimes they change the password so that others cannot examine, change locations or perform the download. Others can be extremely cooperative and helpful.

Verifone Terminal - Check Reader Configuration

Several different check readers can be used with the NCN system. The system requires that the check reader send "raw" (unparsed) data. Spaces must be retained and the special MICR characters for which there are no corresponding ASCII character codes must be encoded as follows:

- TRANSIT – symbol must be encoded as: T or t
- ON-US – symbol must be encoded as: O or o (the letter "oh", not zero)
- DASH – symbol must be encoded as: D, d, or -
- AMOUNT – symbol must be encoded as: A, a, or $

The following paragraphs explain how to set up the common check readers used with NCN.

Checkmate:

Older Checkmate check readers have a program, *CheckLoad*, that runs on a PC computer for configuring their check readers.

To install the Checkmate checkreader:

1. Start the program by typing: CHEKLOAD
   The program starts up and displays a list of applications for use with Velocity PLUS® including:

   Rocky Mountain Retail - Tranz 3xx
   Rocky Mountain Retail - XL/XL 300

2. Highlight the desired application.
3. Connect the cable between the PC computer and the check reader.
4. Run the special HOST PORT CONFIG check supplied by Checkmate through the reader to place it in the programming mode.
5. Press "D" to download the highlighted program
6. Remove the cable from the check reader and connect it to the terminal. Make sure to cycle power on the reader to take it out of configuration mode

IVI (formerly Soricon) MR-1000:

This reader has a set of 8 switches on the rear that configures it to produce the appropriate output for the system.

To install the IVI MR-1000 checkreader:

The required settings are:

- BAUD RATE = 1200
- PARITY = EVEN
- DATA BITS= 7
- STOP BITS=1

TRANZ terminals:

Set the switches to the following positions:

SW-4, SW-5, SW-8 UP

SW-1, SW-2, SW-3, SW-6, SW-7 DOWN

VeriFone ZON Jr XL terminals: Use a bi-directional communications protocol to achieve a handshake and query-response mode. The MR-1000 check reader can communicate in this mode, but it requires different switch settings.

Set the switches to the following positions:

SW-4, SW-5, SW-6, SW-7, SW-8 UP

SW-1, SW-2, SW-3 DOWN

IVI (formerly Soricon) MR-2x00:

The MR-2100 and the MR-2300 use any standard terminal emulation program such as CrossTalk or Procomm to set up the reader. The reader has a multitude of options including preambles, formats, communications parameters, etc. IVI has a manual that documents the procedure for this configuration. Alternately, IVI can supply special configuration checks that program the reader simply by running these special checks through it.

The second option is so easy and the first option is complex and always requires a computer and special cable, that you should obtain and use the configuration checks.

IVI CheckManager 3000:

This combination terminal and check reader usually stands beside other point of sale terminals, sometimes sharing a printer. It is dedicated to running checks and sometimes comes pre-programmed from the vendor. This eliminates the need to add an additional program to the VeriFone terminal that maybe dedicated to credit cards only. The program running on the CM 3000 contains multiple configuration options that can allow it to behave like several different standard programs for VeriFone terminals as listed in Appendix A. Please refer to the Checkmanager 3000 chapter to obtain the details on configuration and setup of this terminal/check reader.

Magtek:

Magtek has a special program, *SET-MICR*, for configuring its reader. This program has several setup screens to choose the proper format and communications protocol.

1. From the main menu (press <F2> to display it), press <ALT>-1 to bring up the communications parameters screen.

2. Set the parameters to 1200 Baud, 7 Bits/ Even parity

3. From the main menu (press <F2> to display it), press <ALT>-2 to bring up the message parameters screen.

4. Select Predefined Comm Mode to send: <data> [CR][LF] (= Comm Mode 3) for a TRANZ 3xx terminal or [STX] <data> [ETX] [LRC] (=Comm Mode 7) for a XL/XL 300 terminal.

5. From the main menu (press <F2> to display it), press <ALT>-4 to bring up the data format screen.

6. Select the Raw Data Format (Format 00)

7. Change the substitution table to “T” “O” “A” “D” “?”

8. Change the handling of spaces to “Send all spaces”

9. From the main menu (press <F2> to display it), press <ALT>-5 to operate the program and load the reader.

Stone West (formerly Direct Data) Cheq'r:

Its configuration can be changed using a special program developed by Stone West, called *CONFIGURAT'R.* To set up a Cheq'r reader for a TRANZ terminal, load the *CONFIGURAT'R software on a PC computer, select the directory containing the program, and type:*

CHEQR 1 -app A2DA1

NOTE

Loading a Cheq'r using *CONFIGURAT'R* requires a special cable that normally comes with the software. The above line assumes that this cable connects to the COM1 port on the computer.

To set up a Cheq'r for ZON Jr XL terminals, follow the same procedure except the entered line should be:

CHEQR 1 -app A2DB1

Welch Allyn:

Welch Allyn has two alternatives for configuring their check reader:

- Use a bar code reader with a special collection of codes and programming menu.
- Use special pre-printed configuration checks that changes the reader to output the proper data and format

The second option is so easy and the first option is so tedious, that you should obtain and use the configuration checks.

Verifone Terminal - Other Setup Parameters

Other setup options that you can configure are described in the following paragraphs.

Horizontal scroll

Some messages have more characters than the 16 character display can accommodate. When such messages are sent to the terminal, only the first 16 characters appear. To see the rest of the message, the <#> key serves as a right arrow. The <*> key serves as a left arrow if the display should move in the reverse direction On the ZON Jr PLUS, the scroll keys are the "9" for scroll to the right, and "7" for scroll to calendar/Clock

Resetting Time and Date on Verifone Terminals

The following steps describe how to change the Date and Time display on Verifone terminals. The Date and Time display is the default for the Terminal Idle Prompt.

ZON Jr XL / XL 300 / TRANZ 330

To set the time and date:

1. **Idle prompt** – Simultaneously press [*] and [3].

2. **DIAGNOSTICS** – Press [ALPHA] to begin the "reset clock" function.

3. **RTC CHIP TEST –** The terminal displays this message for two seconds while it tests the real time clock (RTC) chip. The terminal then prompts you through the following entries for resetting the date and time.

   If you make a mistake, press [BACKSPACE] and reenter the correct information.

4. **DAY OF WEEK –** Enter a digit identifying the current day of the week. Valid entries are:

   0 = Sunday

   1 = Monday

   2 = Tuesday

   3 = Wednesday

   4 = Thursday

   5 = Friday

   6 = Saturday

   7 = Sunday

   Press [FUNC/ENTER] after your entry.

5. **YEAR = 19 –** Enter the last two digits for the current year. Press [FUNC/ENTER].

6. **MONTH = –** Enter a number, 1 through 12, to identify the current month. For example, enter the number "6" for June. Press [FUNC/ENTER].

7. **DATE = –** Enter a number, 1 through 31, to identify the current date. For example, enter "14" for the date June 14. Press [FUNC/ENTER].

8. **HOUR = –** Enter a number, 1 through 12, to identify the current hour. For example, enter "10" if the time is 10:14. Press [FUNC/ENTER].

9. **AM = 0 PM = 1 –** Enter a "0" to indicate AM or a "1" to indicate PM. Press [FUNC/ENTER].

10. **MINUTES = –** Enter the number of minutes, from 0 to 59, currently past the hour. For example, enter "14" if the time is 10:14. Press [FUNC/ENTER].

11. **SECONDS = –** Enter the number of seconds from 0 to 59, currently past the minute. For example, enter “23” if the time is 10:14:23. Press [FUNC/ENTER].

12. **Day of week, Date –** The terminal displays the new date and time.

TRANZ 380 / TRANZ 420

To set the time and date:

1. **Idle prompt** – Simultaneously press [*] and [3].

2. **DIAGNOSTICS** – The terminal displays this message for two seconds while it tests the real time clock (RTC) chip. The terminal then prompts you through the following entries for resetting the date and time.

   If you make a mistake, press [BACKSPACE] and reenter the correct information.

3. **YEAR 1980-2079 =** – Enter two digits for the current year. For example, enter “91” for the year 1991. Press [FUNC/ENTER].

4. **MONTH =** – Enter a number, 1 through 12, to identify the current month. For example, enter the number “6” for June. Press [FUNC/ENTER].

5. **DAY =** – Enter a number, 1 through 31, to identify the current day. For example, enter “14” for the date June 14. Press [FUNC/ENTER].

6. **HOUR 0-23 =** – Enter a number, 0 through 23, to identify the current hour in a 24-hour format. For example, enter “10” if the time is 10 a.m.; enter “16” if the time is 4 p.m. Press [FUNC/ENTER].

7. **MINUTES =** – Enter the number of minutes, from 0 to 59, currently past the hour. For example, enter “14” if the time is 10:14. Press [FUNC/ENTER].

8. **SECONDS =** – Enter the number of seconds from 0 to 59, currently past the minute. For example, enter “23” if the time is 10:14:23. Press [FUNC/ENTER].

9. **Day of week, date** – The terminal displays the new date and time.

Terminal Idle Prompt

The default Terminal Idle Prompt for the ZON Jr XL, XL 300, TRANZ 330, TRANZ 380 and TRANZ 420 is the Date/Time display. The default for the ZON Jr PLUS is “Ready”. All of these defaults can be overridden by entering an alternate Terminal Idle Prompt in a specific Memory Location. Follow the instructions below to alter the Terminal Idle Prompt.

ZON Jr XL / XL 300 / TRANZ 330 / TRANZ 380 / TRANZ 420

1. **Idle Prompt** – Press [FUNC/ENTER].

2. **FUNCTION?** – Press [8].

3. **ENTER PASSWORD** – Enter the terminal password to unlock memory information. The terminal password supplied with each TRANZ 330, TRANZ 380 and TRANZ 420 terminal is Z66831. You can enter this password by pressing [1] [ALPHA] [ALPHA] [6] [6] [8] [3] [1]. For ZON Jr XL's and XL 300's the password is simply 166831.

4. ****** – The terminal displays an asterisk (*) for each key entered (except for the ALPHA key press). After entering the complete password press [FUNC/ENTER].

NOTE

Some credit card processors change the standard terminal password to one of their own. If after pressing the [FUNC/ENTER] key, the display does not read what is shown in Step 6, then you can press [CLEAR] and repeat steps 2-4 or call the credit card processor and explain to them that you are attempting a partial download of your check program into one of their credit card terminals and you need their terminal password. Enter the credit card processors unique password then press [FUNC/ENTER] if applicable.

5. **STORE WHAT?** – Enter the desired memory location number (000 to 999) of the data you want to change. In this case enter [0] [3] [0] or [0] [0] [3] [0] for the TRANZ 380.

6. **030 =** – Enter the characters you want to display as the new

   or

   Terminal Idle Prompt, then press [FUNC/ENTER].

   0030 =

NOTE

Memory Location 30 holds 16 characters in the ZON Jr XL, TRANZ 330 and TRANZ 380; 20 characters in the XL 300; and 30 characters in the TRANZ 420.

ZON Jr PLUS

The ZON Jr PLUS, if downloaded with our Jr PLUS program, displays CHECKCARE PLUS. There probably is no need to change this since the terminal cannot be shared with another processor. However, if the need arises, please follow the instructions below.

1. **Idle prompt** – Press [FUNC/ENTER].

2. **FUNCTION** – Press [8].

3. **PASSWORD?** – Enter the terminal password to unlock memory information. The password is 166831. Press [#].

4. **STORE WHAT?** – Press [6] [0].

5. **60 =** – Enter the characters you want to be displayed as the Terminal Idle Prompt, then press [#].

NOTE
Remember to press [#] before and after each alpha character.

Resetting the Terminal Idle Prompt back to the Default Setting

If you want to set the Terminal Idle Prompt back to the default, Date and Time or "Ready" for the Jr PLUS, this can be easily done by "blanking out" the alternate memory location. Follow the instructions below.

1. **Idle prompt** – Press [FUNC/ENTER]

   or

   [#] for the Jr PLUS.

2. **FUNCTION?** – Press [8].

3. **ENTER PASSWORD** – Enter the terminal password to unlock memory or information and select FUNC/ENTER. The terminal password supplied with each TRANZ 330, TRANZ 380 and TRANZ 420 terminal is **Z66831**.

   For ZON Jr XL's, XL 300's and the ZON Jr PLUS the password is **166831**.

   Press [FUNC/ENTER]

   or

   [#] for the Jr PLUS.

4. **STORE WHAT?** – Press [0] [3] [0]

   or

   Press [0] [0] [3] [0] for the TRANZ 380

   or

   Press [6] [0] for the Jr PLUS.

5. **030 =** – Press [FUNC/ENTER]

   or

   0030 = – [#] for the Jr PLUS.

   or

   60 =

6. **STORE WHAT?** – Press [CLEAR]. The Terminal Idle Prompt is now back to the default.

Terminal Troubleshooting

Table 10-3. Terminal Troubleshooting

Display Message	Problem	Solution
APPL NOT FOUND	This message is displayed on the Verifone terminal while attempting to download a program whenever the application name in memory location 019 is not found	Use the RECALL feature to inspect the program name you have stored in memory location 019. The program you are attempting to download does not exist. There is probably a missing or incorrect character in the program name you have entered. Make the necessary changes and try again
BAD LOC/RULE NUM	This message is returned to the point of sale device if the location/rule number is in an improper format.	Use the RECALL feature to inspect the location number in x04. The number should be no more than 11 characters long. If it is that long, it must be in the 999999-9999, location - rule set format. If it is not in this format, it can be no longer than 6 digits.
DOWNLOAD AGAIN	This message is displayed on the Verifone terminal 8 seconds after "NO SERIAL # USED" is displayed, when you initially push the key the check program is loaded on.	You have either done a "full" download instead of a "partial", or you have done a "partial" download without putting your serial number in location 001. Use the RECALL feature to inspect location 001 - make sure it is correct. Re-download the program making sure to do a "partial" download - [FUNC/ENTER] [0] [*].
ERROR IN ID	This message is returned from the verification system if the ID (Driver's License) number is not compatible with the information stored in the ruleset that was setup by your agency in the National Database system.	Ensure you are using the correct State code - alpha or numeric, and that you are entering the ID correctly. If you are swiping a magnetically encoded ID through the Verifone, the data picked up on the magnetic strip probably has more than just the ID/DL number encoded. Try the transaction again, entering the ID/DL number manually.
ERROR IN MICR	This message is returned from the verification system if the ABA and/or Account # do not have the proper amount of digits, or there are missing Transit or On-Us symbols from the check's MICR line.	If you are using a manual check program, ensure the user knows how to key in the ABA and Account numbers. If utilizing a checkreader, inspect the check to ensure the appropriate symbols and ABA and Account numbers exist in the MICR line. The ABA number must be 9 digits long - no more or less. The Account number must be 4 digits or greater .

Table 10-3. Terminal Troubleshooting (Cont.)

Display Message	Problem	Solution
INVALID MEM SIZE	This message is displayed on the Verifone terminal during a Terminal to Terminal download when the EPROM versions are incompatible. Refer to page for proper versions and release numbers.	Power-off the two terminals, then back on again and read the display to determine if they are compatible. EPROM versions should be the same.
KEY IN ACCT NUM	This message is displayed as soon as you press the "Check" key on the Verifone terminal, instead of *INSERT CHECK*.	The version release number of the terminal is too old. Disconnect the power cord from the rear of the terminal, reconnect it and check the release number. See pages - for correct version release numbers for each terminal type. This also happens on a ZON Jr XL or XL 300 if you have input a "6" in location *x*06 - *x*06 should be empty.
KEY IN ACCT NUM	This message is displayed after you attempt to run a check through the checkreader, either immediately, or after the "time-out" period.	Press [CLEAR] and try the transaction again. If the problem persists it could be one of the following: n DIP switches (Soricon checkreaders only) are improperly set. Power-off the reader, set the switches, power-on and try again. n Possible old firmware protocol reader (MAG-TEK MICR before '1996 or CHEQ'R). n Replace the unit with a known working reader. n Replace the cable with a known working cable. n An older reader (Soricon, IVI, Checkmate) could need cleaning. Clean the checkreader and try again.

Table 10-3. Terminal Troubleshooting (Cont.)

Display Message	Problem	Solution
LOST COMM W/HOST	The host computer has disconnected the phone line. This message can also come about when the Verifone attempts to call a number from within an internal phone system that requires a 9 to access an outside line. It appears as if a connection was made with the download or verification system, then abruptly dropped. But the connection was made with the internal phone system that did not know how to interpret the Verifone information and then dropped the line. Try inserting a 9, and a pause (-) if needed, and try again. There have been cases where the client insisted the line was a direct line, only to discover later that it was part of their internal phone system. Try the 9 anyway - it can't hurt, and could save a lot of diagnosing time and headaches.	This indicates that the phone line had problems and the terminal lost communication with the host (download or verification) computer. Check your telephone line connections, then attempt the download (or verification) again. If no other clients are reporting this problem, then it is unlikely that the nation host system is at fault. If you are attempting a download, there can be a problem with the 800 number connection. Try the regular phone number, 1-303-442-2105. There can be a problem with the Verifone modem. (Even though the Credit Card program is not experiencing problems with transactions, their dial-up process and host modem can be much more sophisticated - allowing for line problems.) Download the check program onto a spare terminal and try it with the same phone lines. If it consistently works, then you have a problem with the other terminal.
NO ANSWER	This message is displayed on the Verifone terminal if it does not detect a carrier from the host computer.	Use the RECALL feature to check the phone number you are dialing. If you are attempting to download a program this is memory location 000. If you are attempting a verification, this is memory location X00, where "X" is the key on which the program is stored. Remember, you may have to input a "9" and possibly a pause (-) in front of the phone number to access an outside line. If the number is entered correctly, then the host computer is probably busy with another verification or download. The terminal re-dials two more times, 8 rings each, on its own. You can press [CLEAR] to stop this in order to check the phone number or you can wait a few minutes and try again.
NO ENQ FROM HOST	This message is displayed if the Verifone terminal does not receive the expected character from the host computer in the specified time-out period.	This indicates that a connection was established with the host computer but the transaction was not completed. Probably due to noise on the telephone line or poor telephone line connections. Check the connections and try the procedure again. If no other clients are reporting this problem, then it is unlikely that the nation host system is at fault.

Table 10-3. Terminal Troubleshooting (Cont.)

Display Message	Problem	Solution
NO SERIAL # USED	This message is displayed on the Verifone terminal when you initially push the key the check program is loaded on.	You have either done a "full" download instead of a "partial", or you have done a "partial" download without putting your serial number in location 001. Use the RECALL feature to inspect location 001 - make sure it is correct. Redownload the program making sure to do a "partial" download - [FUNC/ENTER] [0] [*].
PACKET ERROR *or* **--RETRY**	These messages can be displayed at the point of sale device after a transaction attempt. The verification machine has a detected a problem with the packet structure.	Try redownloading the program and attempting another transaction. If you continue to get one of these messages after reprogramming, call NCN. If you are attempting a transaction from a terminal type other than Verifone, contact NCN - the POS terminal is sending a packet that the National Database does not recognize.
PROGRAMMING ERR X	The Verifone terminal has detected bad data in its memory. It has been found that option 2 also clears the error - "**D.C. MEMORY ERROR**".	It remains frozen until memory is reinitialized or a programming error override is performed. **CAUTION** **Reinitializing memory completely erases <u>all</u> credit card transactions, check information and all programs from the terminal**. 1. To perform a programming error override, press the [5] and [3] keys simultaneously and hold them down one or two seconds. After this, you can attempt another download, however, Verifone suggests that a reintialization be performed and all programs reloaded. This is because even though the override worked, you still can have corrupted memory that will cause problems later. 2. To reinitialize the terminal, press the [1] and [FUNC/ENTER] keys simultaneously and hold them down one or two seconds. After this you must reload all credit card and check programs. 3. Powering the terminal off and back on does not reset it.
SERIAL # NOT FND	This message is displayed on the Verifone terminal when the host (download computer) does not recognize the number in memory location 001.	You have probably entered your SERIAL download number incorrectly into memory location 001. Inspect this location with the RECALL feature. If it is not correct, make the appropriate changes and try again.

Table 10-3. Terminal Troubleshooting (Cont.)

Display Message	Problem	Solution
UNKNOWN LOC/RULE	This message is displayed on the Verifone terminal when the host (verification computer) does not recognize the number in X04 (where "X" is the check program key).	Check the number stored in memory location X04 using the RECALL feature and verify that it is correct. . Delete and reenter the Terminal Identification: (site#-Location- ruleset)
UNSUCCESSFUL DL	This message is displayed when the Verifone terminal is unable to complete the program download	This could be due to bad telephone lines, or problems not related to the terminal. Insure the telephone is functioning properly and try the download again.
WAITING FOR LINE	This message is displayed on the Verifone terminal when the telephone line it is trying to access is in use or not connected to the terminal.	Insure the telephone line is properly connected to the terminal. Check to see if there is a telephone connected to the same line that can be in use or off the hook. Check to see if the line has a dial tone.

Communication Problems

There have been a few suggestions discovered in the field that have been invaluable in solving a variety of communications problems when downloading to a terminal or performing transactions.

Table 10-4. Communication Problems Troubleshooting

Suggestions	Explanation
Slow down the Communication Speed	Speed is usually a good thing when performing verification transactions. But it can be a hindrance if the line/connection quality is very poor. Sometimes the merchant has no trouble connecting and completing Credit Card transactions, but has continual trouble connecting to your local Verification system. This is almost always the result of a poor connection. It doesn't necessarily mean that either you or the merchant has a bad line – it only means that the "path" opened by the phone company when A dials B is of poor quality. This problem can result in messages such as "LOST COM W/HOST", "BAD RX COMMUN", "BAD TX COMMUN", and even "WAITING FOR ANSR" – "NO ANSWER". If you are using a TRANZ type terminal (one that communicates at 1200 Baud), you can slow the transaction speed down to 300 Baud. This is accomplished by putting an "M" in front of the phone number in location x00 and x01. Example: If you are on key 7, and 700 and 701 contain "18005551212", then change that to "M18005551212".
Download Slower	The same principle applies to problems with downloading. If you are having problems with the download, you can slow the download speed on TRANZ terminals by changing the value of location 960 from a "2" to a "1". Just be sure to change it back after you're finished.

Selection and List of VeriFone Programs from NCN

The following tables help you select the features and the programs for VeriFone terminals from NCN.

Selection Guide

Table 10-5. Selection Guide

	ZON Jr XL	TRANZ 330	TRANZ 380
SINGLE KEY PROGRAMS			
MICR (any check reader) w/ chk amount		SK33x	SK38x
MICR (any reader) thru PIN pad port, w/ chk amt		SK33xP	SK38xP
MICR (Soricon MR-1000 reader only) w/ chk amt	JRXLx		
MICR (non-MR-1000 reader) w/ chk. amount	JRXLDx		
MICR w/ chk amount & sale amount		SKS33x	SKS38x
MICR w/o amount (non-MR-1000 reader on XL)	FKXLDx	FK33x	FK38x
MICR (manually keyed) w/ chk amount	JRXLMx	SK33xM	SK38xM
ID-based (DL) w/ chk. amount	ZONIDDx	33IDDx	38IDDx
ID-based (SS) w/ chk. amount	ZONIDSx	33IDSx	38IDSx
MULTI-FUNCTION PROGRAMS			
MICR (any reader) 3 key, w/ chk amount		SP33789	SP38789
MICR (MR-1000 reader) 3 key, w/ chk amount	XL789		
MICR (non-IVI reader) 3 key, w/ chk amount	XLD789		
MICR (any reader) plus Driver's License		SPMDLx	SPMDL8x
MICR (any reader) 3 function (1 key) w/ chk amt		SPxPYRL	SPxPYR8
MICR 3 function/1key, w/ chk amt & W/D print		MFxPNTR	MF38xPT
ID-based (DL) w/ check amount, & W/D print		33DLxPT	

NOTE

The XL300 uses the same programs as the ZON Jr XL EXCEPT when used with an IVI MR-1000 check reader, that requires a special cable and a special program.

Program List

In the lists that follow, please note the distinction between **check amount** and **sale amount**. All programs, with the exception of FK33x and FK38x, ask for the check amount. Few users want sale amount except supermarkets, who return cash to the customer.

Programs for the ZON Jr XL or XL 300

These programs all prompt for the check amount after getting the MICR or ID. Four of them also prompt for the sale amount that is used to calculate cash back to the customer. Note that the letter "*x*" denotes your choice of the key used for the program, always between 2 and 9.

Table 10-6. Program List

Program Name	Description
JRXL*x*	MICR transactions with check reader input (IVI=Soricon)
JRXLD*x*	MICR transactions with check reader input (non-IVI)
JRXLM*x*	MICR transactions with manual keying of check data
FKXLDx	MICR transactions w/ check reader input (non-IVI) and amount = 0.00
ZONIDC*x*	I.D.-based transactions with courtesy card
ZONIDD*x*	I.D.-based transactions with driver's license
ZONIDP*x*	I.D.-based transactions with phone number
ZONIDS*x*	I.D.-based transactions with Social Security number
ZNIDC*x*S	I.D.-based transactions with courtesy card, check amount & sale amount
ZNIDD*x*S	I.D.-based transactions with driver's license, check amount & sale amount
ZNIDP*x*S	I.D.-based transactions with phone number, check amount & sale amount
ZNIDS*x*S	I.D.-based transactions with Social Security number, chk amt & sale amt
XL789	Key "7" = MICR transaction w/o ID; Key "8" = MICR transaction w/ ID; Key "9" = payroll check w/ ID; All use Soricon check reader ; Early dial if Loc 399 = 1; Sale amount if Loc 397 = 1. Uses extra Locs 380-399.
In this table, "x" is any integer between 2 and 9 (inclusive)	

Table 10-6. Program List (Cont.)

XLD789	Key "7" = MICR transaction w/o ID; Key "8" = MICR transaction w/ ID; Key "9" = payroll check w/ ID; All use non-Soricon check reader; Early dial if Loc 399 = 1; Sale amount if Loc 397 = 1. Uses extra Locs 380-399.
In this table, "x" is any integer between 2 and 9 (inclusive)	

Programs for the XL 300 with IVI reader

The XL 300 requires a special cable for IVI reader.

Table 10-7. Programs for the XI 300 with IVI reader

Program Name	Description
XL300	MICR transactions with check reader input (Soricon)
XL3789	Same functions as XL789

Programs for the TRANZ 330

Except for FK33*x*, these programs all prompt for the check amount after getting the MICR or ID. Five of them also prompt for the sale amount that is used to calculate cash back to the customer. Note that the letter "*x*" denotes your choice of the key used for the program, always between 2 and 9. Programs for the TRANZ 330 work for all check readers.

Table 10-8. Program for the TRANZ 330

Program Name	Description
FK33*x*	MICR transactions with check reader input but NO CHECK AMOUNT
SK33*x*	MICR transactions with check reader input
SK33xP	MICR transactions with check reader input through PIN pad port
SKS33*x*	MICR transactions with check reader input & sale amount
SK33*x*M	MICR transactions with manual keying of check data
33IDD*x*	I.D.-based transaction with driver's license
33IDS*x*	I.D.-based transaction with Social Security number
SP33789	Key "7" = MICR transaction w/o ID; Key "8" = MICR transaction w/ ID; Key "9" = payroll check w/ ID; All use check reader; Early dial if Loc 923 = 1; Skip sale amount if Loc 712 = 1. Uses extra Locs 913-923.
SPMDLx	Always gets both MICR (any reader) plus driver's license and check amount; never gets sale amount; Uses Locs 914-921 (regardless of key)
In this table, "x" is any integer between 2 and 9 (inclusive)	

Table 10-8. Program for the TRANZ 330 (Cont.)

SPxPYRL	All three transaction types initiated by key "x", using a secondary menu to select specific type; Skip sale amount if Loc x12 not empty. Locs x13-x33. Check reader input can use printer port or PIN pad port.
MFxPNTR	All three transaction types initiated by key "x", using a secondary menu to select specific type, and printing Warnings or Declines on roll printer. Skip sale amount if Loc x12 not empty. Locs x50-x80 for x=2,3,...,8; Locs 913-941 for x=9. Check reader input can use printer port or PIN pad port.
33DLxPT	ID-based transaction w/ driver's license and printing Warnings or Declines on roll printer. Locs x87-x99 for x=2,3,...,8; Locs 937-949 for x=9.
RMRS330	Full interactive program capable of performing all types of transactions on Velocity PLUS®
In this table, "x" is any integer between 2 and 9 (inclusive)	

Programs for the TRANZ 380

Except for FK38*x*, these programs all prompt for the check amount after getting the MICR or ID. Five of them also prompt for the sale amount that is used to calculate cash back to the customer. Note that the letter "*x*" denotes your choice of the key used for the program, always between 2 and 9. Programs for the TRANZ 380 work for all check readers.

Table 10-9. Programs for the TRANZ 380

Program Name	Description
FK38x	Same as FK38*x*
SK38*x*	Same as SK33x
SK38xP	Same as SK33x except check reader input through PIN pad port
SKS38*x*	Same as SKS33*x*
SK38*x*M	Same as SK33*x*M
38IDD*x*	I.D.-based transaction with driver's license
38IDS*x*	I.D.-based transaction with Social Security number
38IDC*x*S	I.D.-based transaction with courtesy card & sale amount
38IDD*x*S	I.D.-based transaction with driver's license & sale amount
38IDP*x*S	I.D.-based transaction with phone number & sale amount
38IDS*x*S	I.D.-based transaction with Social Security number & sale amt
In this table, "x" is any integer between 2 and 9 (inclusive)	

Table 10-9. Programs for the TRANZ 380 (Cont.)

SP38789	Key "7" = MICR transaction w/o ID; Key "8" = MICR transaction w/ ID; Key "9" = payroll check w/ ID; All use check reader (Soricon); Early dial if Loc 923 = 1; Skip sale amount if Loc 712 = 1. Uses extra Locs 913-923.
SPMDL8x	Always gets both MICR (any reader) plus driver's license and check amount; never gets sale amount; Uses Locs 914-921 (regardless of key)
SPxPYR8	Same as SPxPYRL
MF38xPT	Same as MFxPNTR
380	Full interactive program capable of performing all types of transactions on Velocity PLUS®. It uses the entire terminal and does not coexist with any credit card program
RMRS380	Full interactive program capable of performing all types of transactions on Velocity PLUS®. It uses the upper half of the terminal memory (non-split key) and can coexist with any credit card program that uses only the lower half of memory (Locs 0000 - 0999)
In this table, "x" is any integer between 2 and 9 (inclusive)	

Programs for the TRANZ 340

Table 10-10. Programs for the TRANZ 340

Program Name	Description
RMRS400	Credit card transactions into MAPP network (using external modem connected to TRANZiT 1200C) plus single packet MICR transactions (using internal modem of TRANZiT 1200C) with same functions of SP33789.

Programs for the ZON Jr PLUS

The ZON Jr PLUS does not provide for a program name. Instead, the download ID placed in location 01 accomplishes all program selection.

Table 10-11. Programs for the ZON Jr PLUS

Program Name	Description
(download ID)	MICR transactions with manual keying of check data
(download ID)	I.D.-based transactions with driver's license
(download ID)	I.D.-based transactions with Social Security number

1200C/340 Terminal Multilane System Setup

The following paragraphs provide information on setting up the 1200C/340 terminal.

TRANZiT 1200C Programming

The TRANZiT 1200C runs different programs depending upon whether it is connected directly to an In Store Computer or it dials out to a Multi Store Server or a Host.

The program for connecting directly to an In Store Computer is downloaded directly from a Velocity PLUS® system. The 1200C uses the same cable as for loading a TRANZ 340 or TRANZ 330, and it connects into the HOST port of the terminal. The steps were given earlier in this section along with the steps for loading a 330 or 340.

The 1200C can also use its internal modem to dial into a Velocity PLUS® system and conduct transactions initiated by a 340. If another 340 terminal starts a transaction before the first one finishes, the second one proceeds in parallel with the first. As long as new transactions come in before all pending ones are complete, the system maintains an open phone line. Furthermore, the system has the option of specifying an amount of time to hold the open line after all transactions are complete (see setup of COM_MAP.DAT in Section 3.2). As long as the line remains open, transactions occur at the same rapid response as found with the In Store Computer. For installations using local phone calls that do not incur charges based on the length of the call, this can provide extremely good service without the cost of an In Store Computer. The only negative is the requirement to dedicate a phone line for each store using the system in this way.

RMRS has a program for the 1200C to conduct transactions using this “dial-up LAN” approach on its download computer. To load the 1200C with this program, follow the download and setup procedure given below. It assumes that the 1200 is operating, an outside telephone line is attached, and that one or more VeriFone TRANZ 340's have been connected to the LAN input on the 1200.

To load the dial-up LAN:

1. Enter the system mode on the 1200. Perform the following key sequence:

   <CLEAR> 1 6 6 8 3 1 <ENTER>

   As you press these keys, the 1200 display remains unchanged, which is unnerving. After pressing the <ENTER> key at the end of the sequence, the 1200 should display:

   SYSTEM MODE

2. Enter the function mode on the 1200. Press the <ENTER> key and the message should change to:

   FUNCTION?

3. Store the Download ID in location 992. Press key “8” to enter the store mode. The 1200 should display:

   STORE WHAT?

4. Key in 992 <ENTER> and the display should read:

   992=

5. Key in the Download ID your agency uses for downloading programs from the RMRS computer in Boulder, followed by the <ENTER> key.

   The display returns to the "STORE WHAT?" message.

6. **Store the Application name in location 993.** Key in 993 followed by <ENTER> to get the display:

   993=

7. Key in the application name, ISC-31, followed by <ENTER>.

   The display returns to the "STORE WHAT?" message.

8. Enter the download phone number in location 994. Key in 994 followed by <ENTER>.

9. Then key in the download phone number, 18007573583, followed by <ENTER>.

   The display returns to the "STORE WHAT?" message.

10. Perform the download. Press the <CLEAR> key and the terminal display should return to:

    FUNCTION?

11. Press "0" and the display changes to two alternating messages:

    FULL OR PARTIAL?
    1=FULL 2=PARTIAL

12. Press 1 to choose a full download and then wait.

    The terminal displays the download phone number as entered in step 5. This is for your information only.

NOTE

DO NOT press any key at this point unless there is a problem. The download proceeds normally, requiring several minutes to complete.

13. Start up the terminal.

14. After the terminal displays a message indicates that the download is complete, press the <CLEAR> key several times until the terminal returns to the normal idle display with several digits, the word "BUSY" and four more digits. Wait a couple of minutes until the right hand digits in the display settle down with a value of 1790 to 1810.

15. Set up the transaction phone number. For the ISC-31 program, use any of the TRANZ 340's attached to the 1200C to set up to telephone number for performing transactions.

Follow the procedure given in next Section for changing the MSS phone number on the TRANZ 340.

Downloading TRANZiT 1200C & Tranz 340 Terminals

NCN has the following programs to download into the 1200C/340 LAN system.

- SP12789 – for 1200C
- SP34789 Program – for 340 terminals

NOTE
These programs are for use only over telephone lines.

To download:

1. Enter system mode:

   <CLEAR> 1 6 6 8 3 1 <ENTER>

   After pressing <ENTER>, it should display **SYSTEM MODE.**

2. Enter function mode by pressing <ENTER>.

   The display changes to **FUNCTION**?

   Store the download ID in location 992 by pressing key "8".

   The display changes to **STORE WHAT?**

3. Key in:

   9 9 2 <ENTER>

   It displays 992 =

4. Key in your 9-digit download ID (?????????) and <ENTER>.

   The display reads **STORE WHAT?**

5. Store the application name (SP12789) in location 993.

6. Store the download phone number (18007573583) in location 994.

7. Perform the full download. Press <CLEAR>.

   The display reads **FUNCTION?**

8. Press key "0".

   Alternating messages appear:

FULL OR PARTIAL?

1=FULL 2=PARTIAL

9. Press key “1” to choose a full download and then wait for download to complete.

10. Press <CLEAR> enough times to see the alternating display of LAN connection status.:

Table 10-12. MemoRy Location Notes – 1200C Program for SP12789

Location	Description
991	Sets Display for the 1200C
4	Shows the “-“and “*” symbols for each lane
3	Displays numbers rather than lane connections
992	Download ID/Serial Number
993	Name of Program to Download (SP12789)
994	Phone Number for Downloading Program: 18007573583
971	# of lanes/(Tranz 340s) the 1200C will poll. The fewer lanes it polls the faster the transactions as the 1200C doesn’t have to do as much work.
987	Verification phone # for transactions. Can use D(phone#),0 like
987	D18001231234,0 when comm has problems.
970	Baud Rate (1-5). Must match what is in location 21 on Tranz 340s. 1 is the slowest, 5 is the highest baud rate. This is the speed between the 1200C and the Tranz 340s

Tranz 340: SP34789

1. Store the lane number in location 20.

2. Store the download ID (?????????) in location 1.

3. Store the application name (SP34789) in location 19.

4. Perform a full download for a single terminal.

Table 10-13.

Notes:-Pre-dial (early dial function):	
Location 923	1 (early dial) = <empty> (no pre-dial) This only affects the program on key #7. The 1200C begins dialing after the check is read by the check reader. There is no pre-dial on the MICR W/ID or the PAYROLL (key#8 or 9).
Location 703	default state for DL
Location 903 =	ID type (C,D[driver’s license],M,P,S)

Table 10-13.

Notes:-Pre-dial (early dial function):	
Location 704, 804, and 904	terminal ID
Location 712	for sale amount
Baud Rate:	Baud rate value is from 1-4 whereas 1 is the slowest and 4 is the highest(default).
1200C location 970	4
Tranz 340 location 21	4

NCN
NATIONAL CHECK NETWORK

Section
11

Lipman - Nurit Terminals

In this section...

11 - Nurit Terminals

Nurit has programmed an application for the RMRS format. You can choose a number of options including attaching a check reader. There is a **Download Form** that you can fill out and fax to Nurit and they configure the check service and download the merchant for you.

The Nurit Terminals are made by a company called ***Lipman USA.*** Their phone number is 800-454-7626. Nurit has the following models: 2050, 2060, 2070, 2080, 2080+, 2085, 2090, 3000

Table 11-1. Nurit Terminals

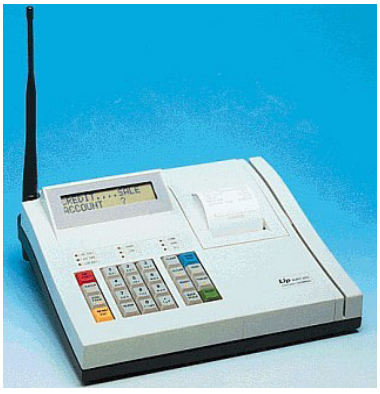
Name	Picture
Nurit 2070	

Table 11-1. Nurit Terminals (Cont.)

Name	Picture
Nurit 2085 & 2090	 
Nurit 3000	

NURIT DOWNLOAD FORM

For Downloading NCN Check Verification Application

Name of your Company:_____

Your Name:_____ Phone:_____ Date:_____

Type of NURIT: 2050 2060 2070 2080 2080+ 2085 Nurit PC

MANAGER CARD#:_____SERIAL#:_____

* * *MERCHANT INFORMATION* * *

NAME OF MERCHANT:_____

ADDRESS:_____

CITY/STATE/ZIP: _____

TELEPHONE #:_____

* * *HOST INFORMATION* * *

ATTACH PRINTOUT FROM THE TERMINAL:

To print out the Host information from the terminal:

Press the <MENU> key

Press 43

Host report will printout.

ROCKY MOUNTAIN PARAMETERS FOR CHECK VERIFICATION

Phone # for Terminal to Dial:_____

Terminal ID: ___ ___ ___ - ___ ___ ___ ___ ___ ___ - ___ ___ ___ ___

(Site #) (Merchant location #)(Rule set #)

Example: 100-000050-0008 (must include leading zeros)

Enable the Following Features: (check the ones to be enabled)

MICR:_____ State Code:_____SS#:_____

(enter State code)

Payroll or

DL:_____ Check #:_____Personal Check

(circle one)

ALL INFORMATION MUST BE COMPLETED TO HAVE THIS PROCESSED

RETURN FAX# 516-484-7093

Phone#: 800-454-7626

Check Reader Settings for the Nurit Terminals

The Setting for the Magtek check reader to be used with the Nurit terminal is:

- Comm mode 1
- Format 0002
- Baud 1200
- Parity, even

(same as setting for the Tranz 330)

The standard settings for any check reader to be used with the Nurit terminal is:

- 1200 baud
- 7,1,even parity
- raw MICR with TOAD substitution
- ending in <CR> or <CR><LF> (That's carriage return or carriage return and line feed, either works.)

These are the same settings used for any checkreader being attached to a Tranz 330 Terminal using NCN programs.

Nurit Check Verification download instructions.

The following sections are technician notes from Lipman USA regarding specifications and downloading of the NURIT series terminals.

NCN - GENERIC Check Protocol, using NCN system on an Lipman/Nurit Terminal - Technician Notes

Minimum application version = 04.64

Supported Checkreaders

The following checkreaders are supported with the NCN Generic Check Protocol.

Table 11-2. Supported Checkreaders

Check Readers (RAW format)
MAGTEK format 0001
Welch Allyn format 00
SORICON format 25
RDM Check Readers

Entering Terminal Identification data including rulesets

Based on the Terminal ID requirements of the NCN national database the following information should be programmed in each terminal prior to performing a verification:

Terminal ID structure (include the dashes):

Table 11-3. Terminal ID/Ruleset Entry

xxx-yyyyyy-zzzz{-aaaaaaa}	
xxx	Host number
yyyyyy	Merchant number
zzzz	RuleSet number (from 1 to 9999)
aaaaaa	Optional Affinity Group (Mandatory in credit card transactions)

NOTE
Ignore the Affinity Group if not performing credit card transactions

Terminal operational reference instructions:

* Customer must close the batch (and transmit "SUMMARY" transaction)

* Some RDM Check readers do not have a built in modem and will not be able to load images to the FTP server. These check readers can be identified by the serial number (and lack of telephone jack?).

* There are two Merchant_ID's - one for verification and one for truncation.

* To get 2nd copy with disclaimer: Esc, 3, 6, 2

Using Drivers Licenses

Magnetic Driver License can be swiped in the Nurit Terminal when the terminal is asking for DL ID, following by the prompt for state code. The default two-letters state code is interpreted from the DL track2 If the program could not recognize the state, it displays the default state from the merchant parameters.

Table 11-4. States using/considering the Mag DL: (as of 2/2002)

State Names					
Arizona	Colorado	Louisiana	Missouri	Newfoundland	Pennsylvania
Arkansas	Florida	Maryland	Montana	Nova Scotia	South Carolina
British Columbia	Iowa	Massachusetts	New Brunswick	Ohio	Texas
California	Kansas	Michigan	New Mexico	Ontario	Wisconsin

Driver's License State Codes:

(Use either numeric or alphabetic code)

Table 11-5. Driver's License State Codes

State and Code		
01 - AL	26 - MI	49 - UT
02 - AK	27 - MN	50 - VT
04 - AZ	28 - MS	51 - VA
05 - AR	29 - MO	53 - WA
06 - CA	30 - MT	54 - WV
08 - CO	31 - NE	55 - WI
09 - CT	32 - NV	56 - WY
10 - DE	33 - NH	72 - PR
11 - DC	34 - NJ	81 - AB
12 - FL	35 - NM	82 - BC
13 - GA	36 - NY	83 - MB
15 - HI	37 - NC	84 - NB
16 - ID	38 - ND	85 - NF
17 - IL	39 - OH	86 - NS
18 - IN	40 - OK	87 - NT
19 - IA	41 - OR	88 - ON

Table 11-5. Driver's License State Codes

State and Code		
20 - KS	42 - PA	89 - PE
21 - KY	44 - RI	90 - PQ
22 - LA	45 - SC	91 - SK
23 - ME	46 - SD	92 - YT
24 - MD	47 - TN	
25 - MA	48 - TX	

Merchant Parameters:

The following fields found within the terminal programming are described below.(When using multiple parameters fields, the letters can be in any order and can be separated by any number of spaces).

Table 11-6. Merchant Parameters

Parameter	Description
Merch_ID_Ver	Merchant ID for Verification transactions (Max size=24)
Merch_ID_Cnv	Merchant ID for Conversion transactions (Max size= 24)
Manual_MICR	Enables Manual entry of MICR. Put 'Y' to enable. Any other value blocks the keyboard for MICR entry. You can use the check reader (or RDM) regardless of this field's settings. The field is protected and can be set from TCC only.
Default_State	Default state when Driver License is entered manually.
Disable_Trns	Disable transactions (keys). Put a letter to DISABLE! V = Verification (VERIFY Key) C = Conversion (no key - default trans) D = Void (VOID key) I = ID Check (FORCED key)

Table 11-6. Merchant Parameters (Cont.)

Parameter	Description
Add_Prompts	Additional prompts: D = Driver License (Most common) S = Social Security C = Courtesy Card B = Cash Back A = ACH card as check R = Retype MICR **NOTE** When verifying a Paycheck, at least one ID letters must be specified: D/S/C. Anyway, only one ID is transmitted Example: "D B" (Prompt for D.L. and enable Cash Back)
Print_Opt	Control the printout of the following fields. Each letter is representing one field. Some fields are followed by a number (x=1-5) that defines the number of characters to reveal from the right side of that field. Example: D4 prints the Driver License as: ****4321 Dx = Driver License Sx = Social Security Cx = Courtesy Card Mx = MICR info.(if RDM is used, it is already defined as M4) H = Host detailed Messages **NOTE** If the letter 'H' is omitted, only the first message line is printed. Example of standard settings: "H D4 M5" (Print all Host messages, the DL (****4321) and the MICR (****12345).
Req_ID_Vrf	Specify the minimum amount for which the terminal prompts for IDs. The ID prompts are specified in "Add_Prompts". Field can accept only whole dollars, up to 8 digits. Example: The value "5000" causes the terminal to prompt for ID in any verification transaction of $5,000.00 or more.
Req_ID_Cnv	Same as above but for conversion transactions. Example: Enter "1" in the field to prompt for ID on transactions of $1.00 and up. Put "1" in "Min_Amount" field to make sure no transaction can be processed without ID.

Table 11-6. Merchant Parameters (Cont.)

Parameter	Description
Min_Amount	Specify the minimum amount that can be entered. Sale Amount (when using "Cash Back") is not subject to this rule. Field accepts only whole dollars, up to 8 digits.
Max_Amount	Specify the maximum amount that can be used. Field accepts only whole dollars, up to 8 digits.
Confirm_Amt	Amounts that exceed this field; causes the terminal to prompt for confirmation. The operator must reenter the exact amount in order to continue the process. Field can accept only whole dollars, up to 8 digits.
VOID_PSWD	When using this option, the terminal asks for the "DDMM" password, anytime when doing a VOID transaction. Put 'Y' to enable this option. (DDMM stands for current date. DD=day, MM=month).
MNGR_PSWD	When the host is responding to a conversion transaction with "MANAGER NEEDED" and this option is set to "Y", the terminal asks for the "DDMM" password. Put 'Y' to enable this option. (DDMM stands for current date. DD=day, MM=month).

Known Errors

Error in ID: Caused by the State Code not matching the structure of the driver license.

Example:

"NY" state-code requires a 9 digit DL ID#, whereas a

"TX" state-code requires an 8 digit DL ID#.

Anything more or less will generate this error message.

Mobile (Cell phone) Transactions

Can I use a cell phone to conduct transactions?

This is a question that many people have asked. Applications for this would include merchant's that do not have access to a phone line such as at trade shows or a delivery type business. There is a solution that the merchant can obtain from his cell phone company.

Get a cell phone with an RJ11 jack ..... whether built into the phone or an adapter.

When they go to the Cell phone company, tell them to say they are plugging in a FAX MACHINE.

DO NOT tell them it is a terminal. The Cell phone company gets confused or tries to sell the customer something they do not need. Anything that allows a FAX machine to communicate works with any terminal.

NCN
NATIONAL CHECK NETWORK

Section
12

Hypercom Terminals

In this section...

12 - Hypercom Equipment

Three models are available from Hypercom, the T7, T7E, and the T7P. The following pictures show the Hypercom terminals.

T7P Terminal

T7E Terminal

The T7P has a built in printer. Both the T7E and T7P have no RS-232 port to plug in a check reader. An additional piece of hardware (called the FIP 11) can be purchased for the T7P that allows a check reader to be plugged in.

Currently, RMRS does not have any specially developed programs for the Hypercom Terminal. We use an existing Telecredit format that many machines are already set up to handle. RMRS has certified directly with Hypercom under the name Rocky Mountain Retail Systems but our certification was done using the existing Telecredit format. Whether the processor recognizes the RMRS name or the Telecredit name does not matter. Either way, in most situations you must rely on the processor to set the merchant's terminal with the proper settings.

The terminal can be set up for RMRS if the credit card processor is using one of the following:

- Standard Application Check Formats (Telecredit is one of them)
- VisaNet application
- American Express application (see section on American Express 2200)

VisaNet Application:

If the **VisaNet** application is being used, you have the instructions to setup the check service on the terminal yourself. You may need the processor to open the terminal up for reconfiguring the check program. If the other two applications are being used you have to fax over the information to the processor and let them make the changes to the terminal.

American Express 2200 Application:

The American Express 2200 Terminal is just the name that American Express has given to the **Hypercom T7P** terminal they sell that is loaded with their software. Like any other Hypercom terminal, we are certified with American Express using the old Telecredit format with either ID only (Driver's License) or MICR only. For more information see the section in this manual entitled ***American Express 2200 Application***.

Hypercom Telecredit Format Limitations:

Unfortunately, the Telecredit format has some limitations. It only handles two types of transactions:

- DL only verification
- MICR only verification

The Telecredit format does not handle a combination of both DL and MICR. Other limitations include:

- On DL transactions, the State Code **40** for Oklahoma does not work. The clerk must enter the letters **OK** as the State code for Oklahoma. The number 40 conflicts with a code used for another reason by the Hypercom.
- Will not print a receipt on Declines
- Some terminal applications do not handle a checkreader
- No payroll check capability
- No cash back capability
- Two line display that eliminates many of the detailed messages on warning type transactions
- Does not support mag-strip reading of Driver's Licenses

NOTE

If the merchant is interested in using a checkreader, it is worthwhile to use the IVI CheckManager 3000 terminal and get away from many of the Hypercom limitations.

Hypercom Terminal Setup Information for VisaNet Applications

The following instructions are for setting up VisaNet/Hypercom terminals that support the **Check Select** function. This must be version T7RR07R or higher.

Table 12-1. Instruction Set for Hypercom Terminal with Visaset

Enter the Following	Terminal Displays.
At the terminal's Idle Prompt	SWIPE CUSTOMER CARD (or other custom idle prompt)
Press **FUNCTION, 3, 0, ENTER**	ENTER PASSWRD?
Press **0000, ENTER**	1 - PROGRAM CHK SERV 2 - DELETE AND EXIT
Press **1**	DIAL SERVICE DIRECT YES OR NO?
Press **ENTER** (YES) for Direct	1-JBS=12 2-CRITE=15 3-SCAN 4-TCHK 5-MORE
Press **5** for More	1 - TCRD 2 - ARJAY
Press **1** for Telecredit	1=12 2=13 3=14 4=19
Press **1** for 12 (MICR) or Press **2** for 13 (DL)	PRI. TELEPHONE NO. 00000000000000000000000000000000
Enter your verification phone number and press **ENTER** (any pre-dial code is already set up in Function 2 - do not add here)	SEC. TELEPHONE NO. 00000000000000000000000000000000
Enter your secondary verification phone number and press **ENTER**.	MODEM MODE 00
Enter **04** or **01** and press **ENTER**. (Mode 4=300 baud, Mode 1=1200 baud)	TIMEOUT SECS 00
Enter **30** and press **ENTER** (You may want to increase the timeout if using manual MICR, to prevent the transaction from canceling prematurely.)	TERMINAL ID. NUMBER 00000000000000000000000000000000
Enter your Merchant's site-locnumber-ruleset# with the **leading "V"** (shift 2 or Alpha 2 to make a V and press 2#### to get a "-" dash) (example: **V500-120-10**)	TRANSACTION COMPLETE

NOTE

The Terminal ID **must** start with a "**V**" and then continue with the merchant location code you want to use on the Velocity PLUS or NCN system, e.g. "V500-50-5".

If you use a check reader with the VisaNet Application you must also do the following:

1. Press **FUNCTION 97** and set the following options:
2. 0-none, 2-RS-232, 2-Pin/Check Reader PortChoose 2 for Pin/Check Reader Port
3. Pin Pad Type?Choose 1
4. Hand set Dial Allowed?Choose NO
5. Toll Dial Allowed?Choose NO
6. Memory Fast Dial?Choose YES
7. Referrel Dial Used?Choose NO

Check Reader Settings for the Hypercom Terminal

NOTE

To use a check reader with a Hypercom terminal, the following configurations must be used. FIP 11: An additional piece of hardware (called the FIP 11) can be purchased for the T7P that allows a check reader to be plugged into the Hypercom terminal.

Mag-Tek:

Figure 12-1. Mag-Tek Check Readers

Proper configuration for a **Mag-Tek** check reader when attached to a Hypercom:

- 9600 Baud
- Even Parity
- Commode 3(Data <CR><LF>)
- Format 0001 or Format 0002

Format 1 = lowercase “toad” substitution

Format 2 = uppercase “TOAD” substitution

IVI MR-2100, MR-2300

Figure 12-2. IVI MR-2100. MR-2300 Check Reader

Configuration for the IVI MR-2000 series of check readers:

- 9600 Baud
- (Data <CR><LF>)
- “TOAD” substitution format

CHECKMATE CMR431

Figure 12-3. CheckMate CMR431 Check Reader

Configuration for the IVI MR-2000 series of check readers:

- 9600 Baud
- (Data <CR><LF>)
- “TOAD” substitution format
- Use Configuration checks: SC00155

SORICON MR 1000:

Figure 12-4. SORICON MR 1000 Check Reader

Switch Configuration

Switch	1	2	3	4	5	6	7	8
Position	D	D	D	U	U	D	D	D

U = Up
D = Down

Hypercom Terminal Setup Information for Processor Setup

For use with the NCN Check Verification Systems

The following information should be supplied to the merchant's credit card processor.

This document explains how to set up the merchant's Hypercom terminals to use the Telecredit or RMRS format, which Hypercom refers to as Format 3. All users of the standard Hypercom code have it, but some processors have obtained custom code from Hypercom that may not include it. The processor should run the TNMS download program, supplied by Hypercom, with the following setup:

1. Edit Terminal, page 1 of TNMS screen:

   Check Service = 12 (MICR Number)

   Check Guarantee Service, Issuer Table Name = TELECREDIT

   Acquirer Table Name = TELECREDIT

2. Edit Terminal, page 2 of TNMS screen:

   Check Reader Installed = Y (Y or N)

3. Edit Terminal, page 3 of TNMS screen:

   Acquirer Name = TELECREDIT

4. Edit Acquirer, page 1 of TNMS screen:

Host Message Protocol = TELECREDIT

Transaction Modem Mode = 01 (1200 BAUD)

Visa Terminal ID = V<NCN Terminal ID # assigned by you>

Primary Telephone No. = <phone number for your Velocity PLUS or NCN>

Secondary Telephone No. = <alternate phone number of the system>

5. Edit Acquirer, page 2 of TNMS screen:

   Issuer Name = TELECREDIT

The Terminal ID **must** start with a "**V**" and then continue with the merchant location code you want to use on the NCN system, e.g. "V500-50-5".

Hypercom Terminal Operation for MICR Verification

Once the Hypercom terminal is downloaded, follow this procedure for running transactions:

1. Press the "CHECK" key on the Hypercom terminal (located just to the left of the "7" key).

   The terminal responds with the prompt:

   ENTER CHECK NUMBER

2. Key In the check sequence number as shown in the upper right corner of the check and then press the "ENTER" key.

NOTE
Unfortunately, this step is required even if you use a check reader that reads the number automatically. If the check does not have the check number in the MICR line, the system uses the manually entered number.

   The terminal responds with the prompt:

   ENTER CHECK ACCOUNT #

3. Feed the check into the reader or key in the MICR data manually. If keying data manually, you must include both the ABA routing number and the customer's checking account number with no spaces or punctuation. Press ENTER at the end of manual keying. Once the terminal has received the check account data, it immediately starts dialing.

   The terminal responds with the prompt:

   AMOUNT$0.00

4. Key in the amount of the check, omitting the decimal point. As you key digits, it replaces the “0.00” that initially appears in the display.

5. Press the “ENTER” key when finished.

   The terminal displays the sequence of messages shown below as it communicates;

   DIALING NOW

   PROCESSING NOW

   The terminal ends by beeping four times and displaying the response. If the check is approved, the first line of the display is the “Idle Prompt” used by Verifone terminals and the second line contains the approval code. If a warning or decline condition occurs, the first line contains “WRN” or “DEC”, followed by the first reason for the problem, and the second contains the second reason (if there is one) for the warning or decline.

Hypercom Terminal Operation for DL Verification

Once the Hypercom terminal is downloaded, follow this procedure for running transactions:

1. Press the “CHECK” key on the Hypercom terminal (located just to the left of the “7” key).

   The terminal responds with the prompt:

   ENTER CHECK NUMBER

2. Key In the check sequence number as shown in the upper right corner of the check and then press the “ENTER” key.

   The terminal responds with the prompt:

   DRIVER’S LIC. NUMBER

3. Key in the DL number and be sure to include any letters that are part of the DL number. (The Telecredit format does not support mag-strip DLs). Press ENTER at the end of manual keying.

   The terminal then responds with the prompt:

   STATE CODE

4. Key in the code the State the license was issued. You can enter a 2-digit number for the State or enter the two letter abbreviation for the State by holding down the <SHIFT> key and pressing the key with the letter you want. Press ENTER at the end of keying.

   The terminal responds with the prompt:

   BIRTHDATE - MMDDYY

5. Key in the date of birth from the Driver's License. The terminal requires you to enter 6 digits but since this piece of information is not sent to the verification system it doesn't matter whether it is entered correctly or not. Press ENTER.

   The terminal displays:

   AMOUNT$0.00

6. Key in the amount of the check, omitting the decimal point. As you key digits, it replaces the "0.00" that initially appears in the display. Press the "ENTER" key.

7. The terminal displays the sequence of messages shown below as it communicates

   DIALING NOW

   PROCESSING NOW

   The terminal ends by beeping four times and displaying the response. If the check is approved, the first line of the display is the "Idle Prompt" used by Verifone terminals and the second line contains the approval code. If a warning or decline condition occurs, the first line contains "WRN" or "DEC", followed by the first reason for the problem, and the second contains the second reason (if there is one) for the warning or decline.

American Express 2200 Terminal

The American Express 2200 Terminal is just the name that American Express has given to the **Hypercom T7P** terminal they sell that is loaded with their software. Like any other Hypercom terminal, we are certified with American Express using the old Telecredit format with either ID only (Driver's License) or MICR only. The program is the Standard Check Applications module and works the same as it is described in the ***Hypercom Terminals*** section of this manual.

When setting up a merchant you need to call the American Express Setup Department at 800-528-0682. You need the following information so they can setup the merchant with check verification.

- The American Express Merchant number for this merchant.
- RMRS can be listed with American Express. If not, just have them set the terminal up for the Telecredit check format.
- Primary Telephone Number for the terminal to dial for verification.
- Secondary Telephone Number for the terminal to dial for verification. (If you do not have a secondary number, you can use the same number as the Primary number.)
- Terminal ID number (sometimes referred to as the Visa Terminal ID). This Terminal ID number must start with the letter 'V'. (For example: V100-156-10)
- Check Reader Installed (Yes or No): If the answer to this is no, then you are setting up the terminal for ID only (Driver's License) verification.

- in order to have them set the terminal up for you. You need to supply the usual information (phone number to dial, the merchant # you need put in, i.e. V400-134-10, etc.)

Hypercom Certifications via NCN

The following information refers to the various Hypercom programs certified with the National Check Network.

The following certifications have been completed as of July 30th, 2002 with Hypercom from NCN:

!SPOSi

Application Name: !SPOSi

Application Version#: 06A

Terminal make &Model: Application can be use on ICE 5500+

Veification, ACH and Payroll Transactions

Verification Date: June 10th, 2002

SPOS7

Application Name: SPOS7

Application Version #: 06A

Terminal make and model: T7+ Series

Verification, ACH and Payroll Transactions

Verification Date: June 6th, 2002

VHDT

Application Name: VHDT

Application Version #: 8.1

Terminal Make and Model: ICE5500

Verification, ACH and Payroll Transactions

Verification Date: May 7th, 2002

Certified Processors using Hypercom software

Listed below are the names of the processors who have Class 'B' certified the SPOS 06A software.

AMEX
Cross-Check
Global
Nationwide Check
Nova
Paymentech
Vital

NCN
NATIONAL CHECK NETWORK

Section
13

Dassault Terminals

In this section...

- Models
- Linkpoint Terminals
- Zontalk parameters for RMRS check service:

13 - Dassault AT Terminals

Dassault AT has completed an extensive applications that is like the MFxPNTR program on the Verifone Tranz 330 terminals. You need to call Dassault AT to have the check application that works with RMRS downloaded to the merchant's terminal.

Models

The models offered by Dassault are the Freesia and the Talento.

Customer Service: 1-888-710-0100

Figure 13-1. Feesia

Figure 13-2. Talento

Linkpoint Terminals

RMRS is supported on LinkPoint 2000 terminal applications LFRET5 (for retail) and LFRST3 (for restaurants) and higher releases. The LinkPoint 3000 terminal applications L3FRET1 (for retail) and L3FRST1 (for restaurants) and higher releases. The function is supported for both manual entry and check reader (Mag-Tek Mini Micr).

Check readers: The Magteck Mini MICR reader is the only check reader that has been certified with the LinkPoint terminal. The Mag-Tek Mini MICR check reader must be configured to format (0002) with the following special settings.

Table 13-1. LinkPoint Terminal Settings

Item	Setting
Format	0002
MICR Type (Options)	RS232 (Fullset)
Comm mode	none
Baud Rate	9600
Data Bits	8
Stop bits	1
Parity	none
Invalid Command Response?	<CR>/No Header
Check the following Options to yes:	
Trailing <CR>	yes
Send Status	yes

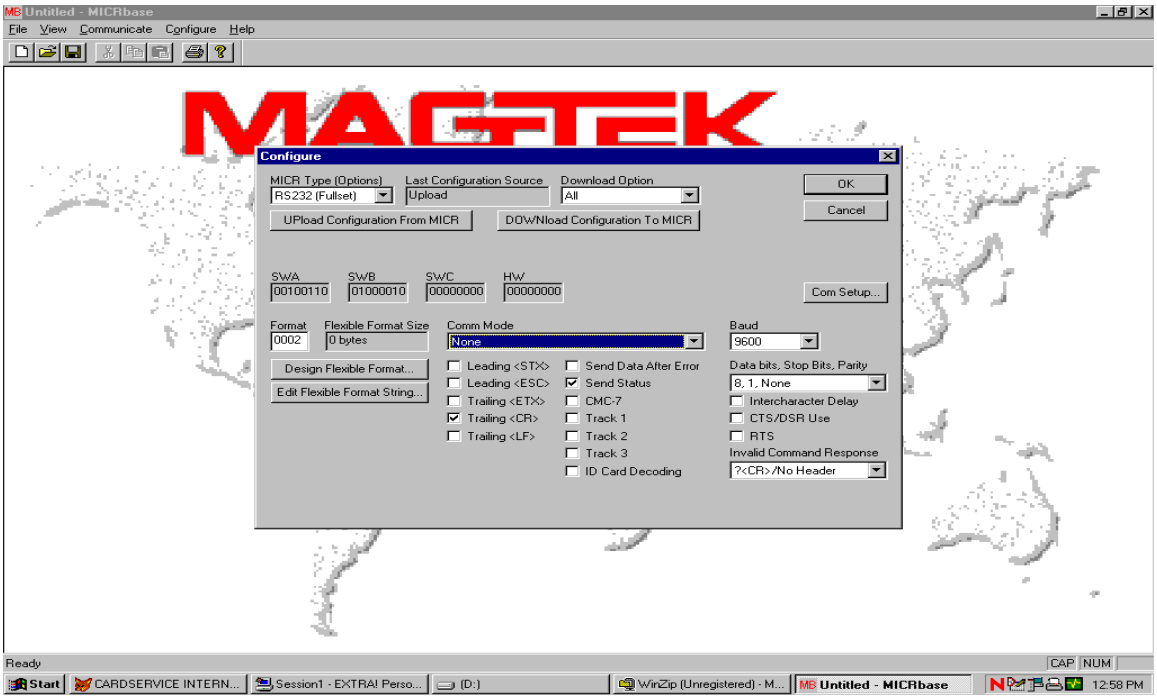


Figure 13-3.

When setting up a LinkPoint terminal for the RMRS check service, the merchant's credit card processor/ISO must have that merchant's terminal downloaded with the following parameters/options to enable the check service.

Zontalk parameters for RMRS check service:

Table 13-2. Zonetalk Parameters for RMRS Check Service

Variable	Type	chrs	Explanation	Data
#CKMID	X	17	Check Guarantee Merchant ID	Xxxxx-xxxxxx-xxxx
#CKPNP	P	20	Check Guarantee Primary Phone Number	x-xxx-xxx-xxxx
#CKPNS	P	20	Check Guarantee Secondary Phone Number	x-xxx-xxx-xxxx
#CKSVC	N	1	Check Service: 3=RMRS	3
#RMMAP	N	1	PROMPTS 1=MICR 2= MICR-ID 3=ID ONLY	2

#CKMID. The Merchant ID must contain three numbers separated by dashes. The format is always (Site# - Merch# - Rule Set #), for example 100-153-12. The dashes are required.

#CKSVC. The number 3 is the proper number for RMRS check setup.

#RMMAP. You can set up the program to only offer 1 of the 3 methods of verification (1=MICR, 2=MICR+ID, 3=ID ONLY). However, if you set the terminal to option 2=MICR+ID, you can skip the ID portion and the terminal does a MICR only transaction. If you get an ID IS NEEDED back, you then enter everything. This allows for the one-time ID viewing option or other situations where you only enter an ID when the rule set requires it.

NOTES

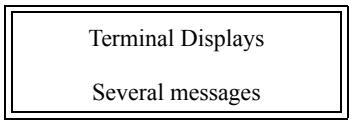
– This program prints a receipt on everything, not just the declines.

– This program handles either hand keyed MICR or data from a Mag-Tek Mini-MICR check reader.

– This program handles hand-keyed Driver's license or electronically swiped DL when available.

RMRS Check Service Manual Entry Option 1

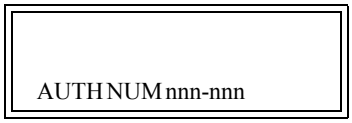
Display Message	Operator Action
READY XXX JAN-04-99 MON 12:00P [s] [s] [s]	Press [Check] key.
CHECK RMRS SLIDE CK OR KEY MICR [s] [s] [s]	Key in the micr number
ENTER MICR NUMBER [s] [s] [s]	Press [ENTER] once micr number is entered
ENTER CHECK # [s] [s] [s]	Key in the check number and press [ENTER]
AMOUNT OF SALE? $0.00 [s] [s] [s]	Key in the sale amount and press [ENTER]



The terminal will dial into the host and send

A response back to the terminal

[s] [s] [s]



If the transaction is approved you will receive

An approval

[s] [s] [s]

If the transaction is declined or there is an

Error a receipt will print and you will be able

To press the [#] key to view

[s] [s] [s]

NCN
NATIONAL CHECK NETWORK

Section
14

Support Server

In this section

- Log In
- Using the Support Server
- Support Server Menu items

14 - Support Server

This User Guide is intended to guide the Direct Agency user through the new NCN Support Server for ***ECHO*** Check programs. The NCN Support Server enables Direct Agency users to (a) find check verification transactions in order to answer questions from customers whose checks have been declined, and (b) search transaction logs and view the POS Response to the check's presentment, thus enabling them to provide customers with more complete details for the check rejection.

Log In

To log into the NCN Support Server, click on this website address:

www.check.net

Once the website is accessed, the Welcome screen appears.

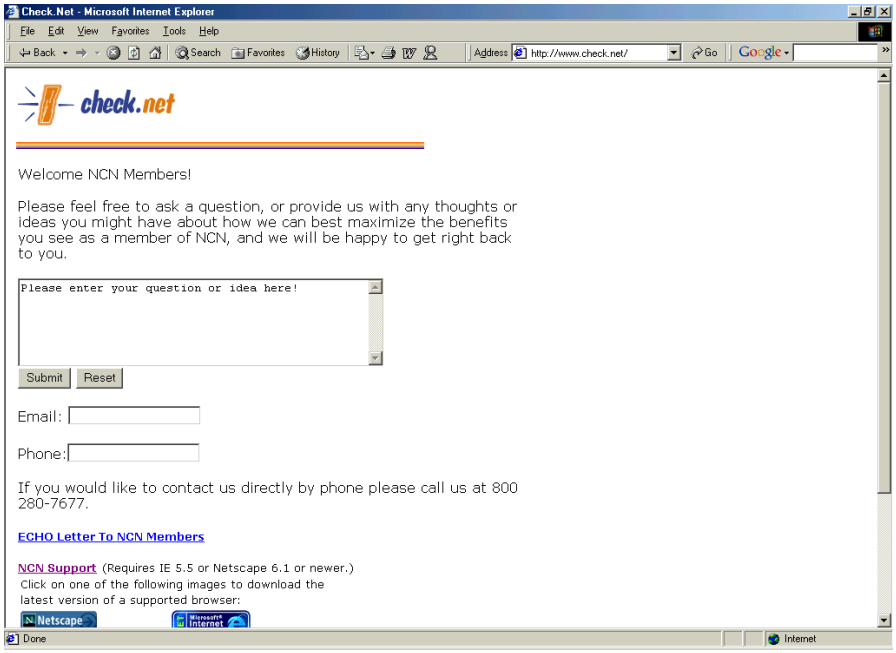


Figure 14-1. Welcome Window

To log in to the System:

1. Click on **NCN Support** in the lower left corner of the screen to open the log in screen.

2. Enter the following information:

   Username: – assigned by your Agency Administrator;

   Password: – initially assigned by your Agency Administrator;

   Log on to: – the name of your agency assigned by NCN

3. Click the Login button

Agency Home Screen

Upon entering the login information correctly the following screen displays on the Agency Home Screen:

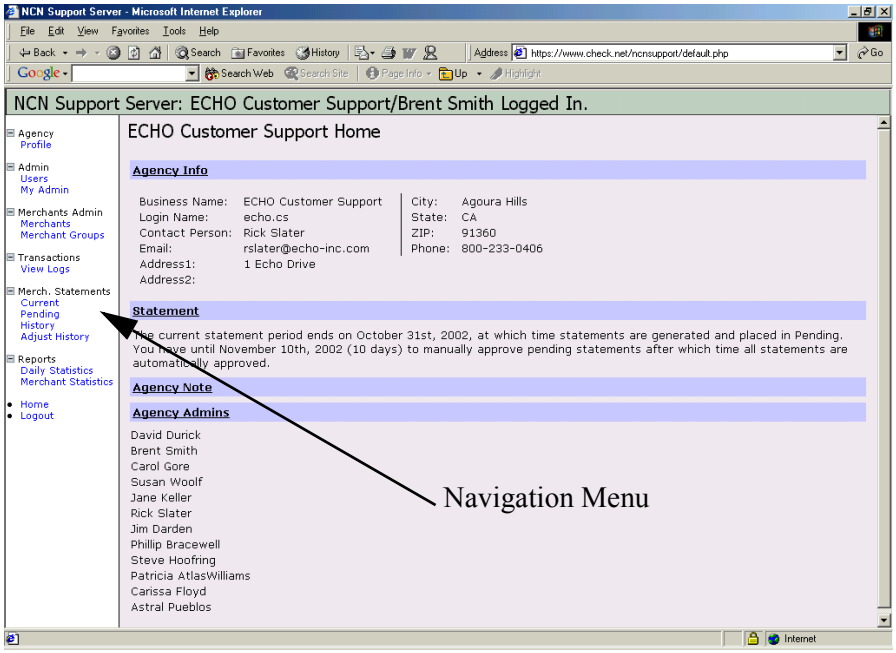


Figure 14-2. NCN Support Server: Agency Home Screen

NOTE

Due to constant enhancements to the support server, may be items that are not listed in the graphics, or text, of this document.

Support Server Menu items

The left side of the screen, or Navigation Menu, shows the selections of the support server. The five main menus available are:

- Agency
- Admin
- Merchants Admin
- Transactions
- Merch. Statements
- Reports
- System Management

Each of the five menus has a dropdown list available submenus. Each submenu is highlighted in blue. Clicking on any blue-highlighted submenu changes the text on the right side of the screen. The following sections guide you, step-by-step, through each menu and its submenus.

Agency Menu

Profile

The Profile submenu allow the Agency Administrators, and/or users with special permissions, to change general agency parameters. The following options can be changed:

Agency Info:

This information lists the company's general information which is printed on each statement produced for your customers.

Statement:

The setting adjusts the current statement period at which statements are generated and placed in the **Pending** folder. The default setting is the last day of the current month.

Agency Note:

This is a note area for use to place any type of notes for your agency's use.

Agency Sites:

This setting is setup by NCN to reflect your agency's site number(s). This cannot be edited by your agency.

Fee Profiles

Fee profiles are "templates" designed for attaching fees to each merchant, and applying them to every transaction generated from that merchant into the verification system. The result of using these fee profiles are reflected as charges on each merchant statement produced at the end of a billing cycle. Once profiles are created, agencies will be able to easily choose, or modify templates, when setting up a new merchant or customer. There are two types of fee profiles managed with the NCN Support Server:

Standard Fee

Standard Fee profiles apply to all non-guarantee transactions, or transactions not meeting guarantee qualification criteria. Options exist for supporting both paper and ECC (Electronic Check Conversion), or limiting the scope of the profile to just one, or the other. Additional options establishing a rate structure, and allowing or preventing modification of the fee profile after assignment to a merchant.

Guarantee Fee

Guarantee Fee profiles are intended to support paper or ECC check guarantee programs. Options exist for excluding checks over a specified dollar amount, including or excluding special case transactions, establishing a rate structure, and allowing or preventing modification of the fee profile after assignment to a merchant.

Viewing Standard Fee Profiles

With every new NCN agency there are two default Standard Fee Profiles created and applied, Transaction Based Fee Profile and Volume Based Fee Profile.

Upon logging into the NCN support server, select **Fee Profile** underneath the Agency Submenu on the left side of the screen.

The four columns underneath the Standard Fee (and Guarantee Fee) areas, are subitems which reflect a summary of each Fee Profile setup within the system:

- Fee Profile - This is a summary of the type of profile used, the name of the profile used in the statement
- Used - Reflects how many merchants are currently assigned this particular fee profile (this is a hypertext link to list those merchants)
- Qualification for Criteria - Are the minimum requirements which "triggers" this Fee Profile to be used. This setting can only be changed for guarantee fee profiles.
- Standard Processing Fees - Reflects the transaction rate, which is attached during a new merchant setup process.

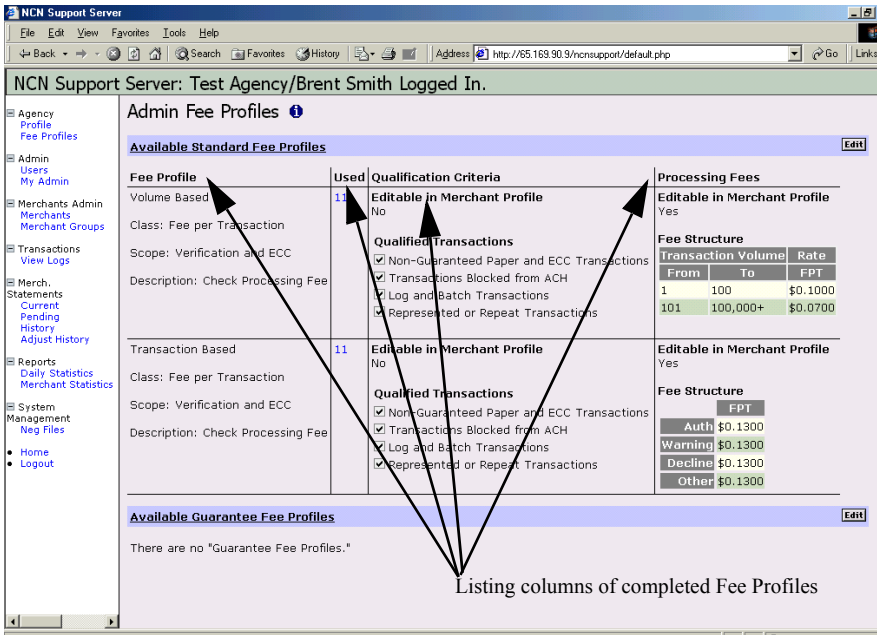


Figure 14-3. Completed Fee Profiles which are available to use

Editing Fee Profiles

Select the Edit button at the right side of the type of fee profile which is chosen to edit

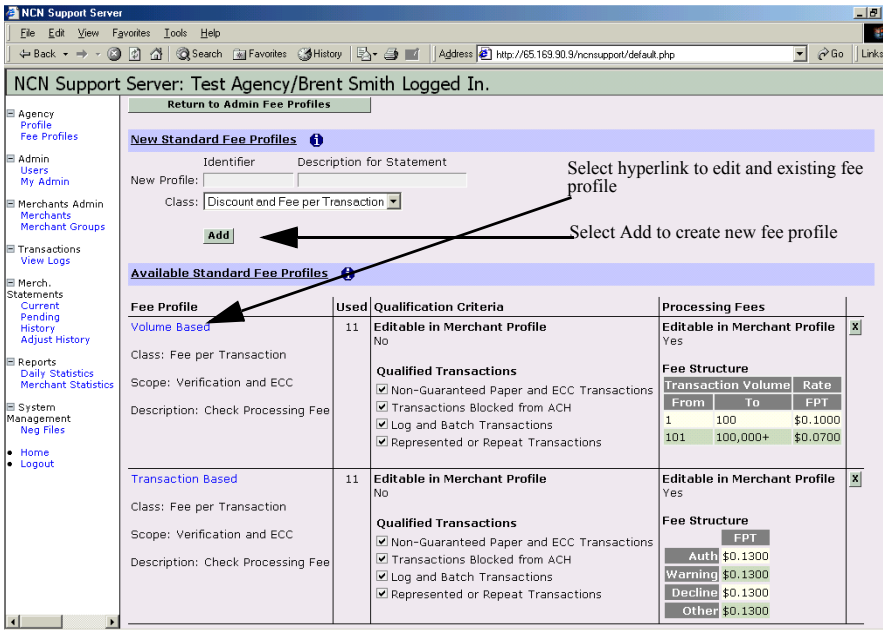


Figure 14-4. Editing or Creating New Fee Profiles

Standard Fee Profiles

There are two default types of Fee Profiles available with each new merchant setup, Volume Based and Transaction based profiles.

Guarantee Fee Profiles

Guarantee Fee profiles are intended to support paper or ECC check guarantee programs. Various setup options include:

Excluding checks over a specified dollar amount

Including or excluding special case transactions

Establishing a rate structure

Allowing or preventing modification of the fee profile after assignment to a merchant.

General Fee Profile Setup

Creating a Standard Fee Profile

1. Login to the NCN Support Server
2. Underneath Agency select the submenu item **Fee Profiles**. A new screen will appear.
3. Select the **Edit** button on the right side of the Available Standard Fee Profiles. A new screen will appear.
4. Place the name, and a description of the fee profile, in the Identifier and Description of statement fields.

NOTE
The Description of Statement will appear on your customer statement.

5. Select the Class from the dropdown menu. Click the **Add** button. A new screen will appear.
6. Underneath the profile menu - select which "Scope of Coverage" is preferred - which kinds of transactions will be billed. Fill in the comment section, and select the **Update** Button.

Qualification Criteria Setup

NOTE
The next section "Qualification Criteria" cannot be edited using fee profiles unless a guarantee profile is being setup.

1. Underneath the “Processing Fees” section, select this checkbox if it is decided NOT to edit and assign this fee profile from the merchant profile screen.

2. Create a fee structure and range of fees (if applicable) by placing a maximum transaction amount and a Fee per Transaction (FPT) in the appropriate fields. When all options for the range are entered, select the **update** button. The chart will update with the fee structure created.

3. Select the **Return to Standard Fee Profile Management** button at the top of the page to return to the main Fee Profile screen. This fee profile is now ready to add to any or new merchant setup.

NOTE

When there is a need to edit this profile, select the blue hyperlink name of the fee profile to advance to a new screen to enter the changes necessary.

Creating a Guarantee Fee Profile

1. Underneath Agency and select the submenu item **Fee Profiles**. A new screen will appear.

2. Select the **Edit** button on the right side of the “Available Guarantee Fee Profiles”, and an new screen will appear.

3. Place the name and the description of the fee profile in the Identifier and Description of statement fields.

NOTE

The Description of Statement will appear on the customer statement.

4. Select the Class item from the dropdown menu. Select the **Add** button. A new screen will appear.

5. Underneath the “Profile” - select which Class of Coverage is preferred for transactions to be billed. Fill in the comment section and select the **Update** Button.

Qualification Criteria Protection

Underneath the “Qualification Criteria” area select the following:

1. Select this checkbox if its decided NOT to edit or add this fee profile from the merchant profile (setup) location.

2. Enter a “Maximum Check Amount”. This amount is described as the largest dollar amount to qualify for a guarantee transaction.

3. Qualified Transaction - Depending on what kind of profile class was selected, there are up to four options which can be selected or deselected.

NOTE
Some Qualified Transactions cannot be edited due to the type of profile selected.

4. Select the "Conditionally Qualified Transactions" checkboxes that will apply in which the fees will be applied. Typically most agencies will select all checkboxes when performing guarantee.

5. Select the **Update** button.

6. Underneath the "Processing Fees" area - Select this checkbox if its decided NOT to edit or add the this fee profile from the merchant profile (setup) location.

7. Create your fee structure, and range of fees, by placing a maximum transaction amount, discount rage, and a Fee per Transaction (FPT) in the appropriate fields. Once all options for the range are entered, press the **Update** button. The chart will update with the fee structure created.

8. Select the **Return to Standard Fee Profile Management** button at the top of the page to return to the main Fee Profile screen. The new Fee Profile is shown underneath the "Standard Fee Profile" section. This fee profile is ready to select when a new merchant is setup.

NOTE
When there is a need to edit this profile, select the blue hyperlink name of the Fee Profile. This advances you to a new screen to enter necessary changes.

Admin Menu

The Admin menu contains two submenus: **Users** and **My Admin**.

Users

The **Users** submenu allows the Agency Administrator (and any other users with permission) to set up authorized users to use the NCN Support Server. Click on **Users** to open a screen that contains a list of all authorized user names for the NCN Support Server, as shown below:

User Accounts Screen

NOTE

New Users can be added only by the Agency Systems Administrator, *or users who have permission to do so. (Permission is established in the initial client setup.)*

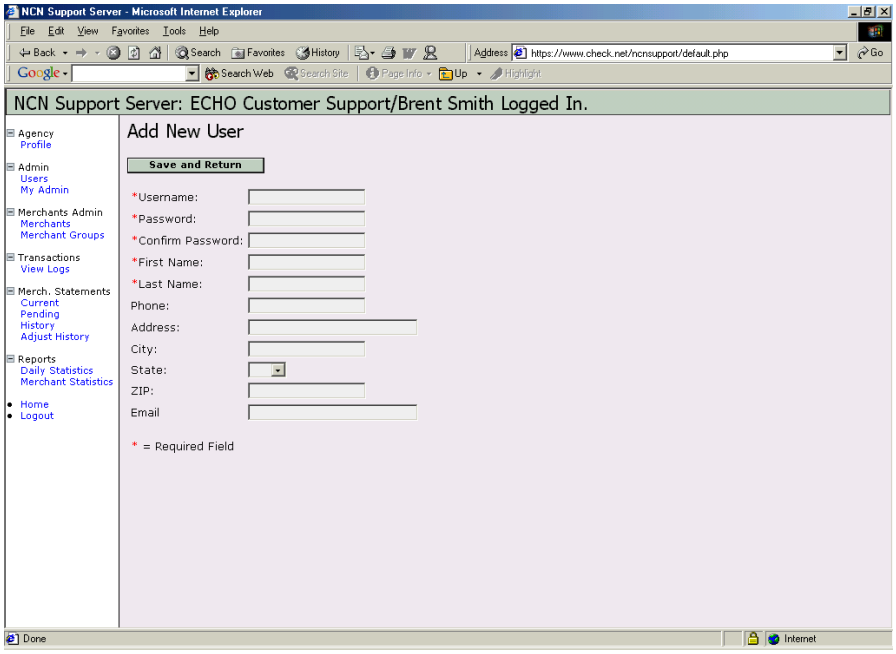


Figure 14-5. Add New User Screen

In order to add a new user, please follow these steps:

1. Under the "Admin" menu select **Users**.

2. Select the **Add New User** button at the top of the page

3. Fill in the following five fields: Username,Password,Confirm Password,First Name and Last Name. Entering information in the six remaining fields is optional, but highly recommended.

4. Select **Save and Return** button.

   This saves the information and refreshes the Add New User screen so that you can continue to add New Users. When you have finished, click on **Users** on the left side of the screen to display the updated "User Accounts" Screen.

My Admin

The **My Admin** submenu allows individual users to access and change their personal information. Click on **My Admin** to open the screen shown below:

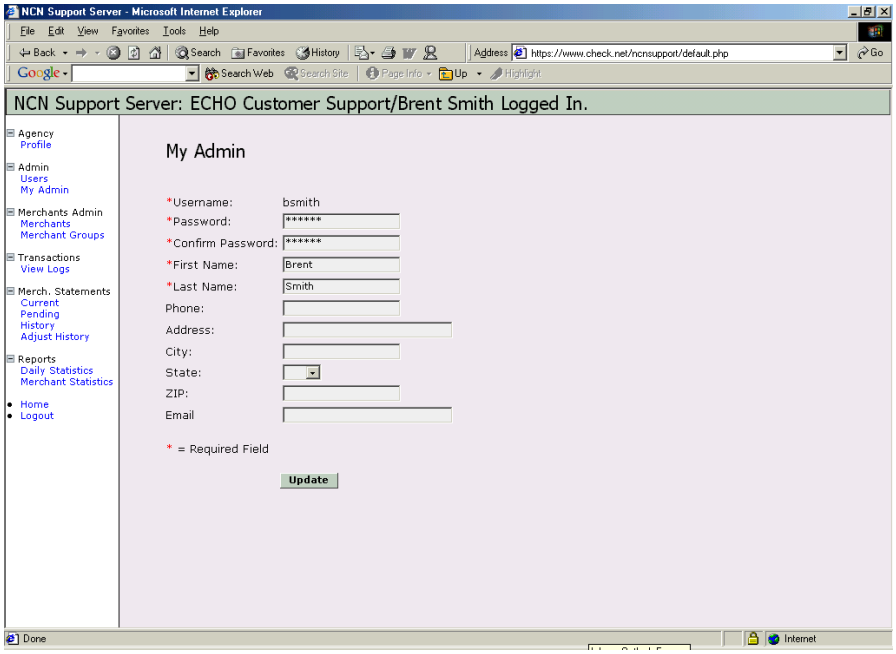


Figure 14-6. My Admin Screen

The first five fields of this screen require input, since this information enables you to log on to the Support Server. When you log on to the Support Server for the first time, your username, password, confirmed password, first and last name have been assigned by the Agency Administrator and are automatically entered into the required fields. Again, its recommended to have all fields filled in. This is for your benefit.

NOTE

Direct Agency users can change information in all of the fields except the Username field. If a Direct Agency user wishes to change his or her Username (e.g., adding a middle initial), this can only be performed by the Agency Administrator.

Changing your individual account preferences

1. Select the **My Admin** under the "Admin" menu item.

2. Change any information needed in the required or optional fields. The required fields include: Username, password, confirm password, first name and last name.

3. Once you have made changes to the information on this screen, Select the **Update** button and your computer screen refreshes itself

NOTE

The Password and Confirm Password field allows you to change your assigned password. To do this, type your new password in the password field, then retype it in next field to confirm it. (Your password can be a minimum of 5 characters, up to a maximum of 20 characters.)

NOTE

After pressing the update button - If changes are not accepted by the system for any reason, it will display error message in red print at the top, or bottom of the screen. reenter the login information again and click on If this second attempt is unsuccessful, contact your Agency Administrator.

Merchants Admin. Menu

NOTE

Though there are two default fee profiles already setup on the support server, make certain that the appropriate fee profiles are setup before setup of any new merchants. This will allow the selection of the desired fee profile during the new merchant setup procedure. See “General Fee Profile Setup” on page 14-7 to setup a fee profile.

The Merchants Admin menu contains two submenus: **Merchants** and **Merchant Groups**.

Merchants

The Merchants submenu contains a list of all merchants (whether “Unassigned” Merchants, or as part of a “Merchant Group”) signed up for NCN Check Programs. Click on the blue-highlighted Merchants to display the Merchant window.

NOTE

The Agency Administrator (and any other users with permission) can only set up authorized Merchant Users so that they can use the NCN Support Server.

Admin Merchants Screen

The Agency Systems Administrator (or other users with permission) can **Add New Merchants**.

To add a new merchant:

1. Click on **Merchants** under the Merchant Admin menu item to display Admin Merchants screen.

2. Select the **Add New Merchant** button

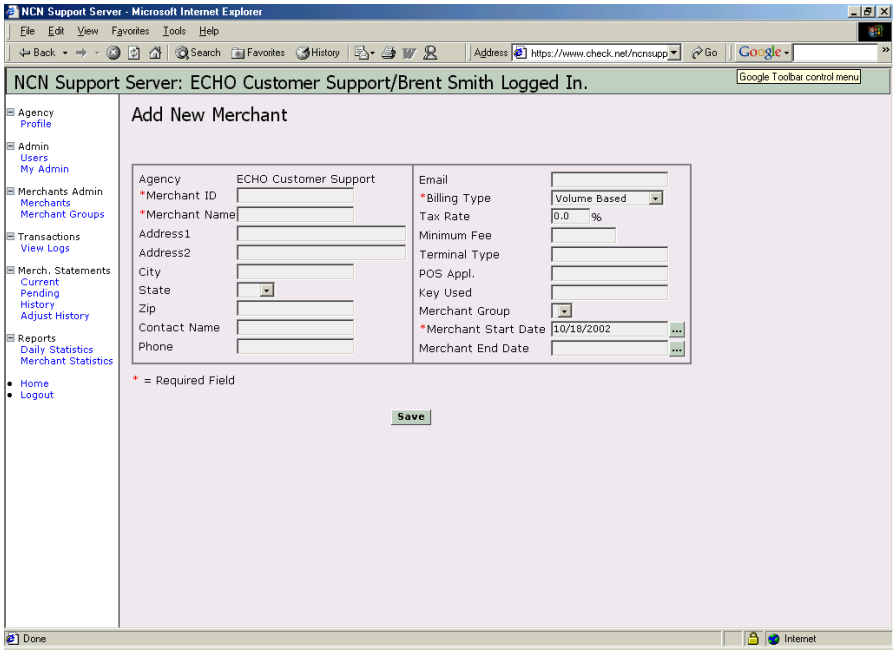


Figure 14-7. Add New Merchant screen

3. Add the information in each field to complete the merchant entry. See the information below these steps in descriptions of each field.

4. Once you have made changes to the information on this screen, Select the **Save and Return** button. Your computer screen refreshes itself. You are directed to the Merchant Profile screen.

Merchant Entry Field Description

Please refer to the following table on the next page for the description of each field within the “Add New Merchant” window. Four fields are required for a new merchant entry, however for your benefit, it is highly recommended that all fields are completed.

:

Table 14-1. Merchant Entry Field Descriptions

Field Value	Field Description
Required Fields	
Merchant ID	A **combination** of the **Agency ID** assigned internally by ***NCN*** and the **agency's own** internal assigned or created merchant number.
Merchant Name	Name of Individual Merchant (e.g., "Tony's Tamales").
Billing Type	Can be "Transaction Based" or "Volume Based" (which can be selected by placing the cursor on the down arrow to the right of "Transaction Based" and clicking on it to open the drop-down menu).
Merchant Start Date	Used to establish a start date of verification for the system to start logging information in producing statements.
Non Required Fields Many of these options appear on the final printout of merchant statements	
Address 1	Enter Address of Business (which appears on the statement)
Address 2	Additional Address Entry
City	Enter City of merchant
State	Enter State of merchant
Zip	Enter Zipcode of merchant
Contact Name	Main Contact Name at Merchant location
Phone	Telephone number to reach Contact at merchant location
Email	Email address of main contact person at merchant location
Tax Rate	Local service tax rate (if applicable)
Minimum Fee	Minimum fee, flat rate - for your merchant to use the service (i.e. $19.00 per month just to use the service with or without any verification volume)
Terminal Type	Point of Sale Terminal type at this location
POS Application	Terminal Application downloaded in the terminal, other info
Key Used	If a Verifone terminal - application key used on the terminal
Merchant Group	If this merchant needs assigned to a merchant group, and groups are setup, you can assign this merchant to a group here
Merchant End Date	Optional setting - can be used for a promotion or if merchant terminates services and you need to cancel statement calculation to not include this merchant.

Merchant Profile Screen

The merchant Profile Screen is accessible after the initial merchant is added to the system. This screen is accessible two ways - just after pressing "Save" when adding and creating a new merchant, or by selecting the Merchants sub menu item (under Merchants Admin) and then selecting the merchant you'd like to edit. The Merchant Profile screen provides a profile that contains four subsections that are required to generate statements. These subsections include:

- Merchant Info
- Assigned Site-Location-Rules
- Taxes
- Other Fees
- Guarantee Fee Profiles
- Standard Fee Profiles

NOTE
After the five subsections are completed, and saved, the merchant setup is completed.

To enter information under any of these subheadings you'll need to select the **Edit** button at the right hand side of the subheadings.

To create an Assigned Site-Location -Rules item:

1. Select the **Edit** button on the right side of the title "Assigned Site-Location -Rules"
2. A new screen pops up. Insert the Merchant Number (i.e. Location) and Ruleset Number (i.e. Rule) assigned to this merchant. (Optional - If you have multiple site numbers assigned to you from NCN, there is an option to select which site number you want to use it from drop down box.)
3. Select "**Add**"
4. Select the **Save and Return** button to save these entries and return to the Merchant Profile screen.

NOTE
Repeat the above steps for entering multiple locations, and/or rulesets.

Taxes

1. Select the **Edit** button on the right side of the title “Taxes”. A new screen appears.

2. Enter the percentage amount to charge in all of the fields labeled for local or state tax.

3. Once you have made changes to the information on this screen, Select the **Save and Return** button. Your computer screen refreshes itself. You are directed to the Merchant Profile screen.

NOTE

Once a tax rate is established, this rate may be selected included to any fee profiles. See “Editing Fee Profiles” on page 14-6 on including tax rates with fee profiles.

Other Fees

1. Select the **Edit** button on the right side of the title “Other Fees”. A new screen appears.

2. Enter the Start Date, and end date, if applicable, fee description and amount. Select the tax box if the item or service is taxable.

3. Once you have made changes to the information on this screen, select the “**Save and Return”** button. Your computer screen refreshes itself and you are directed to the Merchant Profile screen.

Guarantee Fee profile

1. Select the **Edit** button on the right side of the title “ Guarantee Fee Profile”. A new screen appears.

2. Using the Drop down menu boxs - select which kind of guarantee (ECC or paper) class to assign this merchant. This will depend if there is a paper guarantee, or ECC guarantee. If there isn’t any options to select underneath the drop down menu, the guarantee fee profile needs to be setup. See “General Fee Profile Setup” on page 14-7 for more information.

3. Select the **Edit** button next to the subheading “Common Settings” to input a tax rate and/or a minimum processing fee for the billing cycle. Select the **Update** button.

4. Select the “**Return to Guarantee Fee Profile Management”** button to return. Select the “**Return to Merchant Profile”** button to return to the Merchant Profile screen. The applied changes are reflected on this screen.

Standard Fee Profile

1. Select the **Edit** button on the right side of the title "Available Standard Fee Profile". A new screen appears.

2. Using the Drop down menu box - select which kind of Standard profile to assign this merchant. This will depend if there is a verification, ECC or Verification and ECC fee profile setup. If there isn't any options to select underneath the drop down menu, the guarantee fee profile needs setup. See "General Fee Profile Setup" on page 14-7 for more information.

3. Select the **Edit** button next to the subheading "Common Settings" to setup a tax rate and/or a minimum processing fee for the billing cycle. Select **Update**.

4. Select the Return to **Standard Fee Profile Management** button to return and then select the **Return to Merchant Profile** button to return to the merchant profile screen. The changes will apply and reflect on this screen

Deleting a Merchant

To delete a Merchant perform the following steps:

1. Select the Merchant Profile Screen.

2. Click on at the end of the blue-highlighted Merchant Info heading row in order to display the Merchant Info screen

3. Select the "Delete Merchant" button.

NOTE
Read the on screen message carefully, before deleting any merchant

4. Select "OK" if you are certain you want to delete this merchant.

Merchant Groups

The Merchant Groups submenu allows authorized users to access and change merchant profile information for individual merchants and to assign these merchants to a group. Using this group feature you are able to assign a single statement that contains transaction and pricing totals of multiple individual locations.

Under **Merchant Groups**, individual merchants in various geographic locations belonging to a larger organization are grouped together under their ID number. Their individual Merchant ID numbers are also listed within the window.

Adding Merchant Groups

To add a merchant group:

1. Select the **Merchant Group** link under Merchant Admin. A new screen appears.

2. Select the **Add New Group** button at the top of the screen. A new screen appears.

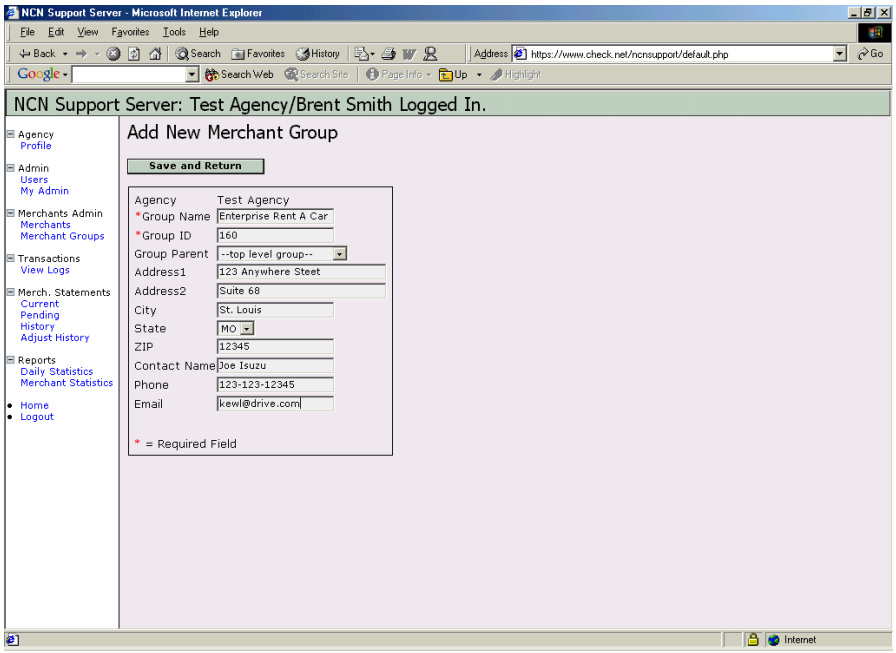


Figure 14-8. Add New Merchant Group Screen

3. Complete the following fields on the screen and press the **Save and Return** button at the top of the screen. The screen refreshes and returns to the Merchant Group Screen. It is recommended that all fields are filled in.

Table 14-2. Merchant Group Field Descriptions

Field Name	Description
Group Name	Name of this group to be created. This is required
Group ID	Unique number (up to 6 digits) to assign to this group being created. This is required.

Table 14-2. Merchant Group Field Descriptions

Field Name	Description
Group Parent	Typically this is setup as a top level option. However, this option allows a newly created group to be listed as a subgroup for an earlier created group. (For example - National Rent a Car has a corporate office that is already created as the top level group. You are able to assign a new group, such as the western regional division, as a subgroup of this headquarters top level group.)
Address 1	Address of business.
Address 2	Continued Address
City	City
State	State
Zip	Zipcode
Contact name	Contact Person
Phone	Phone Number
Email	Email Address

After the group is created, Merchants can be added.

Adding an Unassigned Merchant to a Group

1. Select the **Merchant Group** link under “Merchant Admin”. A new screen appears.

2. In the right column on the screen labeled Unassigned Merchants, select the merchant that you want to add to a group. The screen refreshes to the Merchant Profile Screen.

3. Select the **Edit** button on the right hand side of the screen, next to the label of “Merchant Info”. A new screen labeled Edit Merchant Info appears.

4. In the right hand column there is a field named “Merchant Group”. Select the drop down box arrow on the right side of this field, and then select the group you would like to assign this merchant to.

5. Select the **Save and Return** button at the top of the page. The screen refreshes and returns to the “Merchant Profile” screen.

   When you are finished, click on any of the blue-highlighted submenus on the left side of the screen to continue through the NCN Support Server.

Transactions

The Transactions menu is the one of the most significant enhancements of the Support Server for Direct Agency Users. This feature allows support personnel to actually view and research transaction data when answering customer calls. There is only one submenu that is labeled “View Logs”.

To access the Transaction Logs - select the **View Logs** link under “Transactions” menu item.

View Logs

The “Search Logs” screen allows Direct Agency support personnel to find the data they need in order to answer customer questions regarding checks that have been declined, approved or otherwise.

The “Search Logs” screen is divided into four sections, otherwise known as “Filters.”

NOTE
A user searching for specific transaction information can use any one of these filters in order to access the needed information. It is not necessary to enter information in all fields.

Each field’s value and function in each of these four filters are described below:

Table 14-3. Transactions – Point of Sale Filters

Field Name	Field Description
Merchant	Name of individual Merchant
Merchant Group	Name of Merchant Group
Include Subgroups	Merchant Group Subgroups
Sites	Agency Site Number
Location Number	Merchant Number (i.e. Merchant ID number)

Table 14-4. Transactions – Check Filters

Field Name	Field Description
Routing Number	The Routing *(ABA)* number of the bank on which the draft (electronic check) is drawn.
Account Number	Customer’s Account Number
Check Number	Customer’s check Serial Number
Check Amount	Transaction dollar amount

Table 14-4. Transactions – Check Filters

Field Name	Field Description
Between (or exact)	Allows the support server to search within a dollar amount range
And (optional)	Allows the support server to search within a dollar amount range

Table 14-5. Transactions - Check Writer Filters

Field Name	Field Description
Issuing Identity	State of issuing Identity
ID Number	Identification number on ID
ID Type	Driver's License, Social Security Number, Courtesy Card.

Table 14-6. Transactions - Transaction Processing Filters

Field Name	Field Description
Transaction Number	Sequential number assigned *by NCN* to transaction
POS Response	There are three classes of response: AUTH = Authorized, or accepted WRN = Warning *(to Merchant), this check, or its face amount, is beyond that Merchant's (or that Customer's) limit for that day* DEC = The check has been declined for *various reasons*
Date Range	Allows user to enter a range of dates within which to search
Time Range	Allows user to enter a range of time, from 12:00 AM to 12:00 PM, Mountain Standard Time

Once all data is entered, Click on the **Search** button (either at the top or on the bottom of your screen) to access the transactions.

NOTES

– If you have entered incorrect information, click on " Clear All" (either at the top or on the bottom of your screen) to refresh the screen. Resume entering information.

– If the data you have entered is insufficient, you will receive an error message in red print at the bottom of your screen.

– If there isn't any activity, or transactions based on the information entered, the transaction screen is be displayed with the following message is displayed : There are no results for your search. Please try again.

Upon a successful search you are able to view the transactions in a new window.

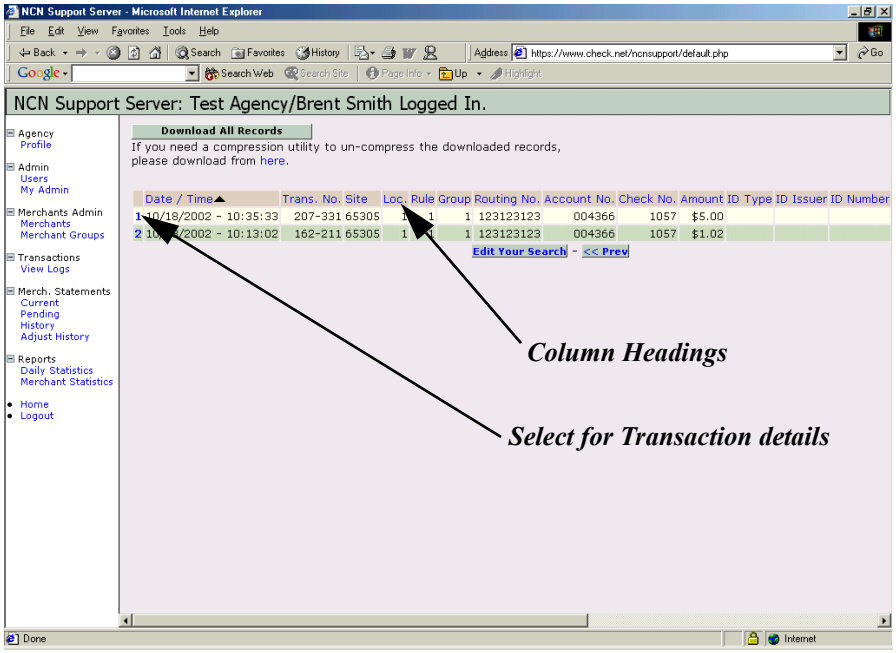


Figure 14-9. Successful Transaction search result screen

With multiple transactions listed you can select the Column Headings to sort in reverse order based on the heading name.

By selecting the number in the left column you are able to view the transaction details Figure 14-10:. Transaction details reflect information

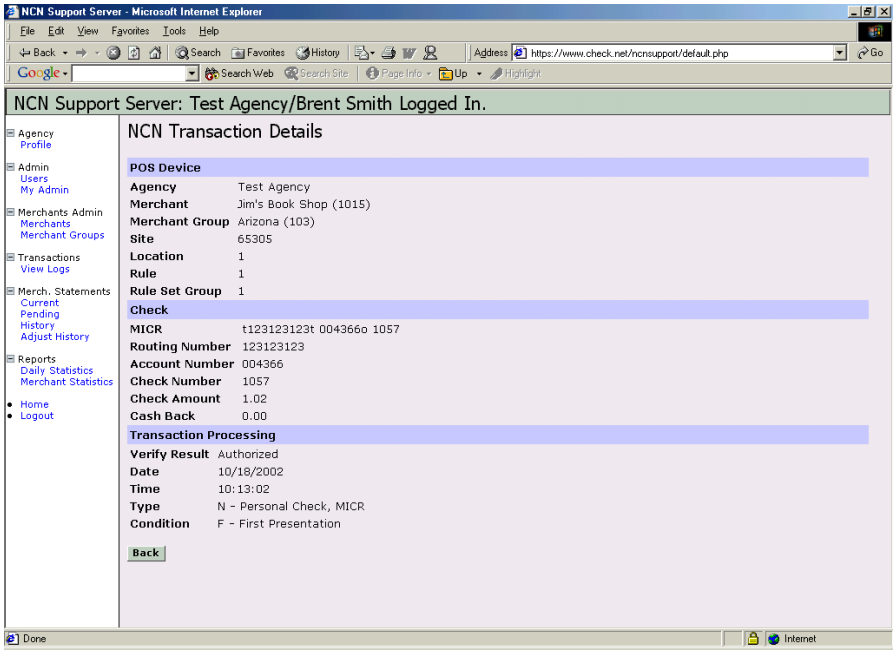


Figure 14-10. Viewing a Transaction Detail

about and individual transaction.

Using the NCN Support Server to obtain Transaction Logs

Once the NCN support server account is setup and accessible, the user is able to view, and download transactions logs. To do this perform the following steps:

1. Select the transaction “View Logs” link on the left panel

2. Enter the appropriate information to view logs. Include the date range of which you would like to view. Select “**search”**. Refer to “View Logs” on page 14-20 for more information to obtain logs.

3. Once transactions logs are listed, select the “**Download All Records”** button at the top of the screen. This displays a window in which you’ll be able to download these transactions onto your personal computer. You can open this comma-delimited file in a program, such as MS Excel, or a database reporting program.

Merchant Statements

The Merchant Statements menu consists of four submenus that allow authorized users to access three types of merchant statements: **Current**, **Pending**, **History** and **Adjust History**.

NOTE

You must have Adobe Acrobat Reader installed on your computer to view the statements. It is available at no charge at www.adobe.com

Current Statements

Click on the **Current** submenu to access the screen shown below:

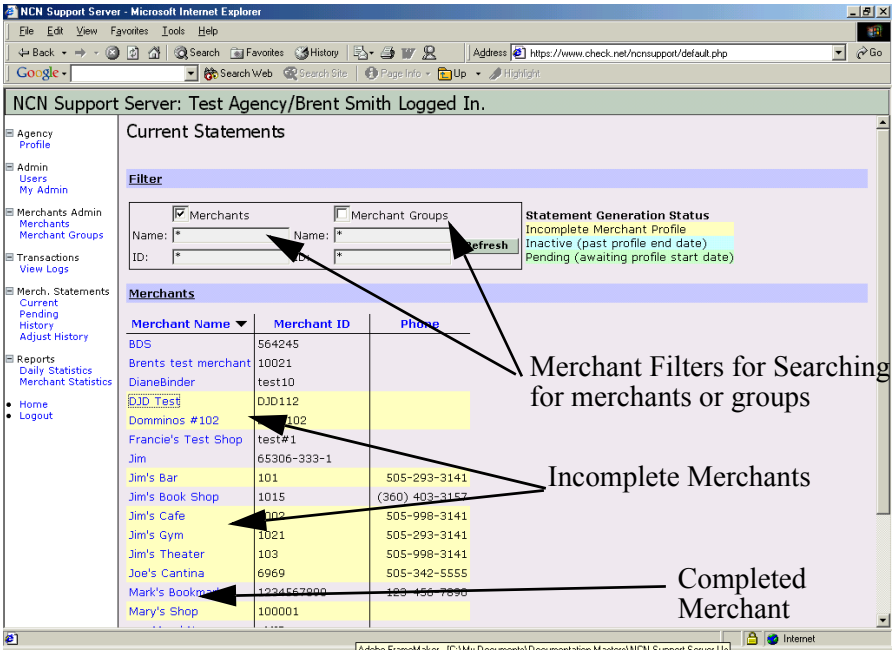


Figure 14-11. Current Statements Screen

The “Current” merchant statements reflect transactions processed prior up to approximately fifteen minutes of live transactions on the *current day’s date of business*.

1. To access Merchant Group Statements select the **Current** link under the Statements menu item

2. Select the merchant in which to review their statement. A new screen appears in Adobe Acrobat that displays the current statement.

NOTE

A merchant is highlighted in yellow, light blue or green indicates a problem in the way the “Merchant Profile” is setup in regards to the required files. The results in the statement do not reflect any transaction or billing amounts until these merchants are setup and completed.

Pending

The pending statement section reflects an adjustment windows before the statements are automatically placed in the history section or archived. There is room for adjustment in the statement totals within this time frame by the user. Initially, this time frame is setup with the agency

To access the pending statements for each merchant:

1. To access “Merchant Group Statements” select the **Pending** link under the Statements menu item.

2. Select the merchant in which to review their statement underneath the Pending Merchant Statement section. A new screen appears in Adobe Acrobat that displays the current statement.

   If statements are in the default 10 day window (after the end of the month) there are individual or group statements listed underneath the Pending Merchant Statement section of the window. Follow the steps to review, edit, and approve the process to permanently complete the statement process and move them into archive (history).

3. Once the individual or group merchants are listed:

a. If changes need added - select the EDIT button next to the merchant. A new screen appears where you can edit charges.

b. When statement has been reviewed a looks okay - select the APPROVED button next to the merchant. This PERMANTELY moves the statement into the history folder

NOTES

– Make certain you changes are correct - once the Approved button is pressed the statement moves to the history folder in which changes are no longer permitted. If you do not edit, change or approve the statements within the time period noted (default 10 days), the system automatically assumes that the statements have been reviewed, and moves them to "History" automatically.

History

The statement history screen is used to review and retrieve statements that have completed the final process of "Pending" and are archived here. This is the location of your merchants statements when they are archived. To access the History statements:

1. Select the **History** link underneath the Merch. Statements submeu.
2. Underneath the Filter section - select the month of statement range from the drop down menu.
3. Select the **Refresh** button

You'll then see a listing underneath the Statement section that shows individual merchants that can be downloaded, or one can download all of the statements by pressing the Download PDF statements button.

NOTE

These statements cannot be edited

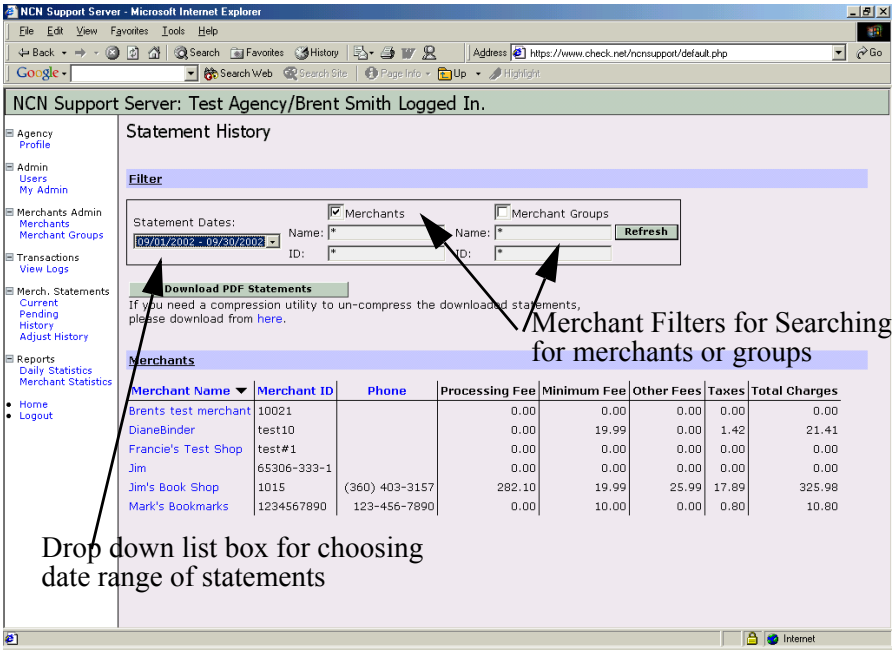


Figure 14-12. Statement History screen

Adjust History Link

The Adjust History link is used to change the end date of the most recently archived statement period. This change adjusts and recalculates all merchant statements and all merchant group statements within this period.

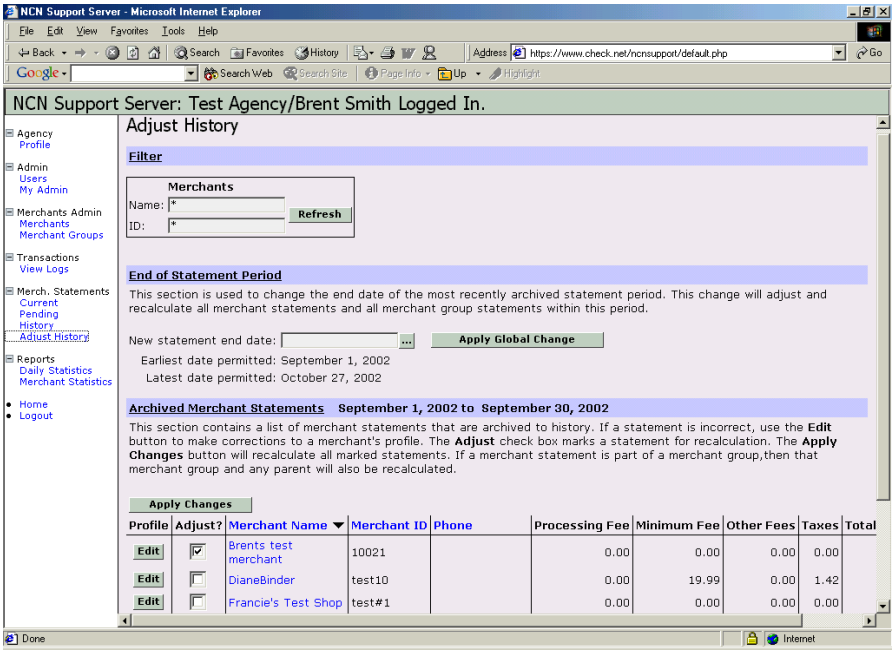


Figure 14-13. Adjust History screen

To change and Adjusted History:

1. Select the Adjust History submenu item.
2. Select the "..." button to visually select a date to place in the date field.
3. Select the "**Apply Global Change**" button to change the Adjusted History date.

Reports

There are two submenus listed as Daily Statistics and Merchant Statistics. The Daily Statistics shows a report which reflects the daily activity for a date range entered into a search engine. The Merchant Statistics reflects the total amount of activity for a date range entered into a search engine.

Daily Statistics

The Daily Statistics shows a report that reflects the daily activity for a date range entered into a search engine.

This is a tool designed as an alternative to searching transaction logs. You can search by each merchant location and view daily activity.

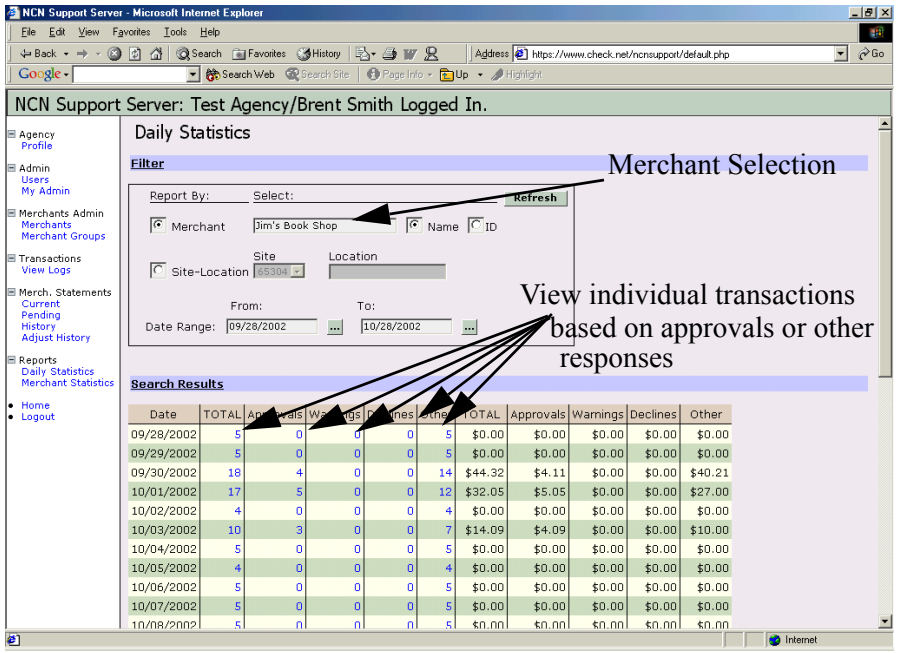


Figure 14-14. Daily Statistics Window

To lookup and view a daily statistic for a merchant:

1. Select the **Daily Statistics** link underneath the "Report" submenu. A new window appears.

2. Input the information necessary to select the merchant, and date range required for the search.

NOTE

Placing an asterick * in the merchant field yields a list of merchants programmed into the support server.

3. Select the "Refresh buttons". A List of Merchants will appear below. Select the merchant to view the "Daily Statistic" report.

NOTE

If transactions are NOT listed, double check to make certain the merchant information was entered into the search field correctly. Transaction activity for the date range area AND the merchant needs to be entered into the search area to obtain successful results

At the bottom of the report - the support server displays the total amount of the information provided in the search. An example is listed below:

Average daily approved amount = $1.97

Average daily warned amount = $0.00

Average daily declined amount = $0.00

Average daily other amount = $1.59

Merchant Statistics

The Merchant Statistics *reflects the total amount of activity* for a date range entered into a search engine.

To lookup and view a merchant statistic for a merchant:

1. Select the **Merchant Statistics** link underneath the Report submenu. A new window appears.

2. Input the information necessary to select the merchant and date range required for the search.

NOTE
By placing an asterick * in the merchant field yields all of the merchants programmed into the support server.

3. Select the "Refresh buttons". A List of Merchants will appear below. Select the merchant to view the "Merchant Statistic" report.

NOTE
If transactions are NOT listed, double check to make certain the merchant information was entered into the search field correctly. Transaction activity for the date range area AND the merchant needs to be entered into the search area to obtain successful results

System Management

Negfile

This submenu item allows your agency to submit, manage and retrieve negfiles via the support server.

Submit Negfiles to the national database

To upload a negfile to the system:

1. Select **NegFiles** submenu link under the System Management Menu item

2. Select the **Submit File** link on the top right hand of screen to open up a new user screen as shown:

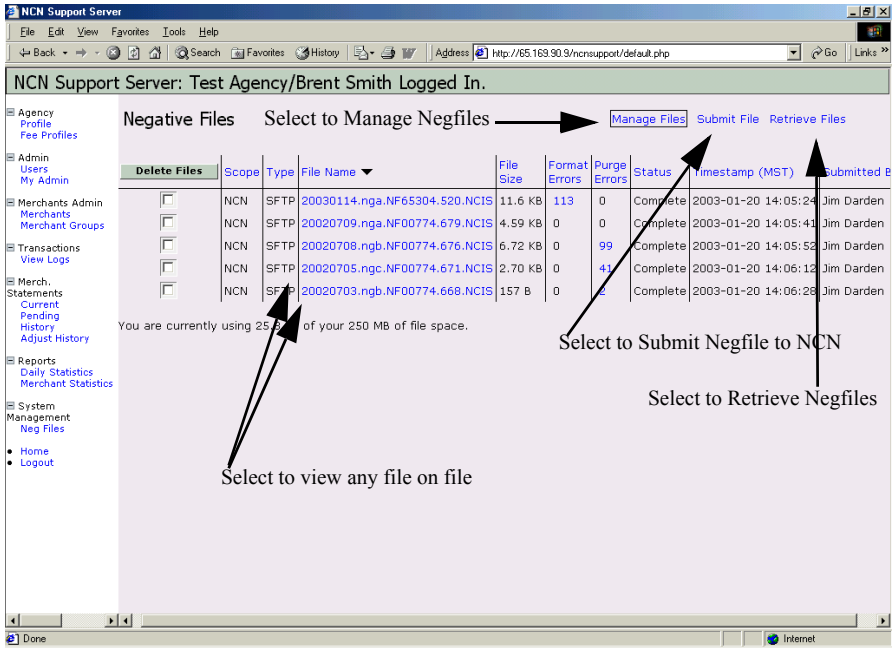


Figure 14-15. Negative File Submission, Management and Deletion

Under the submenu of "Add Negative File", type in the filename to upload, or press the Browse button to locate the file on your local workstation.

Underneath the option menu there are two file types to select:

a. "Daily": Daily describes a changed file since the full upload of a complete database (negfile). This selection is default and will apply most of the time unless the agency has had a recent cleaning of their database and needs to resend a full database

b. "Refresh": This is a full database negfile. Use this option only if your database is purged on the system after a cleaning by the staff in Boulder.

Select "Daily or Refresh" and then the **Upload file** button

NOTE

Files cannot be larger than 32 MegaBytes in size to process with the NCN system. If an agency has a file more than 32 Megabytes, it can be split up and submitted as differential files to the system.

Filescope options:

Apply file to NCN Authorization System - Default

Local copy for reporting only - to be used with Compliance Reports.

Manage Files

This selection describes the options available to view the negative files which were processed by the NCN Authorization system. This includes the option to delete processed negative files to conserve file space.

Each file processed includes hypertext links which the user can select and view information on each processed file. There are three types of processed files:

a. The complete file processed

b. Format Exception errors

c. Purge Exception errors

Rulesets

Coming soon.

Compliance Reporting

Coming soon.

Home

Select the **Home** link at any location in the NCN Support Server, in order to return to the Agency Home Screen.

Logout

Select the **Logout** link to exit the NCN Support Server session.

15 - Appendix and Quick Reference

The appendix and quick reference contains information that you may find helpful in supporting the NCN applications.

Selection and List of VeriFone Programs for NCN

Table 15-1. Selection Guide

	ZON Jr XL	TRANZ 330	TRANZ 380
SINGLE KEY PROGRAMS			
MICR (any check reader) w/ chk amount		SK33x	SK38x
MICR (any reader) thru PIN pad port, w/ chk amt		SK33xP	SK38xP
MICR (Soricon MR-1000 reader only) w/ chk amt	JRXLx		
MICR (non-MR-1000 reader) w/ chk. amount	JRXLDx		
MICR w/ chk amount & sale amount		SKS33x	SKS38x
MICR w/o amount (non-MR-1000 reader on XL)	FKXLDx	FK33x	FK38x
MICR (manually keyed) w/ chk amount	JRXLMx	SK33xM	SK38xM
ID-based (DL) w/ chk. amount	ZONIDDx	33IDDx	38IDDx
ID-based (SS) w/ chk. amount	ZONIDSx	33IDSx	38IDSx
MULTI-FUNCTION PROGRAMS			
MICR (any reader) 3 key, w/ chk amount		SP33789	SP38789
MICR (MR-1000 reader) 3 key, w/ chk amount	XL789		
MICR (non-IVI reader) 3 key, w/ chk amount	XLD789		
MICR (any reader) plus Driver's License		SPMDLx	SPMDL8x
MICR (any reader) 3 function (1 key) w/ chk amt		SPxPYRL	SPxPYR8
MICR 3 function/1key, w/ chk amt & W/D print		MFxPNTR	MF38xPT
ID-based (DL) w/ check amount, & W/D print		33DLxPT	

NOTE

The XL300 uses the same programs as the ZON Jr XL EXCEPT when used with an IVI MR-1000 check reader, which requires a special cable and a special program.

Program List

In the lists that follow, please note the distinction between **check amount** and **sale amount**. All programs, with the exception of FK33x and FK38x, ask for the check amount. Few users want sale amount except supermarkets, who return cash to the customer.

Programs for the ZON Jr XL or XL 300 (except with IVI reader)

These programs all prompt for the check amount after getting the MICR or ID. Four of them also prompt for the sale amount that is used to calculate cash back to the customer. Note that the letter "*x*" denotes your choice of the key used for the program, always between 2 and 9.

Table 15-2. Programs for the ZON Jr XL or XL 300 (Except with IVI Reader)

Program Name	Description
JRXL*x*	MICR transactions with check reader input (IVI=Soricon)
JRXLD*x*	MICR transactions with check reader input (non-IVI)
JRXLM*x*	MICR transactions with manual keying of check data
FKXLDx	MICR transactions w/ check reader input (non-IVI) and amount = 0.00
ZONIDC*x*	I.D.-based transactions with courtesy card
ZONIDD*x*	I.D.-based transactions with driver's license
ZONIDP*x*	I.D.-based transactions with phone number
ZONIDS*x*	I.D.-based transactions with Social Security number
ZNIDC*x*S	I.D.-based transactions with courtesy card, check amount & sale amount
ZNIDD*x*S	I.D.-based transactions with driver's license, check amount & sale amount
ZNIDP*x*S	I.D.-based transactions with phone number, check amount & sale amount
ZNIDS*x*S	I.D.-based transactions with Social Security number, chk amt & sale amt
XL789	Key "7" = MICR transaction w/o ID; Key "8" = MICR transaction w/ ID; Key "9" = payroll check w/ ID; All use Soricon check reader ; Early dial if Loc 399 = 1; Sale amount if Loc 397 = 1. Uses extra Locs 380-399.

Table 15-2. Programs for the ZON Jr XL or XL 300 (Except with IVI Reader) (Cont.)

Program Name	Description
XLD789	Key "7" = MICR transaction w/o ID; Key "8" = MICR transaction w/ ID; Key "9" = payroll check w/ ID; All use non-Soricon check reader; Early dial if Loc 399 = 1; Sale amount if Loc 397 = 1. Uses extra Locs 380-399.
In this table, "x" is any integer between 2 and 9 (inclusive)	

Programs for the XL 300 with IVI Reader

NOTE
The XL 300 requires a special cable for IVI rdr!!!

Table 15-3. Programs for the XL 300 with IVI Reader

Program Name	Description
XL300	MICR transactions with check reader input (Soricon)
XL3789	Same functions as XL789

Programs for the TRANZ 330

Except for FK33x, these programs all prompt for the check amount after getting the MICR or ID. Five of them also prompt for the sale amount that is used to calculate cash back to the customer. Note that the letter "x" denotes your choice of the key used for the program, always between 2 and 9. Programs for the TRANZ 330 work for all check readers.

Table 15-4. Programs for the TRANZ 330

Program Name	Description
FK33*x*	MICR transactions with check reader input but NO CHECK AMOUNT
SK33*x*	MICR transactions with check reader input
SK33xP	MICR transactions with check reader input through PIN pad port
SKS33*x*	MICR transactions with check reader input & sale amount
SK33*x*M	MICR transactions with manual keying of check data
33IDD*x*	I.D.-based transaction with driver's license
33IDS*x*	I.D.-based transaction with Social Security number

Table 15-4. Programs for the TRANZ 330 (Cont.)

Program Name	Description
SP33789	Key "7" = MICR transaction w/o ID; Key "8" = MICR transaction w/ ID; Key "9" = payroll check w/ ID; All use check reader; Early dial if Loc 923 = 1; Skip sale amount if Loc 712 = 1. Uses extra Locs 913-923.
SPMDLx	Always gets both MICR (any reader) plus driver's license and check amount; never gets sale amount; Uses Locs 914-921 (regardless of key)
SPxPYRL	All three transaction types initiated by key "x", using a secondary menu to select specific type; Skip sale amount if Loc x12 not empty. Locs x13-x33. Check reader input can use printer port or PIN pad port.
MFxPNTR	All three transaction types initiated by key "x", using a secondary menu to select specific type, and printing Warnings or Declines on roll printer. Skip sale amount if Loc x12 not empty. Locs x50-x80 for x=2,3,...,8; Locs 913-941 for x=9. Check reader input can use printer port or PIN pad port.
33DLxPT	ID-based transaction w/ driver's license and printing Warnings or Declines on roll printer. Locs x87-x99 for x=2,3,...,8; Locs 937-949 for x=9.
RMRS330	Full interactive program capable of performing all types of transactions on Velocity PLUS®
In this table, "x" is any integer between 2 and 9 (inclusive)	

Except for FK38*x*, these programs all prompt for the check amount after getting the MICR or ID. Five of them also prompt for the sale amount that is used to calculate cash back to the customer. Note that the letter "*x*" denotes your choice of the key used for the program, always between 2 and 9. Programs for the TRANZ 380 work for all check readers.

Table 15-5. Programs for the TRANZ 380

Program Name	Description
FK38x	Same as FK38*x*
SK38*x*	Same as SK33x
SK38xP	Same as SK33x except check reader input through PIN pad port
SKS38*x*	Same as SKS33*x*
SK38*x*M	Same as SK33*x*M
38IDD*x*	I.D.-based transaction with driver's license
38IDS*x*	I.D.-based transaction with Social Security number
38IDC*x*S	I.D.-based transaction with courtesy card & sale amount
38IDD*x*S	I.D.-based transaction with driver's license & sale amount
38IDP*x*S	I.D.-based transaction with phone number & sale amount
38IDS*x*S	I.D.-based transaction with Social Security number & sale amt

Table 15-5. Programs for the TRANZ 380 (Cont.)

Program Name	Description
SP38789	Key "7" = MICR transaction w/o ID; Key "8" = MICR transaction w/ ID; Key "9" = payroll check w/ ID; All use check reader (Soricon); Early dial if Loc 923 = 1; Skip sale amount if Loc 712 = 1. Uses extra Locs 913-923.
SPMDL8x	Always gets both MICR (any reader) plus driver's license and check amount; never gets sale amount; Uses Locs 914-921 (regardless of key)
SPxPYR8	Same as SPxPYRL
MF38xPT	Same as MFxPNTR
380	Full interactive program capable of performing all types of transactions on Velocity PLUS®. It uses the entire terminal and does not coexist with any credit card program
RMRS380	Full interactive program capable of performing all types of transactions on Velocity PLUS®. It uses the upper half of the terminal memory (non-split key) and can coexist with any credit card program that uses only the lower half of memory (Locs 0000 - 0999)
In this table, "x" is any integer between 2 and 9 (inclusive)	

Programs for the TRANZ 340

Table 15-6. Programs for the TRANZ 340

Program Name	Description
RMRS400	Credit card transactions into MAPP network (using external modem connected to TRANZiT 1200C) plus single packet MICR transactions (using internal modem of TRANZiT 1200C) with same functions of SP33789.

Programs for the ZON Jr PLUS

Note that the ZON Jr PLUS does not provide for a program name. Instead, the download ID placed in location 01 accomplishes all program selection.

Table 15-7. Programs for the ZON Jr PLUS

Program Name	Description
(download ID)	MICR transactions with manual keying of check data
(download ID)	I.D.-based transactions with driver's license
(download ID)	I.D.-based transactions with Social Security number

Rule Set Parameter Definitions

This document explains the items used in specifying a rule set for NCN. Each item is referenced by number or number-letter. Section 4: "NCN Rule Set Maintenance" contains a detailed list of these numbers.

NCN site number. This number was assigned to your agency by Rocky Mountain Retail Systems when you became a member of NCN. It is used to "tag" your contributions to the database and must also be placed in the VeriFone terminals at your customer locations so that verification transactions can be "tagged" with your site number (see note following item 2 for additional information).

Rule set number. This must be a number between 1 and 9999. This number must placed in the VeriFone terminals at your customer locations and causes verification transactions from that terminal to be evaluated using that set of "rules". The "rules" are primarily limits placed on check passing activity, face amount of checks, etc.

The first field of any verification request packet sent to NCN must contain a terminal ID (sometimes called merchant ID) that includes an NCN site number, a merchant number, and a rule set number. Following is a valid terminal ID:

3718-812759-22

In the above example, 3718 is the NCN site number, 812759 is the merchant number, and 22 is the rule set to be applied to transactions from this terminal. The merchant number may be freely assigned by an NCN site and can contain from 1 to 6 digits.

Terminal idle prompt. This field of 16 characters is displayed by VeriFone terminals (except the ZON Jr PLUS) when a terminal begins a check verification transaction. Any word or phrase may be used, but it is preferable to choose a name that includes some reference to the rule set number and to your agency. This practice provides a way to easily determine which rule set is being invoked by transactions from a particular terminal. This is a required rule set item and may not be left blank.

The NCN software sends a response packet back to the point-of-sale terminal that includes the above mentioned "terminal idle prompt" as the first 16 characters. Most VeriFone terminals can strip this idle prompt off and then display the remainder of the message for the clerk. ZON Jr PLUS terminals lack the capability to separate this idle prompt from the rest of the message, so such terminals display the received idle prompt upon completion of the transaction. On ZON Jr PLUS terminals, the clerk must then press the "9" key to scroll the display to the right in order to see the response to the verification request. This is easier for clerks to remember if the idle prompt is more descriptive, e.g. "PRESS 9 FOR ANS" for those locations using ZON Jr PLUS terminals.

Group number. This field allows selection of data from a group of merchants (usually a specific store chain or merchants with similar characteristics). Its use is for excluding NCN database information that is not "tagged" with the matching site and group number during the evaluation of a transaction. When specified, it should be a number between 1 and 99 inclusive and rule set item 23 (Group set) must be specified as well.

Point-of-sale options affect what is shown on the terminal display at the completion of a verification transaction.

5a Return reason list. Selecting this option makes detailed information available at the point of sale terminal whenever a check is not authorized. Thus, in addition to either a warning or a decline message, "scrolling" the terminal displays more detail such as which limits are exceeded, the break down of unpaid checks by site/location, site/group, and total system, the name and telephone number of the agency (or agencies) that holds any unpaid check items, etc.

5b Require ID if none. Selecting this option causes the NCN system to examine whether the MICR account specified in the verification request packet has at least one ID associated with it. If it does not, and the verification request packet from the POS terminal did not include an ID, then the transaction is refused with a message returned to the terminal stating ID IS NEEDED. At this point, the transaction must be repeated using a "key" that allows an ID to be entered as part of the transaction. This option should ONLY be used when the point-of-sale terminal has the capability of prompting for an ID and including this in the verification request packet.

Single transaction limits apply to amounts involved in an individual verification request.

6a Amount requiring ID. This sets the limit on the amount of a check that requires an ID to be included in the verification request packet.

NOTE

for this particular limit (6a) 0 is treated as special case. If 0 is used for this limit, it is always considered to be exceeded. This in turn forces an ID to be required for all checks, a feature that is used by agencies that are offering a check guarantee service through NCN.

6b Maximum check amount. This sets the maximum amount of a check that is approved.

6c Cash back requiring ID. This sets the maximum cash that can be returned without supplying an ID in the verification request packet. This option is only usable when the point-of-sale terminal prompts the clerk for both the check amount and the sale amount. Only then can "cash returned" be calculated.

6d Maximum cash back. This sets the maximum cash that can be returned. This option is only usable when the point-of-sale terminal prompts the clerk for both the check amount and the sale amount. Only then can "cash returned" be calculated

Single day activity limits are used to set limits on the cumulative number or amount of transactions for a specific account for the current day. Which transactions are added together can be: unrestricted (from anywhere); restricted to transactions from a particular site/group set; tightly restricted to transactions from a particular site/location.

The **personal check activity window** option sets the number of days of information that are to be included in measuring the activity (often this is referred to as "velocity") of an account. This can be set from 1 to 14 days. A setting of 1 includes only today's activity. A setting of 2 includes today and yesterday.

Personal check "window" limits are applied against the cumulative activity that has occurred on an account during the activity ("velocity") window specified by rule set item 8.

Maximum payroll check amount. Sets the maximum face amount of a payroll check that is accepted.

Payroll activity window. Set the activity "window" for payroll checks.

Sets **limits on payroll check cashing activity** accumulated within the activity "window" set by item 11.

NOTE

Payroll check cashing activity is accumulated against the ID that is presented as a required part of the transaction.

12a Number payroll checks per window. Sets limit on the number of payroll checks cashed using a particular ID within the "window" period of days.

12b Amount payroll checks per window. Sets limit on the cumulative dollar amount of payroll checks cashed using a particular ID within the "window" period of days.

ID approval required. IDs must be presented when a payroll check verification is conducted. Options 13a through 13d specify the level of approval required to make an ID acceptable for use in conjunction with payroll check cashing. Either 13a, 13b, or 13c must be "YES" to set the scope of approval required. Note that you cannot change 13a, 13b, or 13c to "NO"---you must set the desired option to "YES" and the others are automatically change to "NO". Use 13d to determine whether such approval is automatic or requires a manager.

13d Manager required to approve payroll ID. This option selects whether manager approval is required before an ID can be used for payroll check cashing. If such approval is required, the manager must use a specially programmed VeriFone terminal to communicate an ID approval packet to NCN. If manager approval is NOT required, then any ID submitted in conjunction with a payroll check transaction is automatically approved at the level specified by option 13a through 13c.

13e Manager required to approve payroll account. This option selects whether manager approval is required before an account can be used as a payroll check. If such approval is required, the manager must use a specially programmed VeriFone terminal to communicate a payroll account approval packet to NCN. If manager approval is NOT required, then any account is accepted as a payroll account.

Unpaid check limits. This group of options sets limits on the number of outstanding unpaid checks that are tolerated. Only in very unusual circumstances would a number other than 0 be used here. In fact, these options may be left blank, in which case the default is 0.

Federal Reserve list. The first 2 digits of the transit/routing number indicate the Federal Reserve district where the bank is located that holds the checking account. The Federal Reserve districts are numbered 01 through 12. If a bank is a savings and loan institution rather than a full service bank, 20 is added to the Federal Reserve number where the savings and loan institution is located. In addition, 00 is reserved to indicate a US Government check and 80 indicates a traveller's check. NCN allows the use of the first 2

digits of the transit/routing number to indicate whether the check is to be considered "local" or "out-of-area". If no entries are made for this option, all checks are treated as "local". If one or more entries are made for this option, those banks and saving and loans that are in the listed Federal Reserve districts are treated as "local".

NOTE

If 10 is entered, 30 is assumed, so there is no need to make an entry for a regular bank and another one for a savings and loan in the same district.

"Out-of-area" checks receive a message (usually a warning message, but a decline message may be sent if desired) indicating that the check is "out-of-area" unless there is one or more IDs associated with that account.

Allowing the presence of an ID to override an "out-of-area" condition accommodates "naturally out-of-area" accounts such as those from college students or military personnel. Once an ID has been accepted by a local merchant, the account is treated as local, even though the Federal Reserve district may be far away.

Special limits for "young" accounts. A new account is one that has never been "seen" by NCN. There are two ways an account becomes known to NCN: a verification transaction is conducted involving the account; a returned check drawn on the account has been entered in the NCN database. If an account becomes "known" through a verification transaction, there is no information, positive or negative, on which to base an authorization. In this case, many merchants want to use a different set of criteria (limits) in evaluating the verification request until enough time has passed for a check to clear and thus generate positive information. NCN allows for this by putting an account in the "new" category for a number of days specified by rule set items 16a (for "local" checks) and 16b (for "out-of-area"). Verification requests for accounts that are in the "new" state use the limits given in rule set items 17, 18, and 19.

CAUTION

Setting the new account hold period for either local checks or out of area checks to a non-zero value requires setting alternate limits (items 17-19) as well. Otherwise, any new account has NO limits until the end of the new account hold period.

16a New local account window. This sets the number of days a never-before-seen "local" checking account is to be considered "new". Setting this number to 0 inhibits the use of an alternate rule set (limits 17, 18, and 19) for "local" checks. 0 to 14 days can be specified.

16b New out-of-area account window. This sets the number of days a never-before-seen "out-of-area" checking account is to be considered "new". Setting this number to 0 inhibits the use of an alternate rule set (limits 17, 18, and 19) for "out-of-area" checks. 0 to 14 days can be specified.

New account transaction limits. These are the same as rule set item 6 except that they are only applied to accounts that are in the "new" state.

New account single day velocity limits. These are the same as rule set item 7 except that they are only applied to accounts that are in the "new" state.

New account window velocity limits. These are the same as rule set item 9 except that they are only applied to accounts that are in the "new" state.

Point-of-sale messages. NCN allows the authorization/warning/decline messages that are returned to the point-of-sale terminal to be customized. An example where this capability might be useful is if your agency wants all verification transactions other than authorizations to result in a message on the terminal requesting a call be made to a "help desk" to get an authorization. If no entries are made for rule set items 20a...c, the following defaults are used:

Approval message	AUTH NUM 021-81
Warning message	MANAGER NEEDED
Decline message	DECLINE CHECK

For approval messages, a 6 digit (plus dash) transaction number is always appended, so only the first 9 characters are available for modification. In the default approval message shown above, 021-815 was the transaction number.

Bad ID criteria. When an ID is included in a verification request packet, the NCN system looks to see if any negative information is connected to that ID. If any are found, the transaction is not given an authorization. Because there are multiple sources of such negative information and there may be cases where a merchant does not want some of those reasons to cause an authorization failure, NCN provides a "mask" that permits each merchant to select which of the negative items are to be used in determining the goodness of the ID. Rule set items 21a through 21h allow the selection of such items. By default, if none of these items are marked as selected, NCN assumes that 21a, 21b, and 21c are "selected". 21d through 21h are not "selected".

NOTE
The use of special purpose ID "flags" 1 through 5 must be coordinated through NCN management.

Warning and Decline conditions. This option determines which type of result message is returned to the terminal when particular conditions are detected during the verification request evaluation. If more than one condition is detected, the more "serious" message is returned to the terminal. Thus, if a condition was detected that would return a warning message together with another condition that would return a decline message, only the decline message is sent to the terminal, along with (if enabled by item 5a) the reason (or reasons) for all detected conditions. The defaults for this item are:

22a= D	Account Problem
22b= D	Unpaid Items
22c= W	Transaction Limit
22d= W	Day Velocity Limit
22e= W	Window Velocity Limit
22f= W	Out of Area
22g= D	ID Flagged (personal check)
22h=D	ID Flagged (payroll check)

Group set list. This set of ten 2-digit numbers specifies the groups to be used for

transaction activity and returned check limit tests for this rule set (see discussion of rule set item 4). If no groups are specified, all groups defined in the system are used which is the same as accepting data from anywhere. There is no need to specify a group set unless a limit such as 7b, 7e, 7h, 9b, 9e, 9h, 18b, 18e, 18h, 19b, 19e, or 19h as been specified.

Canadian checks accepted. When a check is used for MICR input at point-of-sale, Canadian checks can be detected by the presence of a dash in the sixth position of the transit/routing field (ABA number). Some agencies may want to refuse verification for such checks due to collection difficulties. This option allows them to indicate to NCN whether or not to refuse Canadian checks. If this field is left blank, then Canadian checks are NOT accepted. Note that if manual input of MICR numbers is permitted at the point-of-sale terminal, it is not possible to detect Canadian checks unless the clerks can be trained to include a dash in the proper place.

Manager password for payroll authorizations. The manager password is used for authenticating payroll ID and account authorization packets. It consists of three alphanumeric characters that must be keyed at the point-of-sale to be included with packets sent to NCN for authorizing IDs for use with payroll checks and authorizing specific MICR accounts for use as payroll checks. This option is only relevant when either 13d and/or 13e have been set to Y (which is the default). The default password here is YES which, on a VeriFone terminal requires 11 keypushes to enter because of the alpha characters. The manager, to key YES, must press:

9 <ALPHA> <ALPHA> <ALPHA> 3 <ALPHA> <ALPHA> 7 <ALPHA> <ALPHA> <ALPHA>

If the password contains leading, trailing, or imbedded spaces, these too must be keyed.

Point-of-Sale Messages

This document defines the format and content of packets sent by NCN in response to verification request packets from the point-of-sale. The format of request packets is defined in a separate document and is not dealt with in this specification.

General Information

The form of a response packet from NCN is:

<STX><iden message><result message>{<reason message>}{<unp loc>}<ETX><LRC>

where <STX> is the single character with hex value 02

and <ETX> is the single character with hex value 03

and <LRC> is the single character check character computed (per usual Verifone practice) as the XOR of all the bytes in the packet except the <STX>

and <iden message> is a 16 character identification message

and <result message> is a 16 character verification result message

and <reason message> is a 16 character "reason" message

and <unp loc> is a 2x16 character message giving the name and telephone number of the agency (or agencies) that hold the unpaid checks for the account referenced in the verification packet. and { } means repeat 0 or more times

All response packets contain at least two 16 character messages. The first 16 characters are just an identifying string that can be ignored or used as an idle prompt on the terminal or cash register. The second 16 characters contain the result of the verification or an error message. If the verification resulted in other than an "accept", additional messages giving the reason (or reasons) for the non-accept message is appended if the rule set specifies that this be done. In no case are more than 240 characters returned in the response packet.

In this section, the messages that NCN can return to the point-of-sale are shown in quotes as C format strings. All messages are padded as required with trailing blanks so that each message contains exactly 16 characters.

The following pages contain an exhaustive list of all the messages that can appear in a response packet from NCN.

Identification Messages

"idle prompt spec" – This string is specified in the NCN rule set and is usually used as an idle prompt on VeriFone terminals.

"CHECK VERIFY" – If a problem has occurred that makes it impossible to find an NCN rule set to use with this verification request, this is the default <iden message> that is output.

Verification Result Messages (Succeeded)

In NCN, the result messages that appear when the verification request can be satisfied may be customized. The messages shown below are the standard defaults that are used.

"AUTH Muons" – This is the "accept" message issued by NCN. There are no further messages following this one.

Example: AUTH NUM 681-522

The authorization number is numeric only and starts at 000-000 and runs to 999-999

"MANAGER NEEDED" – This is the "warning" message. It usually is followed by one or more "reason" messages.

"DECLINE CHECK" – This is the "decline check" message. It is usually followed by one or more "reason" messages.

"RE-PRESENTED CHK" – This message appears when NCN processes a check that it had encountered in a previous transaction. If the account has no other problems, NCN returns an AUTH code as well. Scroll to see this code.

Verification Result Messages (Failed)

The following result messages indicate why a verification request cannot be satisfied:

“ID IS NEEDED” – This transaction cannot be completed without an ID included in the request packet. This occurs if either the rule set has a limit set that requires an ID or the MICR account is associated with an ID that is “flagged”. If an associated ID is flagged, the transaction must be repeated with an included ID so that the actual ID belonging to the check presenter can be tested.

“ERROR IN MICR” – Either a ? was found in the transit or on-us field (for machine read check), or the transit field check digit (US checks only) was found to be in error. Note that the transit field check digit is tested for both manual entry and check reader entry for US checks.

“NO MICR GIVEN” – A MICR number was not found in the request packet.

“NO CANADIAN CHKS” – A Canadian check was detected (by the dash in the sixth position of the transit (ABA) field) and the system is set to reject same.

“AGENCY UNKNOWN” – The terminal ID referenced an NCN agency number (site number) that is not valid.

“AGENCY PROBLEM” – The terminal ID referenced an NCN agency number that is defined but has been set to refuse transactions by NCN management.

“SYS ERR -- RETRY” – Some error (usually transient) in the system operation has been detected.

“SYS BUSY - RETRY” – System is too busy to respond within 20 seconds. A retry usually succeeds.

“PACKET ERROR” – Packet format problem.

“AGENCY DATA ERR” – The terminal ID referenced an NCN agency number that has an illegal entry in its data file.

“BAD TERMINAL ID” – The terminal ID has been improperly entered in the terminal.

“UNDEF RULE SET” – The terminal ID references a rule set that has not been defined.

“SERVICE CUT OFF” – All NCN transaction service has been terminated

Reason: Velocity Messages

The following messages are "velocity" messages. Messages with DAY refer to daily limits, while the ones with WIN refer to "window" limits where the "window" is from 1 to 14 days, as selected by the merchant.

LOC in a message means that the limit was exceeded when check transactions from only that store location were considered.

GRP in a message means that the limit was exceeded when check transactions from a group of related stores were considered.

ALL in a message means that the limit was exceeded when check transactions from anywhere were considered.

Multiple “velocity” messages can occur. However, within each of the three message groups shown below, only one is output, even if more than one limit was exceeded. The priority is given first to LOC (local site) limits, then to GRP (group of stores) limits, and finally to ALL (data from everywhere utilized).

Table 15-8. Velocity Messages

Message	Description
“DAY LOC/NCHKS=%d” “DAY GRP/NCHKS=%d” “DAY ALL/NCHKS=%d”	This reports that a number of checks limit has been exceeded for the day.
“DAY LOC/AMT=%d” “DAY GRP/AMT=%d” “DAY ALL/AMT=%d”	This reports that the cumulative face amount of check has been exceeded for the day.
“DAY LOC/CASH=%d” “DAY GRP/CASH=%d” “DAY ALL/CASH=%d”	This reports that the cumulative of cash returned from checks has been exceeded for the day.
“WIN LOC/NCHKS=%d” “WIN GRP/NCHKS=%d” “WIN ALL/NCHKS=%d”	This reports that a number of checks limit has been exceeded for the time window.
“WIN LOC/AMT=%d” “WIN GRP/AMT=%d” “WIN ALL/AMT=%d”	This reports that the cumulative face amount of checks has been exceeded for the time window.
“WIN LOC/CASH=%d” “WIN GRP/CASH=%d” “WIN ALL/CASH=%d”	This reports that the cumulative of cash returned from checks has been exceeded for the time window.

Reason: Unpaid Item Messages

Table 15-9. Unpaid Item Messages

Message	Description
"%2d UNPAIDS (LOC)" "%2d UNPAIDS (GRP)" "%2d UNPAIDS (ALL)"	One of these three messages appears if a number of unpaids limit has been exceeded. LOC has priority over GRP. GRP has priority over ALL.
"UNPAID AMT=%5d"	This message always follows the above messages and gives the cumulative amount of the outstanding unpaid items reported in the previous message.

Reason: Individual Check Transaction Limit Exceeded Messages

Table 15-10. Transaction Exceeded Limit Messages

Message	Description
"CHECK TOO LARGE"	The face amount of the check is greater than the limit imposed by the merchant.
"TOO MUCH CASH'	The amount of cash returned with the purchase exceeds the limit imposed by the merchant. This message only appears if both sale and check amount are included in the request packet and cash back limits have been imposed by the merchant.

Reason: Account Problem Messages

Table 15-11. Account Problem Messages

Message	Description
"OUT OF AREA ACCT"	The federal reserve area of the check was not in the list of areas the merchant has specified as acceptable.
"BANK STOP"	Bank has stopped account (probably closed).
"CUSTOMER STOP"	The account owner has requested that transactions on this account be stopped. This is likely because checks have been lost.
"STORE STOP"	The merchant has requested that all checks with this account be stopped.
"AGENCY STOP"	The collection agency has requested that all checks with this account be stopped.
"STLN/FRGD"	Someone has reported that checks with this account have been stolen or forged.

Table 15-11. Account Problem Messages

Message	Description
“CHECK STOPPED”	The check sequence number matches a range stopped by the account owner (used in the case of lost checks).
“YOUNG ACCOUNT”	The rule set has specified that previously unknown MICR accounts be placed in a “new” category with alternate limits applied. This message indicates that the account is still in that “new” period.

REASON: ID PROBLEM MESSAGES

The following messages appear only if an ID was in the request packet.

Table 15-12. ID Problem Messages

Message	Description
“ERROR IN ID”	There was a format error in the id.
“ID IS FLAGGED”	The ID is associated with a checking account that has a problem or the ID has been flagged by the merchant or system operator as one that should not be accepted.
“UNKNOWN ID”	The ID keyed could not be found in the database. This message appears only if double entry of ids was selected in the tender sequence options.

Reason: Payroll Check Messages

Table 15-13. Payroll Check Messages

Message	Description
“PAYROLL NEEDS ID”	The request packet did not include an ID, which is a requirement to process a payroll check verification request.
“NO PAYROLL CHKS”	The maximum amount of a payroll check was set to zero in the rule set to indicate that this merchant does not cash payroll checks.
“PAY CHK TOO BIG”	The merchant set limit on payroll checks has been exceeded.
“DUPLICATE CHECK”	This payroll check has been presented before for cashing.
“NUM PAYCHKS=%d”	The rule set limit on the number of payroll checks that can be cashed on a given ID in a given period of time has been exceeded.
“AMT PAYCHKS=%ld”	The rule set limit on the cumulative face amount of payroll checks has been exceeded.
“NOT PAYROLL ACCT”	The account is not an authorized payroll account and the rule set requires it to be.
“ID NO PYRL AUTH”	The ID has not been authorized for cashing payroll checks at a specific location and the rule set requires this authorization.

Authorization Messages

These messages appear only when a manager is requesting the approval of either an ID or a micr account for payroll check verifications.

Table 15-14. Authorization Messages

Message	Description
“ID AUTHORIZED”	Indicates that the ID is now authorized for use with payroll checks.

Table 15-14. Authorization Messages (Cont.)

Message	Description
"NO ROOM FOR AUTH"	Indicates that the ID could not be authorized because there was insufficient room in the database. There is room for an ID to hold 10 authorizations.
"ACCOUNT AUTHED"	Indicates that the MICR account is now authorized as a payroll account.
"INVALID PASSWORD"	The manager password provided in the request packet does not match that specified in the rule set.
"ID IS NEEDED"	There was no ID included in the request packet.

Examples

<STX> GOOD MERCHANT AUTH NUM 123-456<ETX><LRC>

The above shows a response packet to the store GOOD MERCHANT when the check verification resulted in an approval.

<STX> GOOD MERCHANT MANAGER NEEDED DAY LOC/NCHKS=3<ETX> <LRC>

The above shows a response packet to the store GOOD MERCHANT when a velocity limit was exceeded. In this case the merchant has asked that velocity limits exceeded should be treated as a "warning", hence the MANAGER NEEDED message.

<STX>LOCATION 88734 DECLINE CHECK 2 UNPAIDS (LOC)UNPAID AMT= 376 BANK STOP PHN 800-555-1212 SUPER COLLECT <ETX><LRC>

The above shows a response packet to the store identified only as LOCATION 88734 with a "decline" result from the verification request with 3 messages appended. The unpaid checks are held by the SUPER COLLECT agency. They can be reached by phoning 800-555-1212

Index

T

U

V

W

X

Y

Z