



OTCnetSM
Deposits Made Simple

Chapter 10. Appendix

OTCnet Participant User Guide

(This page left intentionally blank)

TABLE OF CONTENTS

Audience, Overview and Appendixes	iii
Audience	iii
Overview	iii
Appendixes	iv
Appendix A. Administrative Notes	1
Appendix B. Password Requirements	3
Password Assistance	3
Appendix C. Image Quality.....	4
Appendix D. Central Image Research (CIRA) Query.....	5
Appendix E. CIRA CSV File Overview	6
Appendix F. Master Verification Database (MVD)	12
Appendix G. Representment.....	13
Appendix H. Equipment Returns	14
Appendix I. OTCnet Check Capture Codes.....	15
ACH Return Reason Codes	15
Check 21 Return Codes	18
Transaction Status Code Monitoring	19
OTCnet Processing Forward Files.....	20
OTCnet Returns	20
Appendix J. OTCnet Security	22
Purpose.....	22
What is PII?.....	22
Access Control.....	22
Risk Assessment.....	23
Personnel Security and Procedures	24
Physical and Environmental Protection	25
Contingency Planning	27
Configuration Management	29
System Maintenance.....	30
System and Information Integrity	31
Media Protection	32
Incident Response	34
Awareness and Training.....	35
Summary	37
Glossary.....	38
Index.....	55

LIST OF TABLES

Table 1: File layout of CSV Report.....	8
Table 2: Sample file layout.....	10
Table 3. ACH Return Reason Codes	15
Table 4. Check 21 Return Codes	18
Table 5. Transaction Status Codes	19

LIST OF FIGURES

Figure 1. Poor Image Quality	4
Figure 2. Good Image Quality	4
Figure 3. Image Quality Failed Message.....	4

Figure 4. CIRA Query Image..... 5
Figure 5. Manage Verification Tab 12
Figure 6. Transaction Status Codes 13

Audience, Overview and Appendixes

Audience

The intended audience for the *Appendix Participant User Guide* includes the following:

- Primary Local Security Administrator
- Check Capture Administrator
- Check Capture Operator
- Check Capture Lead Operator
- Check Capture Supervisor
- MVD Editor
- MVD Viewer
- CIRA Viewer

Overview

Welcome to the *Appendix*. In this chapter, you will learn:

- About administrative detail for cost, paperwork, policy, training and customer service
- About password requirements
- How to resolve check Image quality
- How to query within the Central Image Research Archive (CIRA)
- About the CIRA CSV File
- About the Master Verification Database (MVD)
- How to establish check representments
- Procedure for returning equipment
- About check capture return codes
- Guidance for OTCnet Security

Appendixes

This chapter is organized by the following appendixes:

- Appendix A. Administrative Notes
- Appendix B. Password Requirements
- Appendix C. Image Quality
- Appendix D. Central Image Research Archive (CIRA) Query
- Appendix E. CIRA CSV File Overview
- Appendix F. Master Verification Database (MVD)
- Appendix G. Representments
- Appendix H. Equipment Returns
- Appendix I. OTCnet Check Capture Return Codes
- Appendix J. OTCnet Security

Appendix A. Administrative Notes

Cost

The Agency's cost for participating in the program is limited to the purchase of hardware. Scanners, scanner cables and USB Flash drives can either be purchased through a vendor of the Agency's choice. The RDM check scanner model supported is the EC7000i or the Panini My Vision Batch scanner models X-30, X-60, or X-90. Older scanner models (RDM EC5000i, EC6000i) are supported but may not be available for purchase. All other computer hardware is purchased through another vendor or by contacting an OTCnet Deployment Specialist. The Treasury/FMS pays all other fees associated with the program so there are no hidden software purchase costs or transaction fees.

Minimal Paperwork

Agencies need to submit a signed Agency Agreement AA, Agency Participation Agreement (APA), an Agency Site Profile (ASP) for each endpoint, and an interagency agreement if purchasing hardware using IPAC. Once agreements are signed and received, the Agency can be up and running within 2-4 weeks.

Endpoint Policy

An endpoint's policy helps automate an Agency's check cashing/collection policy. The endpoint's policy is based upon the agency's overall program or policy to ensure a consistent application of an Agency-wide check verification including returned reason codes, suspension periods, and the inclusion of expired items. As part of the Agency's participation in OTCnet, the agency provides the Treasury OTC Support Center their check collection policy via the ASP.

The endpoint's policy is established during the set-up of a endpoint in the MVD system. Treasury OTC Support Center administers the set-up of all endpoints based on the Agency's and the endpoint's ASP. Treasury OTC Support Center administers all edits or modifications to an endpoint, including the endpoint's policy.

OTCnet Endpoint Group Management

The MVD restricts the display of data based on the endpoint of the user. A user only sees records which are associated with OTC Endpoints at or below the user's OTC Endpoint in the hierarchy or at endpoints specified in the OTCnet Endpoint Group. Depending on the type of data being requested, different rules apply, as appropriate.

User Training

The program offers comprehensive Web-based Training (WBT), Participant User Guides, and optional Instructor-led Training. It is recommended that before using OTCnet, you access the WBT and Participant User Guides to the fullest extent before contacting your Treasury OTC Support Center Deployment Specialist who will work with individuals to determine training type and schedule. To get the most out of the training session, it should be scheduled within two weeks of the Agency's conversion date.

Customer Support Hours

Customer support is available 24 hours a day, 7 days a week. All OTCnet related inquiries should be directed to the Treasury OTC Support Center at (866)945-7920, or 302-324-6442, or military DSN at 510-428-6824, option 1, option 2, option 4, or via email at FMS.OTCChannel@citi.com.

Look up Phone Numbers for Financial Institutions

To find more information including phone numbers and email addresses please go to www.fededirectory.frb.org.

Contact the Treasury OTC Support Center at (866)945-7920, or 302-324-6442, or military DSN at 510-428-6824, option 1, option 2, option 4 or via email at FMS.OTCChannel@citi.com

Appendix B. Password Requirements

Password Assistance

Password requirements are implemented as a security measure. To access OTCnet for the first time, you will need to establish a password. Additionally, every 90 days, you will be required to change your password.

- Passwords must be at least 8 characters in length, and have a maximum of 20 characters
- Passwords must contain at least one upper case letter (A-Z) and one lower case letter (a-z)
- Passwords must contain at least one number (0-9), or one special character such as #, \$ or @
- Password cannot be the word 'password' and cannot be the same as the user's login
- Passwords are case-sensitive
- Passwords must be changed upon the first use when a temporary password is assigned by a user with access to the ITIM Provisioning system (e.g. PLSA and LSA)
- Passwords must be unique outside the previous ten passwords for a user
- Passwords must not have been used in the last 10 days
- Passwords will expire every 90 calendar days
- Passwords must not be shared with other users or put in a written, unsecured form
- Must not be a word in a language, slang, dialect, or jargon
- Must not be related to personal identity, history, environment, or other personal associations
- Passwords must be entered twice for verification on the user's initial login and when a user changes their password
- Single Sign On (OTCnet login window) will suspend a user's access to the system after 3 unsuccessful login attempts. See the Password Reset/Account Lock section below
- The OTCnet system settings default is set to 3 unsuccessful login attempts before suspension and cannot be customized

Appendix C. Image Quality

The scanner functionality has a feature that checks for the image quality of every check scanned. Agencies can, however, choose to override a poor image in hopes that it will process anyway. The following examples are of a poor image scan and an image of good quality). Agencies should be aware that overriding a poor image may result in a returned item, depending upon the paying financial institution. Figure 1 below illustrates a poor quality image while Figure 2 below is a demonstration of a good quality image. Figure 3 shows a Image Quality Failed message.

Figure 1. Poor Image Quality

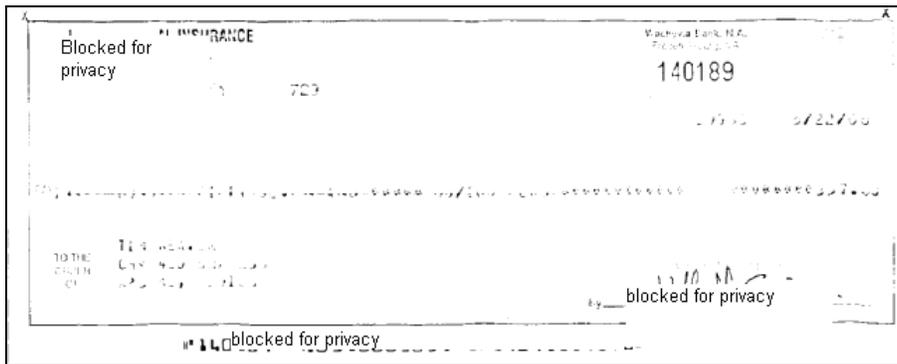


Figure 2. Good Image Quality

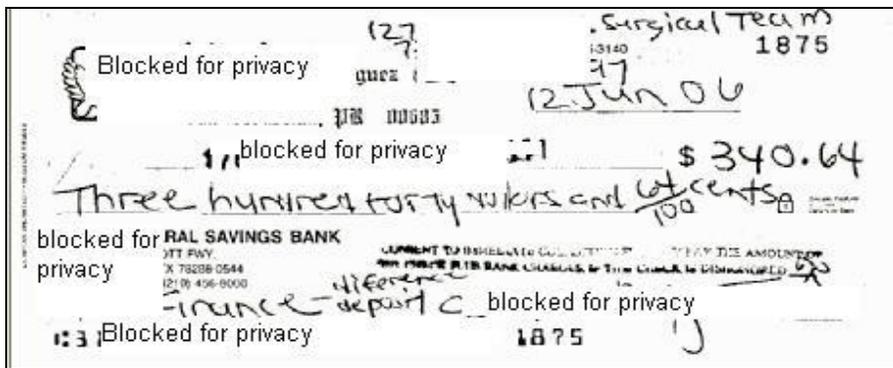
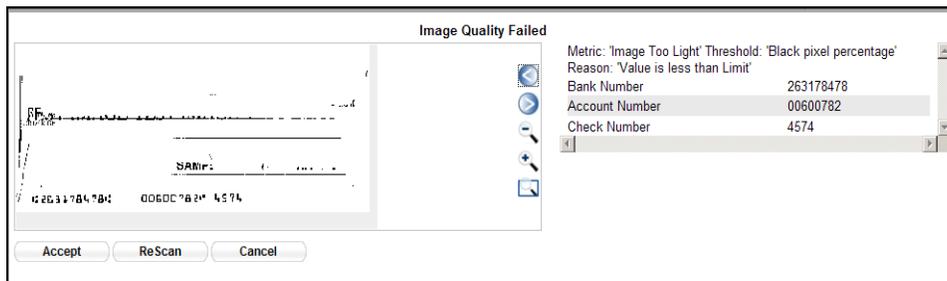


Figure 3. Image Quality Failed Message



Appendix D. Central Image Research (CIRA) Query

The Central Image Research Archive (CIRA) (see Figure 4 below) is the central database where all check images are stored for seven years after the initial scan and processing in OTCnet.

Figure 4. CIRA Query Image

CIRA Query
Enter search criteria for the CIRA Item(s) you would like to view.
* Denotes required fields.

Search Criteria

OTC Endpoint: *
ALL

Include Subordinates

Form Name:
UDF_TEST1

Deploy Date:
2010-06-09 10:06:43.0 | 1000

User Defined Fields:

ProgramCode:
ReferenceTransactionCode:
Description:
CheckDate:
Account:
Bank Routing Number:
IRN:
Check Number:
Check Amount:
Equal to

Settlement Status:
ALL

5515/Debit Voucher Number:
215/Deposit Ticket Number:
Cashier ID:
Batch ID:

Received Date:
From
To

Check Capture Date:
From
To

Settlement Date:
From
To

Return Settlement Date:
From
To

Cancel Clear Search

As a CIRA Viewer, MVD Viewer and MVD Editor, you can utilize the CIRA query function of OTCnet to search for and locate checks. Each CIRA CSV consists of multiple lines and is defined as follows:

- Each line is terminated by a carriage return followed by a new line (0D0A)
- The first five lines always exist. The CSV data begins on line 6
- The file is terminated by an empty line followed by 0D0A

Appendix E. CIRA CSV File Overview

Introduction

As an OTCnet user, you may need to download the CIRA CSV file. This user guide contains all of the fields available in the CIRA CSV report in OTCnet. The CSV report provides input data for downstream systems, and provides OTCnet users with the ability to download item information in a standard format.

OTCnet Updates

Please note: For OTCnet, two updates have been made to the file format:

1. The column which was titled “Location” in PCC OTC will now be called “OTC Endpoint.” This column will now be populated with the OTC Endpoint short name.
2. The column which was titled “Check Type” in PCC OTC will now be called “Item Type.”
3. Two additional columns will be added to the CSV report generated in OTCnet.
 - a. A column entitled ‘ALC+2.’ The ‘ALC+2’ column will be automatically populated with the ALC+2 that was selected for the submitted item*
 - b. A column entitled ‘Return Settlement Date.’ The ‘Return Settlement Date’ column will be automatically populated with the effective date of settlement of the returned check item

* Endpoints that were migrated over from PCC OTC may contain the same value for ‘OTC Endpoint’ and ‘ALC+2’. This is not an error and will not interfere with the data generated by this report.

Layout

The CIRA CSV report consists of multiple lines and is defined as follows:

- Each line is terminated by a carriage return followed by a new line (0D0A)
- The first 5 lines always exist. The agency’s item data begins on line 6
- The file is terminated by an empty line followed by 0D0A

Available Fields

All possible fields found in the report are as follows*:

- IRN
- OTC ENDPOINT
- ALC +2
- CAPTURE DATE
- RECEIVE DATE
- BANK ROUTING NUMBER

- CHECK NUMBER
- ACCOUNT
- AMOUNT
- CASHIER ID
- ITEM TYPE
- PROCESSING METHOD
- BATCHID
- SETTLEMENT DATE
- RETURN SETTLEMENT DATE
- DEBIT VOUCHER NUMBER
- DEPOSIT TICKET NUMBER
- User Field 1
- User Field 2
- User Field 3
- User Field 4
- User Field 5
- User Field 6
- User Field 7
- User Field 8
- User Field 9
- User Field 10
- User Field 11
- User Field 12
- User Field 13
- User Field 14
- User Field 15
- User Field 16
- User Field 17
- User Field 18
- User Field 19
- User Field 20
- User Field 21
- User Field 22
- User Field 23
- User Field 24

* Please note: Some of the labels in the CSV report appear slightly differently than they do in other part of OTCnet. This will not impact the download.

Location = OTC Endpoint

User Field = User Defined Field

Processing Mode = Processing Method (future)

Check Type = Item Type (future)

File Layout

This section defines the size of all fields and the order in which the fields are laid out within the file:

Table 1: File layout of CSV Report

Line Number	Field Number	Name	Type	Format/Sample	Description
1		Report Title	String	<i>CSV Agency Detailed Item Report</i>	Report Title Constant
2		Date/Time	String	Thu May 05 12:27:53 EDT 2005	Date that the report was executed
3		Total Amount	String	<i>TOTAL AMOUNT</i> :	Constant String
		Total Amount Value	Float	39594.43	Total dollar amount of the items queried
4		Total number of items	String	TOTAL NUMBER OF ITEMS :	Constant String
		Total number of items value	Number	81	Number of items queried
5		<i>IRN</i>	String	IRN	Constant String column header, value of the IRN
		OTC Endpoint	String	LOCATION NAME	Constant String column header, ALC+2
		ALC +2	Number	ALC +2	Number of ALC +2
		CAPTURE DATE	String	CAPTURE DATE	Constant String column header, Time the image and data was originally captured
		RECEIVE DATE	String	RECEIVE DATE	Constant String column header, Time the data was processed by PCC OTC
		ROUTING TRANSIT NUMBER	String	ROUTING TRANSIT NUMBER	Constant String column header, Routing number parsed from RAW MICR
		CHECK NUMBER	String	CHECK NUMBER	Constant String column header, Account number parsed from RAW MICR
		ACCOUNT	String	ACCOUNT	Constant String column header, Check number parsed from RAW MICR
		AMOUNT	String	CHECK AMOUNT	Constant String column header, Amount of the payment
		CASHIER ID	String	<i>CASHIER ID</i>	Constant String column header, Value provided by ALC+2 for the operator id
		CHECK TYPE	String	CHECK TYPE	Constant String column header, Check Type – either “Personal” or “Non-Personal”

Line Number	Field Number	Name	Type	Format/Sample	Description
		PROCESSING METHOD	String	PROCESSING MODE	Constant String column header, Processing Mode – 3 options “Not Present”, “Present” or “Back Office”
		BATCH ID	String	Batch ID	Constant String column header. Batch containing the IRN
		SETTLEMENT DATE	String	Settlement Date	Constant String column header. Settlement Date
		RETURN SETTLEMENT DATE	String	Return Settlement Date	Constant String column header. Return Settlement Date
		DEBIT VOUCHER NUMBER	String	DEBIT VOUCHER NUMBER	Constant String column header. Debit Voucher Number
		DEPOSIT TICKET NUMBER	String	DEPOSIT TICKET NUMBER	Constant String column header. Deposit Ticker Number
		User Field 1	String	User Defined Field 1	Constant String column header
		User Field 2	String	User Defined Field 2	Constant String column header
		User Field 3	String	User Defined Field 3	Constant String column header
		User Field 4	String	User Defined Field 4	Constant String column header
		User Field 5	String	User Defined Field 5	Constant String column header
		User Field 6	String	User Defined Field 6	Constant String column header
		User Field 7	String	User Defined Field 7	Constant String column header
		User Field 8	String	User Defined Field 8	Constant String column header
		User Field 9	String	User Defined Field 9	Constant String column header
		User Field 10	String	User Defined Field 10	Constant String column header
		User Field 11	String	User Defined Field 11	Constant String column header
		User Field 12	String	User Defined Field 12	Constant String column header
		User Field 13	String	User Defined Field 13	Constant String column header
		User Field 14	String	User Defined Field 14	Constant String column header
		User Field 15	String	User Defined Field 15	Constant String column header
		User Field 16	String	User Defined Field 16	Constant String column header
		User Field 17	String	User Defined Field 17	Constant String column header

Line Number	Field Number	Name	Type	Format/Sample	Description
		User Field 18	String	User Defined Field 18	Constant String column header
		User Field 19	String	User Defined Field 19	Constant String column header
		User Field 20	String	User Defined Field 20	Constant String column header
		User Field 21	String	User Defined Field 21	Constant String column header
		User Field 22	String	User Defined Field 22	Constant String column header
		User Field 23	String	User Defined Field 23	Constant String column header
		User Field 24	String	User Defined Field 24	Constant String column header

Sample File Layout

Following is a sample file layout starting on line 6 is displayed below.

Table 2: Sample file layout

Field Number	Name	Type	Sample value
	IRN	String	111201500244600000608
	OTC Endpoint	String	0000633502
	ALC +2	Number	0000347601
	Capture Date	Date/Time	2002-07-19 14:11:14
	Receive Date	Date/Time	2002-07-22 07:31:19
	BANK ROUTING NUMBER	String	251480576
	CHECK NUMBER	String	787910415647
	ACCOUNT	String	4114784
	AMOUNT	String	38.81
	CASHIER ID	String	Patrick
	ITEM TYPE	String	Personal Non-Personal
	PROCESSING METHOD	String	Customer Not Present Customer Present Back Office
	BATCH ID	String	FF1E9FE2-FB22-4353-A27A-06C86FC3D2AA
	SETTLEMENT DATE		2002-08-22 07:43:10
	RETURN SETTLEMENT DATE		7/30/2010
	DEBIT VOUCHER NUMBER	String	24
	DEPOSIT TICKET NUMBER	String	8

Field Number	Name	Type	Sample value
	User Field 1	String	User Defined Field 1
	User Field 2	String	User Defined Field 2
	User Field 3	String	User Defined Field 3
	User Field 4	String	User Defined Field 4
	User Field 5	String	User Defined Field 5
	User Field 6	String	User Defined Field 6
	User Field 7	String	User Defined Field 7
	User Field 8	String	User Defined Field 8
	User Field 9	String	User Defined Field 9
	User Field 10	String	User Defined Field 10
	User Field 11	String	User Defined Field 11
	User Field 12	String	User Defined Field 12
	User Field 13	String	User Defined Field 13
	User Field 14	String	User Defined Field 14
	User Field 15	String	User Defined Field 15
	User Field 16	String	User Defined Field 16
	User Field 17	String	User Defined Field 17
	User Field 18	String	User Defined Field 18
	User Field 19	String	User Defined Field 19
	User Field 20	String	User Defined Field 20
	User Field 21	String	User Defined Field 21
	User Field 22	String	User Defined Field 22
	User Field 23	String	User Defined Field 23
	User Field 24	String	User Defined Field 24

CSV File Sample

The text below shows a sample of the CSV file report:

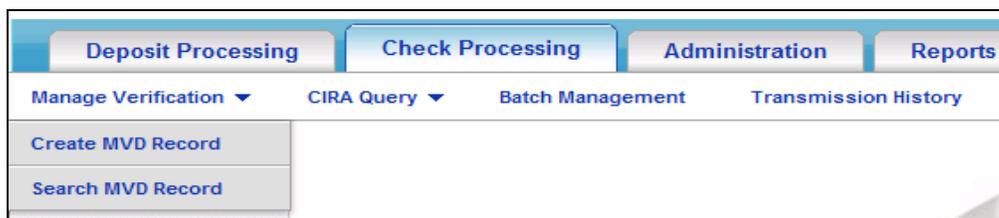
```

"CSV Agency Detailed Item Report"
"Thu Oct 06 11:17:23 EDT 2011"
"TOTAL AMOUNT : ","38509.00"
"TOTAL NUMBER OF ITEMS : ","2"
"IRN","OTC ENDPOINT","ALC + 2","CAPTURE DATE","RECEIVE DATE","TRANSIT
NUMBER","CHECK NUMBER","ACCOUNT","AMOUNT","CASHIER ID","ITEM
TYPE","PROCESSING METHOD","BATCH ID","SETTLEMENT DATE","RETURN SETTLEMENT
DATE","DEBIT VOUCHER NUMBER","DEPOSIT TICKET NUMBER","User Field 1","User Field
2","User Field 3","User Field 4","User Field 5","User Field 6","User Field 7","User Field 8","User
Field 9","User Field 10","User Field 11","User Field 12","User Field 13","User Field 14","User Field
15","User Field 16","User Field 17","User Field 18","User Field 19","User Field 20","User Field
21","User Field 22","User Field 23","User Field 24"
"13154124770015865281","DG1","1000000001","2011-09-07 12:21:17","2011-09-07
12:20:59","044000024","111","111111","11.11","otcqef50","Non Personal","Customer
Present","1C111D1E-C111-1111-BC11-1CD11111ADBA","2011-09-12
00:00:00","null","null","000973","345345333","null","null","null","null","null","null","null","n
ull","null","null","null","null","null","null","null","null","null","null","null","null"
"13154267000015865281","DG1","1000000001","2011-09-07 16:18:20","2011-09-07
16:18:07","073903503","00000013","1111","11.11","otcqef50","Personal","Customer
Present","1C111D1E-C111-1111-BC11-1CD11111ADBA","2011-09-14
00:00:00","null","null","000973","234234223","null","null","null","null","null","null","null","n
ull","null","null","null","null","null","null","null","null","null","null","null","null","null"
    
```

Appendix F. Master Verification Database (MVD)

The Master Verification Database (MVD) (see Figure 5 below) provides the information to ensure a presented check is acceptable. It aids the Agency in determining the history of a particular check writer, managed by a MVD Editor.

Figure 5. Manage Verification Tab



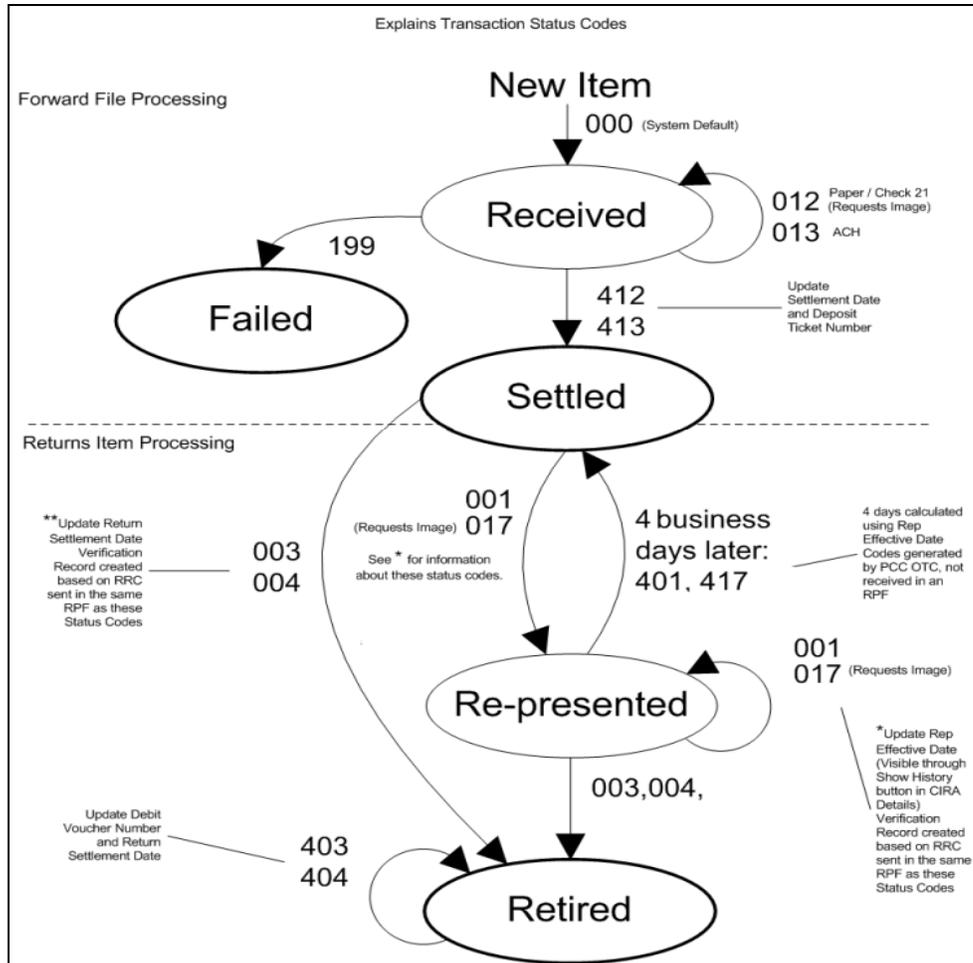
The verification database is an optional online database that maintains the agency hierarchy check cashing policy, dishonored check information, and manually entered blocked items based on an Agency's policy.

The MVD restricts the display of data based on the endpoint of the user. A user only sees records which are associated with endpoints at or below the user's endpoint in the hierarchy or at endpoints specified in the OTCnet Endpoint Group. Depending on the type of data being requested, different rules apply, as appropriate. For more information, refer to the Master Verification Database (MVD) section of the MVD User Guide.

Appendix G. Representation

Figure 6 below illustrates the Representation flow for checks that are not accepted the first time.

Figure 6. Transaction Status Codes



Appendix H. Equipment Returns

If there are problems with the OTCnet equipment that was purchased from the Treasury OTC Support Center, contact the Treasury OTC Support Center. A staff member verifies the warranty and if needed, the dollar valuation on the following pieces of equipment: Scanners and Yes/No keypads. Otherwise, if the OTCnet equipment was purchased directly from a vendor, please contact the vendor for warranty and/or repair information.

Please contact the OTCnet Customer Service at 866- 945-7920, or 302-324-6442, or military DSN at 510-428-6824, option 1, option 2, option 4 or via email at FMSotcdeployment@citi.com.

If the warranty is active, the representative will provide the mailing address for the hardware shipping.

Equipment should be returned either by certified mail with return receipt, or via FedEx. When using either method, please purchase insurance for the equipment's full dollar value. Please include a note explaining the reason for return, i.e., describing the damaged or defective equipment.

Note: In the event that the warranty has expired on the Check Capture equipment, please call the Vendor Point-of-Contact for further instructions or discuss the possible purchase of new equipment with your Deployment Specialist.

Appendix I. OTCnet Check Capture Codes

ACH Return Reason Codes

These return codes are used when an item that has been converted to an ACH entry is returned. They are used by the paying institution from where the item is drawn, when they return an ACH transaction that was processed by Check Capture. The return reason code for a particular item is listed on the Debit Voucher Report (SF5515) as seen in Table 1 below.

Table 3. ACH Return Reason Codes

Return Reason Code (RRC)	Description
R01	Insufficient funds
R02	Account closed
R03	No account/unable to locate account
R04	Invalid account number
R05	Unauthorized debit to consumer account using corporate SEC Code
R06	Returned per Originating Depository Financial Institution's request
R07	Authorization revoked by customer
R08	Payment stopped
R09	Uncollected funds
R10	Customer advises not authorized
R11	Check truncation entry return
R12	Branch sold to another Depository Financial Institution
R13	RDFI not qualified to participate a (ACH operator initiated)
R14	Representative Payee (account holder) deceased or unable to continue in that capacity
R15	Beneficiary or account holder (other than a representative payee) deceased
R16	Account frozen
R17	File record edit criteria
R18	Improper effective entry date (ACH operator initiated)

R19	Amount field error (ACH operator initiated)
R20	Non-transaction account
R21	Invalid company identification
R22	Invalid individual ID number
R23	Credit entry refused by receiver
R24	Duplicate entry
R25	Addenda Error
R26	Mandatory Field Error
R27	Trace Number Error
R28	Routing Number Check Digit Error
R29	Corporate customer advises not authorized (CCD)
R30	RDFI Not Participant in Check Truncation Program
R31	Permissible return entry (CCD)
R32	RDFI Non-Settlement
R33	Return of XCK Entry
R34	Limited Participation DFI
R35	Return of Improper Debit Entry
R36	Return of Improper Credit Entry
R37	Source document presented for payment (adjustment entries) (ARC)
R38	Stop payment on source document (adjustment entries)
R39	Improper Source Document
R40	Non Participant in ENR Program
R41	Invalid Transaction Code (ENR only)
R42	Routing Number/Check Digit Error
R43	Invalid DFI Account Number
R44	Invalid Individual ID Number
R45	Invalid Individual Name

R46	Invalid Representative Payee Indicator
R47	Duplicate Enrollment
R50	State Law Prohibits Truncated Checks
R51	Notice not provided/Signature not authentic/ Item altered/Ineligible for conversion
R52	Stop Pay on Item
R53	Item and ACH Entry Presented for Payment
R61	Misrouted Return
R67	Duplicate Return
R68	Untimely Return
R69	Field Errors
R70	Permissible Return Entry Not Accepted
R71	Misrouted Dishonor Return
R72	Untimely Dishonored Return
R73	Timely Original Return
R74	Corrected Return
R75	Original Return not a Duplicate
R76	No Errors Found
R80	Cross-Border Payment Coding Error
R81	Non-Participant in Cross-Border Program
R82	Invalid Foreign Receiving DFI Identification
R83	Foreign Receiving DFI Unable to Settle
R84	Entry Not Processed by OGO (Originating Gateway Operator)

Check 21 Return Codes

These return reason codes are used by the paying Financial Institution from where the item was drawn, when a Check 21 transaction is returned. The returned item was originally processed by OTCnet the return reason code for a particular item is listed on the Debit Voucher Report (SF5515). See Table 2 below for list of Check 21 Return Codes.

Table 4. Check 21 Return Codes

Return Code	Description
A	Not Sufficient Funds
B	Uncollected Funds Hold
C	Stop Payment
D	Closed Account
E	Unable to Locate Account
F	Frozen/Blocked Account
G	Stale Dated
H	Post Dated
I	Endorsement Missing
J	Endorsement Irregular
K	Signature(s) Missing
L	Signature(s) Irregular
M	Non Cash Item
N	Altered/Fictitious Item
O	Unable to Process
P	Item Exceeded Dollar Limit
Q	Not Authorized
R	Branch/Account Sold
S	Refer to Maker
T	Stop Payment Suspect
U	Unusable Image

V	Image Fails Security Check
W	Cannot Determine Account
Y	Duplicate Presentment
Z	Forgery - An affidavit shall be available upon request to the OTCnet database

Items that are processed via Check 21 include all non personal items. Personal items may also be processed via Check 21.

Transaction Status Code Monitoring

This section of Appendix H describes how transaction status codes are applied in OTCnet during forward file and return processing. This section also lists codes that are used and their corresponding descriptions. See the Transaction Status Codes listed in Table 3 below.

Table 5. Transaction Status Codes

Transaction Status Code	Description	System Action
000	Received	In-Process status assigned by Treasury/FMS.
199	Failed	Change status to Failed.
012	Paper Draft	Create an image request.
013	ACH Origination	Does nothing, ignored by system.
412	Paper Draft	Change status to Settled.
413	ACH Origination	Record the Settlement Date and the Deposit Ticket Number.
001	ACH Redeposit	Change status to Represented.
017	Paper Redeposit Draft	Change to status to Represented.
003	ACH Retire	Change status to Retired.
004	Paper Retire	Return settlement date is updated
401	ACH Redeposit	Change status to Settled.
417	Paper Redeposit Draft	

403	ACH Retire	Change status to Retired.
404	Paper Retire	Record the Debit Voucher number. Update Return Settlement Date.

OTCnet Processing Forward Files

- OTCnet forwards the batches for processing to the back end processor to be settled
- The back-end system decides how to settle the items based on the check type of either:
 - Corporate check
 - Consumer POP (customer present)
 - Consumer ARC (customer not present)
 - Back Office – BOC
- Items can be settled as either:
 - ACH – these items are settled electronically and do not require an image
 - Check 21 – these items are settled electronically using a substitute check. They require an image before settlement can occur
 - Paper – these items use the physical check for settlement.
- RPF file is sent. Codes 199, 012 and 013 are sent in this RPF
- Codes 012 and 013 items do not have their status updated but for 012's, an image request is created. 013=ACH origination; 012=Paper Draft.
- 199's are updated with the status code of 'failed'
- A settlement RPF (Return Processing File) is sent the morning after the files were uploaded, usually around 8:30am. Codes 412, 413, and 199 are sent to OTCnet. Items receiving a 412 and 413 code are updated with the status of 'settled'. These items receive a settlement date and a deposit ticket number
- Items receiving a 199 code are failed items and do not receive a settlement date or deposit ticket number
- Settled items are included in the Deposit Ticket Report for that settlement day
- Settlement status is a prediction only – the back-end system will assume that all money can be collected for the items sent in a forward file. This is the end of forward file processing.

OTCnet Returns

- Once settlement occurs, an item can be returned for various reasons, i.e., insufficient funds, account closed, etc.
- A return RPF is sent. This file contains the return reason code. All status codes in the return RPF begin with a zero which indicates 'accepted'. It is NOT in it's final state

- Items with codes 001, 002, 017, 018, & 019 are updated with the status of 'represented' and the date is stored in OTCnet and can be viewed using the CIRA Query 'Show History' button in the 'Rep Effective Date' field.
- If the represented item is not collected within 4 days from the Rep Effective Date, the item status in OTCnet will be updated to a transaction status code of 401 or 417
- An ACH item can usually only be represented twice unless specific arrangements are made. Upon the 3rd representation, the item will be retired in OTCnet. Paper items can only be represented once and will retire in OTCnet upon the 2nd representation. Endpoints can also choose to not have items represent in which case an item would just retire
- Codes 017, update the status code to represented and generate an image request
- Items with 003 and 004 are updated with the status of 'retired' and the return settlement date is updated
- Verification records are created for returned items and can be viewed in the verification Query (based on the endpoints visibility filters)
- A 2nd RPF, the 'return settlement' file is then sent. This file does not contain return reason codes. Transaction status codes in this RPF start with the number 4 which indicates that the item has been completed and is in its final state
- Codes 403, 404 and 409 (refer to Table 1) are already in a retired state so the status remains 'retired'. The return settlement date field in the CIRA Query 'Show History' screen are updated and a debit voucher number is created.

Appendix J. OTCnet Security

Purpose

This section will provide best practices for the OTCnet system that will guide Agencies toward Federal Information Security Management Act (FISMA) compliance. This document outlines points from the *NIST Special Publication 800-53*. Each Agency's internal guidelines should take Treasury security best practices into consideration. Please refer to *NIST Special Publication 800-53* for complete text of the 'Recommended Security Controls for Federal Information Systems'.

What is PII?

Personally Identifiable Information (PII) is information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history. It includes information which can be used to distinguish or trace an individual's identity such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc (*OMB M-06-19 (July 12, 2006)*).

OTCnet batch information contains PII information. It is therefore critical that this data be secured to prevent unauthorized access to this highly sensitive information.

Access Control

Effects on OTCnet

NIST Special Publication 800-53 Guidance

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented access control policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal documented procedures to facilitate the implementation of the access control policy and associated risk assessment controls.

- Agencies must identify authorized users of OTCnet and specify access rights/privileges. Access is granted to OTCnet based on a valid need-to-know/need-to-share that is determined by assigned official duties and satisfying all personnel security criteria and intended system usage. Agencies must monitor and remove unnecessary access when users are terminated or transferred and associated accounts need to be removed, or when a user's access changes.
- Agencies enforce separation of duties through assigned access authorizations by establishing appropriate divisions of responsibility and separates duties as needed, to eliminate conflicts of interest in the responsibilities and duties of individuals who have access to the OTCnet system.

- Agencies employ the concept of least privilege for specific duties.
- Agencies enforce a limit of consecutive invalid access attempts by a user. This limit should be no more than three attempts.
- Agencies must review audit records, i.e., activity logs, of the OTCnet system for inappropriate activities in accordance with organizational procedures. Agencies must investigate any unusual information system-related activities and periodically review change to access authorizations. NIST Special Publication 800-92 provides guidance on computer security log management.

In Summary

- Access to the OTCnet should be given to users at the lowest level available that still allow the user to perform their job duties.
- Review separation of duties for users multiple tasks. Separation of duty can be taken a step further by assigning permission to perform voids, batch close/transmission, and batch input to different individuals.
- Ensure that the maximum number of failed login attempts to the OTCnet computer has not been altered to a number higher than 3.
- Review and certify OTCnet users yearly. FMS performs annual certification of users. Local procedures should be established for performing recertification of OTCnet users on each computer. OTCnet Point of Contacts should print out a listing of users and their associated roles/permissions.

Risk Assessment

NIST Special Publication 800-53 Guidance

Agency develops, disseminates, and periodically reviews/updates:

1. A formal documented risk assessment policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.

Effects on OTCnet

Risk assessment identifies risk through a formal process and makes a conscious decision to accept, mitigate, or avoid that risk. Agencies can request a Business Risk Assessment template that will assist them in their risk assessment of the OTCnet system in their environment. To request the template, contact the Treasury OTC Support Center at (866)945-7920, or 302-324-6442, or military DSN at 510-428-6824, option 1, option 2, option 4 or via email at FMS.OTCChannel@citi.com.

Also, refer to *FIPS Pub 199, Standards for Security Categorization of Federal Information and Information Systems*, which can be used to categorize and measure risk of information and information systems.

Personnel Security and Procedures

NIST Special Publication 800-53 Guidance

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented personnel security policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal documented procedures to facilitate the implementation of the personnel security policy and associated personnel security policy and procedure controls.

Effects on OTCnet

- Assign a risk designation to all positions and establish screening criteria for individuals filling those positions. (NIST Special Publication 800-12 and 5 CFR 731.106(a) and Office of Personnel Management policy and guidance).
- Screen individuals requiring access to the OTCnet system and OTCnet information before authorizing access. (5 CFR 731.106(a) and Office of Personnel Management policy, regulations, and guidance; organizational policy, regulations and guidance; FIPS 201 and Special Publication 800-73 and 800-76; and the criteria established for the risk designation of the assigned position)
- Ensures completion of the appropriate access agreements, i.e., Rules of Behavior, Privacy Statement, Accessibility Statement, and all information security access forms for individuals requiring access to OTCnet before authorizing access.
- Establish personnel security requirements for third-party providers, i.e., service bureaus, contractors, and other organizations providing OTCnet information technology services or network management, and monitor the provider to ensure adequate security. (NIST Special Publication 800-35).
- Establish a formal disciplinary process for individuals that blatantly disregard security procedures. The process can be included as part of the general personnel policies and procedures.
- When employment is terminated, or individuals are reassigned or transferred to other positions within the agency, terminate access to the OTCnet system and to OTCnet information ensure the return of all OTCnet related property, i.e., printouts, flash drives used as secondary storage, etc., and ensure that the appropriate personnel have access to official records created by the terminated employee that are stored on the OTCnet system or paper files.

In Summary

- Assign a risk category or designation to all positions associated to the OTCnet system and screen individuals before granting access to the system.
- Make certain users read and understand the OTCnet ‘Rules of Behavior’, ‘Privacy Statement’ and ‘Accessibility Statement’.
- Ensure that the necessary information security forms have been completed (‘OTCnet Security Contact form’ which is used to designate the OTCnet Security Contact(s), and the ‘OTCnet User Access Request spreadsheet’ which is used to request user access to the ELVIS application). Only authorized users can gain access to OTCnet.
- Exiting users should no longer be in possession OTCnet equipment, i.e., access to or possession of the OTCnet computer, USB flash drive, software or printed materials. Make certain that all OTCnet equipment and printed material is available for the new person filling the position by ensuring that the equipment and material has been relinquished by the former employee.
- When an employee quits or changes their position, delete their access to OTCnet.
- Ensure that third-party service providers have adequate security in place with regard to the OTCnet system.
- Establish procedures to follow when an employee fails to follow the security policies and procedures.

Physical and Environmental Protection

NIST Special Publication 800-53 Guidance

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection policy controls.

Agencies should control physical access points (including designated entry/exit points) to facilities containing information systems (except for those areas within the facility that are officially designated as publicly accessible) and verify individual access authorizations before granting access to the facility. The agency also controls access to areas officially designate as publicly accessible, as appropriate, in accordance with the agency’s assessment of risk.

Effects on OTCnet

- Agencies control physical access to all OTCnet equipment including the screen display to prevent unauthorized individuals from observing/viewing the screen's display output.
- Agencies develop and keep current lists of personnel with authorized access to the area containing the OTCnet system. Designated authorized individuals within the agency should review and approve access list at least annually. The agency promptly removes personnel no longer requiring access to the area containing the OTCnet system.
- Agencies control physical access to the OTCnet computer by authenticating visitors before authorizing access to the area that houses the OTCnet system in areas that are not designated as publicly accessible.
- Agencies monitor physical access to the OTCnet system to detect and respond to incidents.
- Agencies protect power equipment and power cabling for the OTCnet system from damage and destruction.
- Agencies provide a short-term, uninterruptible power supply to facilitate an orderly shutdown of the OTCnet system in the event of a primary power source loss. The hardware should be obtained through your internal procurement channels. A long term power supply option should also be considered in the event of an extended loss of the primary power source.
- Agencies control OTCnet system-related items, i.e., hardware, firmware, software, when such items are entering and/or exiting the facility; and maintain appropriate records of those items.
- Individuals within the agency should employ appropriate OTCnet security controls at alternate work sites. (*NIST Special Publication 800-46*).
- Agencies are responsible for securing OTCnet scanners, peripheral equipment, checks, and other sensitive information in locked rooms, locked cabinets, or security containers supported by appropriate key control and other physical security controls.
- To the extent that the operational environment allows, OTCnet scanners and check processing should be done in controlled environments such as steel cages, cashier cages, behind glass windows, and within offices where access to the OTCnet system and peripheral equipment can be physically controlled.

In Summary

- Know who has physical access to the area that houses the OTCnet computer.
- Ensure that unauthorized individuals cannot view the computer screen of the OTCnet computer.
- Ensure that the OTCnet hardware and software is secured, controlled, and monitored when entering or exiting the building.

- If, as in the case of military agencies, a ‘down-range’ environment is necessary, ensure that all security controls are in place to secure the equipment at the alternate work site.
- For military agencies and other agencies operating in remote or field endpoints, deploy appropriate physical security and access controls to limit unauthorized access to and unauthorized disclosure of OTCnet processing areas and information.

Contingency Planning

NIST Special Publication 800-53 Guidance

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented contingency planning policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning policy controls.

The agency develops and implements a contingency plan for the OTCnet system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the agency review and approve the contingency plan and distribute copies of the plan to key contingency personnel (*NIST Special Publication 800-34* provides guidance on contingency planning).

Effects on OTCnet

- Agencies train personnel in their contingency roles and responsibilities with respect to the OTCnet system and provide refresher training.
- Agencies test the contingency plan for the OTCnet system at least on an annual basis to determine the plan’s effectiveness and the agency’s readiness to execute the plan. The test plan results are reviewed by the appropriate officials at the agency who initiate corrective action.
- Agencies review the contingency plan at least annually and revise the plan to address system/organization changes or problems encountered during plan implementation, execution, or testing.
- Agencies identify an alternate storage site and initiates necessary agreements to permit the secured storage of OTCnet backup information which can include storage of backup hardware, i.e., extra scanners, and backup copies of software, etc.
- Agencies identify an alternate processing site and initiates necessary agreements to permit the resumption of the OTCnet system operations for critical mission/business functions within a pre-determined time period, when primary processing capabilities are unavailable. The alternate site should be geographically separated from the primary processing site so as to not be susceptible to the same hazards.

- Agencies identify primary and alternate telecommunications services to support the OTCnet system and initiates necessary agreements to permit the resumption of system operations for critical mission/business functions with a pre-determined timeframe when the primary telecommunications capabilities are unavailable.
- Agencies conduct backups of user-level and system-level OTCnet information and stores backup information at an appropriately secured endpoint. Each agency shall determine the appropriate frequency of these backups. Backup and restoration of this data should also be a part of the contingency plan testing.
- Agencies store backup copies of the operating system and other critical OTCnet software in a separate facility or in a fire-rated container that is not collocated with the operational software.
- Agencies perform backups of the OTCnet hard drive on a regular basis and store the backup in a secured endpoint.
- Agencies employ mechanisms with supporting procedures to allow the OTCnet system to be recovered and reconstituted to the system's original state after a disruption or failure.

In Summary

- Create a contingency plan and keep it current.
- Ensure people are trained to handle a contingency situation.
- Test the contingency plans yearly to ensure that hardware, communication medium, and software is in working order and current.
- Consider having a backup OTCnet computer and OTCnet related hardware, i.e., scanner, secondary storage, etc.
- Consider having OTCnet related hardware and/or software backups also located off premises in a secured endpoint. A backup of the OTCnet hard drive should be performed on a regular basis.
- Extra scanners can be ordered and stored at an alternate site as backups in case of a failure or disruption. For addition information on ordering extra scanners, please contact the Treasury OTC Support Center at (866)945-7920, or 302-324-6442, or military DSN at 510-428-6824, option 1, option 2, option 4.
- In the event of a failure or disruption, scanners can be delivered overnight to endpoints within the 48 contiguous states. Delivery will take longer for areas outside of this zone.
- Consider alternate processing sites.

Configuration Management

NIST Special Publication 800-53 Guidance

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented configuration management policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal, documented procedures to facilitate the implementation of the configuration management policy and associated contingency planning policy controls.

The agency develops, documents, and maintains a current, baseline configuration of the OTCnet system and an inventory of the system's constituent components.

Effects on OTCnet

- Agencies should keep an inventory of the OTCnet hardware and software. This inventory should include manufacturer, type, serial number, version number, and endpoint (physical and logical within the architecture). This inventory should be kept current and changes should be documented.
- Ensure that OTCnet security settings are defaulted to the most restrictive mode and should not be changed.
- Agencies should restrict access to the configuration information to a select few authorized individuals.

In Summary

- Keep a current, documented listing of all of the settings are set to the recommended defaults as follows
- Only the designated POC's (Point of Contact) or security contacts should be allowed access to the OTCnet SAT.
- The activity log should be regularly reviewed for suspicious activity. Evidence or indicators of increased risks to the OTCnet system and associated information must be responded to with more aggressive audit monitoring, more frequent review of audit logs, and the use of additional monitoring tools as appropriate.

System Maintenance

NIST Special Publication 800-53 Guidance

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented system maintenance policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal, documented procedures to facilitate the implementation of the system maintenance policy and associated system maintenance policy controls.

Effects on OTCnet

- The system maintenance policy ensures that the agency schedules, performs, and documents routine preventative and regular maintenance on the OTCnet components in accordance with the manufacturer or vendor specifications and/or agency requirements.
- All maintenance activities are controlled whether the equipment is serviced on site or removed to another endpoint.
- Remove sensitive information from the OTCnet system components (if feasible) when the components must be removed from the facility when repairs are necessary. This can be accomplished by backing up the OTCnet hard drive to another medium such as CDs or an external hard drive then deleting the OTCnet from the computer. When repairs have been complete, the data can then be restored. Secondary storage devices that contain sensitive data, i.e., flash drives, zip disks, CD-ROMs, and smart cards should be removed from the computer prior to servicing and stored in a secure endpoint.
- Agencies approve, control, and monitor the use of maintenance tools used on the OTCnet system, and maintain the tools on an ongoing basis.
- Agencies maintain a list of personnel authorized to perform maintenance on the OTCnet system. Only those authorized personnel should be allowed access to perform maintenance on the system.

In Summary

- Regularly scheduled preventative maintenance should be performed each terminal, i.e., disk optimization tools, virus checking tools, etc., by authorized personnel only. Contact your local IT department for information on the tools authorized for use by your agency.
- If a component needs to be removed for repairs, all sensitive information should be removed. PII may be contained in the form of names, account numbers, social security numbers, etc., within a batch.
- For agencies located in a dusty/sandy environment, OTCnet computer equipment (computers and scanners) should be regularly cleaned with canned air.

System and Information Integrity

NIST Special Publication 800-53 Guidance

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity policy controls.

Effects on OTCnet

- Agencies identify information systems containing proprietary or open source software affected by recently announced software flaws and potential vulnerabilities resulting from those flaws. The agency should promptly install new released security relevant patches, service packs, and hot fixes, and test patches, service packs, and hot fixes for effectiveness and potential side effects on the OTCnet before use. (*NIST Special Publication 800-40* provides guidance on security patch installation)
- Agencies implement malicious code protection on the OTCnet system that includes a capability for automatic updates. Agency employs virus protection mechanisms at critical information system entry and exit points, i.e., firewalls, electronic mail servers, remote-access servers at workstations, servers, or mobile computing devices on the network and uses the virus protection mechanisms to detect and eradicate malicious code, i.e., viruses, worms, Trojan horses that can be transported by email, email attachments, internet access, removable media such as diskettes, CDs or flash drives, or by exploiting vulnerabilities.
- Virus protection mechanisms should be updated whenever new updates are available.
- Agencies employ tools and techniques to monitor events on the OTCnet system, detect attacks, and provide identification of unauthorized use of the system.
- Agencies implement tools to prevent spam and spyware.
- Agencies restrict information input to the OTCnet system to authorized personnel only.
- Agencies check the OTCnet information input for accuracy, completeness, and validity. OTCnet information includes the scanned check data, and all input fields such as the dollar amount and user defined fields.
- The agencies identify and handle error conditions in an expeditious manner.
- The agencies handle and retain output, e.g., reports, check images, etc., from the OTCnet in accordance with policy and operational requirements.

In Summary

- Protection against viruses, spyware and all other forms of malicious code on both the OTCnet computer and all removable media used on the OTCnet system (diskettes, CDs, flash drives) should be in place.
- Although the NIST 800-53 document recommends keeping your computer up to date with the latest security patches, hot fixes and service packs, it is up to each agency to determine the feasibility of installing every patch or fix and installation may need to be considered on a case-by-case basis. Consult your network support staff for more information.
- Regular updates to the virus protection software should be applied.
- Only authorized personnel should have access to the OTCnet system. If using backup personnel to perform OTCnet duties, backups should be issued their own unique login ID and password. Logins and passwords should never be shared under any circumstances.
- Verification practices should be used to ensure accuracy of input.
- To prevent duplicate processing of checks, checks may be hand stamped with 'Electronically Processed' after the transaction is complete and the check has been scanned. The EC6000i and EC7000i scanners can also be setup to automatically stamp the front of the check with the words, 'Electronically Presented', once the transaction is complete.

Media Protection

NIST Special Publication 800-53 Guidance

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented media protection policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal, documented procedures to facilitate the implementation of the media protection policy and associated system and information integrity policy controls.

Due to the nature of the transaction information which includes check images, the OTCnet media that stores this information is considered PII and must be secured. The OTCnet media to be protected includes both digital media, i.e., diskettes, external/removable hard drives, LAN drives used for OTCnet data retention/storage, flash/thumb drives, compact disks, digital video disks, and non-digital media, i.e., paper, microfilm and checks not returned to the check writer. This control also applies to portable and mobile computing and communications devices with information storage capability, i.e., notebook computers, personal digital media assistants, and cellular telephones.

Effects on OTCnet

- Agencies ensure that only authorized users have access to OTCnet information in printed form or on digital media removed from the information system.
- Agencies affix external labels to removable OTCnet storage media and OTCnet system output indicating the distribution limitations and handling caveats of the information. Certain media may be exempted from this labeling as long as they remain within a secure environment.
- Agencies physically control and securely store the OTCnet system media, both paper and digital, based on the highest FIPS 199 security category of the information recorded on the media.
- Agencies sanitize OTCnet system digital media using approved equipment techniques and procedures. Sanitization is the process used to remove information from digital media such that information recovery is not possible. (NIST Special Publication 800-36 provides guidance on appropriate sanitization equipments, techniques, and procedures.)
- Agencies sanitize or destroy OTCnet digital media before its disposal or release for reuse, to prevent unauthorized individuals from gaining access to and using information contained on the media. (NIST Special Publication 800-36 provides guidance on appropriate sanitization equipments, techniques, and procedures.)
- Agencies physically control and securely store OTCnet system media within a controlled area.

In Summary

- Only authorized users should have access to printed and digital media used for OTCnet. This means all printouts, hard disks, LAN drives, external hard disks, diskettes, CDs, zip disks, smart cards, and USB flash drives.
- Store and label all removable media (both digital and paper) in a secured endpoint. Labeling could include the restrictions on distributing the media and warnings on handling of the media.
- Properly remove all OTCnet related data prior to destruction or reuse. Information stored on OTCnet's hard drive, secondary storage drive, and printed media may contain personally identifiable information (PII) in the form of names, account numbers, social security numbers, etc. within an OTCnet batch.
- OTCnet paper output such as batch lists, report printouts, and scanned checks not returned to customers contain PII information and must be destroyed by shredding. This type of output should never be thrown away with other office trash without shredding.
- Consider additional encryption protection of the information that is contained on the secondary storage drive. OTCnet provides a minimum level of encryption to the data on the secondary storage drive but additional encryption protection may be used. If additional levels of encryption are used, agencies must ensure that the data can be decrypted in the event that the data needs to be restored using the OTCnet 'Batch

Recover' function. Decryption will typically involve the use of a password. If the additional level of encryption cannot be removed, OTCnet will be unable to read the batch data and the batch recovery function will fail.

Incident Response

NIST Special Publication 800-53 Guidance

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented incident response policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal, documented procedures to facilitate the implementation of the incident response policy and associated system and incident response policy controls.

Effects on OTCnet

- Agencies train personnel in their security incident response roles and responsibilities with respect to the OTCnet system and provide refresher training.
- Agencies track and document OTCnet system security incidents on an ongoing basis.

Agencies expeditiously report all OTCnet system security incidents of theft, loss, or data/PII compromise (known or suspected) to the Treasury OTC Support Center at (866)945-7920, or 302-324-6442, or military DSN at 510-428-6824, option 1, option 2, option 4, and their own internal authorized security personnel.

In Summary

OTCnet Point-of-Contacts and users should monitor the OTCnet system for possible security incidents and report any suspected incidents to the Treasury OTC Support Center at (866)945-7920, or 302-324-6442, or military DSN at 510-428-6824, option 1, option 2, option 4 or via email at FMS.OTCChannel@citi.com.

Awareness and Training

NIST Special Publication 800-53 Guidance

Organization develops, disseminates, and periodically reviews/updates:

1. A formal documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, and compliance.
2. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training policy controls

Security awareness and training ensures that all users (including managers and senior executives) are exposed to basic information system security awareness materials before authorizing access to OTCnet system and thereafter, at least yearly. Appropriate content of security awareness must be determined and based on the specific requirements of the OTCnet system. The Agency's security awareness program should be consistent with the requirements contained in 5 CFR Part 930.301 and with the guidance in NIST Special Publication 800-50.

Effects on OTCnet

- Users should be familiar with the password requirements.
- Users should be familiar with the OTCnet Security Guidelines.

In Summary

Information that is covered in the OTCnet Security Awareness Training should include:

- Prevent others from watching while passwords are entered. Prevent others from guessing your password - do not use names of persons, places, or things that can be easily identified with you.
- Login IDs and passwords should never be shared.
- If your password has been compromised, it must be changed immediately.
- Unauthorized use of the system must be reported to Treasury OTC Support Center at (866)945-7920, or 302-324-6442, or military DSN at 510-428-6824, option 1, option 2, option 4 or via email at FMS.OTCChannel@citi.com.
- Log off of the system whenever you leave your computer unattended by clicking on the 'Logout' button on the menu or clicking the 'X' at the upper right corner of the screen to prevent unauthorized access to the system.
- Security contacts or Point-of-Contacts (POC) should be kept current. As soon as an agency is aware of a change in personnel, a new person should be assigned the duties of the security contact to take the place of the exiting person. The exiting person's access should be deleted.

- The OTCnet security personnel, or POC's, should be trained on the proper handling of a user and it's associated password. Proper handling includes writing down the password and locking it up. Since the password will need to be changed every 90 calendar days it is important that the written password is updated whenever the password is changed. It should only be available to the POC.
- Users should be familiar with the Rules of Behavior, Privacy Statement, and Accessibility Statement prior to using the system. The Rules of Behavior, Privacy Statement, and Accessibility Statement can be found as links on OTCnet.

Glossary

A

Access Groups by Users Report - This report displays the roles and the corresponding access groups of the role for a particular OTCnet user. The role assigns the permissions (functions/features) that a user has access to in OTCnet. The access group governs the OTC Endpoint(s) and the data that a user has permission to access.

Accounting Code - A unique agency classification code assigned to a transaction, which identifies the FRB Account Key that is used within the Federal Reserve. In check capture, it is a method of grouping individual check transactions into certain classifications. In deposit reporting, the classification is being done at a voucher level, where a voucher is being classified with one or many agency defined accounting codes or TAS.

Accounting Code Description - A brief explanation that provides further detail about an accounting code.

Accounting Code Name - The title of the accounting code.

Accounting Key - The account number assigned to a deposit when it is submitted to FRB CA\$HLINK. The FRB Account Key is used by FRB CASHLINK in combination with the RTN to determine the appropriate CA\$HLINK II CAN. The FRB Account Key is similar to the CAN, but is only used for FRB financial activity.

Accounting Specialist - A user who is an expert on the organizational structure, reporting needs and accounting rules for their agency. This role will establish and maintain the organizational foundation, accounting data and accounting relationships at the highest level of the agency in OTCnet.

Acknowledged Batch Status – Indicates the batch was transmitted and fully processed by the OTCnet server without error.

Acknowledged Error Batch Status – Indicates the acknowledge batch process experienced system errors and the acknowledgment was unsuccessful, or a user selected to cancel the batch acknowledgment which results in a batch being updated to Acknowledgment Error.

Activity Type - The parameter indicates if a User Defined Field (UDF) is used for capturing custom agency information for a deposit or during classifying the deposit with accounting codes. OTCnet allows for the creation of three UDFs for the deposit activity, and two UDFs for the deposit accounting subtotals activity.

Adjustment Activity (FI) Report - A business report that allows you to view adjustments made by your financial institution (FI).

Adjustment Activity (FRB) Report - A business report that allows you view adjustments made by your Federal Reserve Bank (FRB).

Adjustments by OTC Endpoints Report - A business report that allows you to view adjustments made by Agency Location Code (ALC) and Adjustment Types (Credit, Debit or Return Item Adjustments). An adjustment was created when a deposit ticket has been received by a financial institution and the amount of the deposit does not match the deposit amount reported on the deposit ticket.

Agency CIRA Report - A check processing business report that allows you to view the batch level transaction activity for a specified OTC Endpoint. A user can filter the report by Received Date, Capture Date, Batch ID, or Check Capture Operator.

Agency Contact - A person designated by an agency as the primary contact regarding deposit-related matters.

Agency Information - The optional comments or instructions, receipt processing dates, alternate agency contact, and internal control number for your deposit.

Agency Location Code (ALC) - A numeric symbol identifying the agency accounting and/or reporting office.

Agency Location Code plus 2 (ALC+2) - A numeric symbol identifying the agency accounting and/or reporting office.

Agency Manager - A user that has authorization to view and download CIRA records and view reports.

Alternate Agency Contact – A person designated by an agency as the secondary contact regarding deposit-related matters.

American Bankers Association (ABA) - (also known as **Bank Routing Number**) A routing transit number (RTN), routing number, or ABA number is a nine-digit bank code, used in the United States, which appears on the bottom of negotiable instruments such as checks identifying the financial institution on which it was drawn.

Approved Batch Status - Indicates that the batch is ready for settlement (online only). Indicates that the batch is ready for upload and settlement (offline only).

Audit Log - A table that records all interactions between the user and OTCnet Deposit Reporting, Check Capture, Check Processing, administrative actions and other processes that take place in the application. Some entries also contain before and after values for actions completed. The audit log is available for download to a *comma separated value report (CSV)* and opened in a spreadsheet program or available to print in a formatted audit log report.

Automated Clearing House - A computerized network used by member financial institutions to process payment orders in machine readable form. ACH processes both credit and debit transactions between financial institutions in batches. ACH items are settled electronically and do not require an image.

Awaiting Approval (AWAP) - A deposit that is waiting for deposit confirmation by a Deposit Approver.

B

Back Office Processing Method - Indicates that a customer presented a check in person, but the check is being scanned in a controlled back-office environment away from the customer.

Batch - A file containing the transaction information and tiff images (collection of scanned checks) of one or more checks, which will be sent for settlement.

Batch Approver - An agency user that has the authorization to approve a batch either prior to batch upload from OTCnet Offline or when a batch is uploaded/submitted to OTCnet Online but not yet approved. The Batch Approver permission must be applied to either a Check Capture Lead Operator or Check Capture Operator roles and allows the operators to approve batches that they have created. This role should be granted in limited cases at sites where there is a need for the operator to perform this function without a Check Capture Supervisor present.

Batch Control/Batch Balancing - An optional feature (which can be configured to be mandatory) that agencies can use as a batch balancing tool to perform checks and balances on the number of checks that have been scanned, and ensure their respective dollar amounts and check number totals have been accurately entered. The functionality is available for both single item mode and batch mode.

Batch ID - The unique number assigned to a batch by OTCnet.

Batch List Report - A report that contains transaction information for each batch item, including the Individual Reference Number (IRN), Item Type, ABA Number, Account Number, Check Number, and Amount.

Batch Status - Reflects the current state of a batch during processing, transmission, and settlement. The batch states for OTCnet Online are Open, Closed, Approved, and Forwarded. The batch states for OTCnet Offline are Open, Closed, Approved, Sending, Sent, Acknowledged, Send Error, and Acknowledgment Error (offline only).

Batch Uploader - An agency user that has the authorization to upload a batch from OTCnet Offline to the online database. The Batch Uploader permission must be applied to either a Check Capture Lead Operator or Check Capture Operator roles and allows the operators to auto-upload the batch upon close (if terminal is configured to do so), or upload approved batches. This role should be granted in limited cases at sites where there is a need for the operator to perform this function without a Check Capture Supervisor present.

Blocked - A customer may no longer present checks for a specific ABA number and account number due to manual entry by authorized persons into the MVD rather than the result of a failed transaction. If desired, an authorized user can edit the transactional record to a clear status.

Business Event Type Code (BETC) - A code used in the CARS/GWA system to indicate the type of activity being reported, such as payments, collections, borrowings, etc. This code must accompany the Treasury Account Symbol (TAS).

C

CA\$HLINK II - An electronic cash concentration, financial information, and data warehouse system used to manage the collection of U.S. government funds and to provide deposit information to Federal agencies.

CA\$HLINK II Account Number (CAN) - The account number assigned to a deposit when it is submitted to CA\$HLINK II.

Capture Date - The calendar date and time the payment is processed by the agency.

Cashier ID - The ID of the user that created the transaction.

Central Accounting Reporting System (CARS) – (formerly GWA)The system that addresses the central accounting and reporting functions and processes associated with budget execution, accountability, and cash/other asset management. This includes the collection and dissemination of financial management and accounting information from and to federal program agencies.

Central Image and Research Archive (CIRA) - The Central Image Research Archive (CIRA) is an image archive of all items processed in the OTCnet System.

Characteristics - The properties of a user, organization, deposit, or financial institution.

Check 21 - Provides the legal framework for the creation of substitute checks which can be used in place of the original paper document, without an agreement in place with other financial institutions. A substitute check is a paper reproduction of the original check. Check 21 items require an image before they can settle. Check 21 is also referred to as check truncation.

Check Amount - The dollar amount of the check.

Check Capture – The component of OTCnet used to process scan images of checks and money orders through OTCnet for the electronic deposit of checks and money orders at financial institutions. Check capture can be done online through the internet, or offline through the user's desktop.

Check Capture Administrator - An agency user that has the authorization to define and modify the check capture sites; to manage accounting codes; to modify endpoint mappings; to configure Check Capture functions and perform upgrades of the application; to download user profiles; as well as download software or firmware to the terminal using the Download Check Capture application permission.

Check Capture Lead Operator - An agency user that has the authorization to in scan checks into a batch, close a batch, balance check amounts and enter batch control values during batch closing. Additionally, the user can enter/apply the Accounting Code at the time of scanning checks is established. However, the user does not have authorization to accept duplicates, make MICR corrections, authorize the use of out-of-date LVD, or accept checks with poor quality.

Check Capture Offline – A web-based functionality in the offline Check Capture application that resides in the user's desktop for capturing check images for the electronic deposit of checks and money orders. The check transactions are stored within a local database, and the check information will need to be uploaded to OTCnet server when there is internet connectivity before they can be deposited for settlement.

Check Capture Online – A web-based functionality within OTCnet to allow agencies users to process scanned images of checks and money orders for the electronic deposit of checks and money orders at financial institutions. The check transactions are directly saved to the OTCnet online database, and no upload of batches of checks are needed.

Check Capture Operator - An agency user that has the authorization to perform only very minimal Check Capture activities. This user has authorization to scan checks into a batch and close a batch. This user does not have authorization to accept duplicates, make MICR corrections, authorize the use of out-of-date LVD, or accept checks with poor quality. Additionally, the user can enter/apply the Accounting Code at the time of scanning checks is established.

Check Capture Supervisor - An agency user that has the authorization to perform all the functions on the Check Capture. The user has authorization to accept duplicates (not recommended), make MICR corrections, authorize the use of out-of-date LVD, and accept checks with poor quality as well as view, modify, import, and modify endpoint mappings.

Check Number - The printed number of the check writer's check.

CIRA CSV Report - A check processing business report that allows you to export data based on a query to a comma separated value report (CSV). The exported data can be used to import into other applications within an agency.

CIRA Viewer - A user that has authorization to view CIRA records and download CSV files.

Clear - Indicates that a customer may present checks for a specific ABA Number and Account Number, because the prior restrictions on the individual's check payments have been removed. Note: Manually cleared items are permanently cleared. If a transaction is cleared in error, manual suspend, block or deny records need to be created in its place to prevent transactions.

Closed Batch Status - Indicates the batch is closed and no new checks may be scanned into that batch.

Comma Separated Values (CSV) - A computer data file used for storage of data structured in a table form. Each line in the CSV file corresponds to a row in the table. Within a line, fields are separated by commas, each field belonging to one table column.

Confirmed - A deposit that has been reviewed and then confirmed by a financial institution or FRB.

Cost Center Work Unit (CCWU) – A Federal Reserve cost center work unit that processing the FRB deposits and adjustments. It is normally abbreviated as CCWU, and provided only on non-commercial (FRB settled) transactions. Debits and credits processed by FRB Cleveland will be noted with the CCWU number 9910 on the daily accounting statement agencies receive from the Federal Reserve Bank.

Custom Label - Text defined by OTCnet that describes a level in the organization hierarchy, the internal control number, or agency accounting code.

Customer Not Present Processing Method - The processing method selected in OTCnet when processing a check that has been presented by a check writer who is not present at the agency location i.e., mail.

Customer Present Processing Method - The processing method used in the OTCnet when the check writer is presenting the check in person.

D

Daily Voucher Report - A business report that allows you to view the daily voucher extract.

Data Type - The type of data that should be entered for a user defined field.

Date of Deposit - The date, prior to established cut off times, the user transmits a batch of checks and money orders through check capture, or the date the agency sends the physical negotiable instruments to the financial institution.

Debit Gateway - The financial settlement program that is responsible for the presenting and settling of payment transactions acquired through the OTCnet application. The Debit Gateway receives a transaction file from OTCnet and determines the proper path for settlement of each item. Items are either converted to ACH for direct automated clearing house debit, or are included in an image cash letter, which is sent to the Check 21 system for presentation to paying banks. Once the file is processed, the Debit Gateway sends a Response Processing File (RPF) to OTCnet with the status of each of the items.

Demand Deposit Account (DDA) - The account at a financial institution where an organization deposits collections.

Denied - Indicates that OTCnet system permanently denies an individual from cashing a check through OTCnet based on the combination of ABA number, account number, and User Defined Field 1. User Defined Field 1 is usually the SSN number of an individual.

Deny Date - Indicates when the verification record (MVD/LVD) expires, and OTCnet can start accepting checks that will be presented by a check writer that has previously presented a bad check. The Deny Date is calculated based on suspension periods configured in the Check Cashing policy of an OTC Endpoint.

Deposit - A collection of over-the-counter receipts deposited to a Treasury General Account for credit.

Deposit Activity (FI) Report - A business report that allows the financial institution to view deposits submitted to its location.

Deposit Activity (FRB) Report - A business report that allows you to view deposits submitted to your FRB.

Deposit Approver - A user who has authorization to review and submit deposits to a financial institution.

Deposit Confirmer - A user at a financial institution that has authorization to verify the accuracy of deposits received from an agency.

Deposit History by Status Report - A business report that allows you to view deposits by status.

Deposit Information - The attributes that define a deposit: deposit status, voucher number, deposit endpoint, ALC, voucher date, deposit total, check/money order subtotal, currency subtotal, and subtotals by accounting code.

Deposit Preparer - A user that has authorization to prepare and save deposits for approval to a Deposit Approver.

Deposit Total - The total amount of over-the-counter receipts included in the deposit.

Deposits by Accounting Code Report - A business report that allows you to view deposits by accounting code.

Deposits by OTC Endpoint Report - A business report that allows you to view deposits by OTC Endpoint.

Display Order Number - The order in which user defined fields (UDFs) should be displayed.

Draft - A deposit that is saved for modification at a later date by a Deposit Preparer.

F

Failed - The item was unable to be processed and/or settled by Treasury/FMS. These are item that could not be collected such as foreign items or possible duplicate items. These items are not included on your 215 Report.

Federal Program Agency - A permanent or semi-permanent organization of government that is responsible for the oversight and administration of specific functions.

Federal Reserve Bank (FRB) - A Federal Reserve Bank is one of twelve regulatory bodies throughout the United States that make up the Federal Reserve System. Each Bank is given power over commercial and savings banks in its area and is charged with making sure that those banks comply with any and all rules and regulations.

Federal Reserve Bank-Cleveland (FRB-C) - FRB-C serves as the conduit for settlement of transactions originating from the OTCnet application. FRB-C is responsible for receiving the transaction data from OTCnet via forward file, and performing check clearing/transaction settlement as the 'debit gateway'.

Federal Reserve System's Automated Clearing House (ACH) System - Enables debits and credits to be sent electronically between depository financial institutions.

Financial Institution (FI) - A bank, designated by the Treasury and a Treasury General Account (TGA) of International Treasury General Account (ITGA), which collects funds to be deposited in the Treasury General Account. These banks also include the Federal Reserve Bank (FRB).

Financial Institution Information - The name, address, routing transit number, and the demand deposit account number of a financial institution.

Financial Management Service (FMS) - The bureau of the United States Department of Treasury that provides central payment services to federal agencies, operates the federal government's collections and deposit systems, provides government wide accounting and reporting services, and manages the collection of delinquent debt owed to the government.

Firmware - A release used for initial download or upgrades to the scanner software that allows a scanner to be used on a terminal. The firmware versions also contains a series of other back-end installation files that should be installed on a terminal to enable it to be used for Check Capture in OTCnet.

Fiscal Year - A 12-month period for which an organization plans the use of its funds.

FMS Statistical Report - A check processing administration report that allows you to view statistical details for an OTC Endpoint. The report includes statistical information regarding the total transactions, overall success rate, total returns sent back to the agency, and total returns received. The report is available for 15 rolling days.

Forwarded Batch Status - Indicates the batch has been sent to Debit Gateway to initiate the settlement process.

Forwarded File - A term that is assigned to a file that contains the check transactions that is send from channel applications, such as OTCnet or ECP, to Debit Gateway for settlement purposes.

Franker - An internal stamp unit that stamps a check with "Electronically Processed" after the check is processed and scanned. Franker availability is based on the model of your scanner.

Franking - The process of stamping a check processed through Check Capture. The stamp indicates that the check was electronically processed.

H

Highest Level Organization - The primary level of the organization hierarchy.

I

IBM Tivoli Identity Manager (ITIM) - Refers to FMS's Enterprise provisioning tool for user account and identity management.

Individual Reference Number (IRN) - The auto-generated unique number used in OTCnet to identify Check Capture transactions.

Input Length Maximum - The maximum number of characters that may be entered in a user defined field.

Input Length Minimum - The minimum number of characters that may be entered in a user defined field.

Internal Control Number - A customizable field for agency use to further describe a deposit.

Item Detail Report - A report that contains the information about an individual item (check) associated with a batch. The report print-out will contain MICR information, data entered about the check, and an image of the check obtained during scanning.

Item Type - Indicates whether the check presented is a personal or business check. This determines whether the check is handled through Check 21 (non-personal) or FedACH (personal).

L

Local Accounting Specialist - A user who is an expert on the organizational structure, reporting needs and accounting rules for their depositing endpoint and its lower level OTC Endpoints. This role will establish and maintain the organizational structure, accounting code mappings to individual endpoints and the processing options that one or more lower level OTC Endpoints will use in OTCnet.

Local Security Administrator (LSA) - An agency or financial institution/federal reserve bank user who has authorization to maintain user access to an organization, including

assigning/removing user roles and assigning/removing organization hierarchy access. This user is also able to request and create users for the organization.

Local Verification Database (LVD) - A database (specific to the endpoint using OTCnet) that is downloaded from OTCnet and stored locally on the agencies network, which replicates the information found in the Master Verification Database (MVD).

Lower Level Organization - Any organization created below the highest level organization.

LVD Contents Report - A check processing business report that allows you to view the contents of a Local Verification Database (LVD) for a given OTC Endpoint.

M

Magnetic Ink Character Recognition (MICR) - Digital characters on the bottom edge of a paper check containing the issuing bank's ABA number and account number. The check number may also be included.

Master Verification Database (MVD) - It is an online database specific to the agency that maintains the agency hierarchy check cashing policy, information on bad check writers, and manually entered blocked items based on an agency's policy. Bad check information is accumulated in the MVD as agencies process checks through Check Capture. The MVD provides downloads of dishonored check information and blocked items via the Local Verification Database (LVD) on a daily basis.

MVD Editor - A user that has the authorization to view, edit, and download CIRA records, view verification records, and read blocked records containing only ABA permissions.

MVD Viewer - A user that has the authorization to view and download CIRA records, view verification records, and read blocked records containing only ABA permissions.

N

Non-Personal Item Type - Indicates that the name on check is an organization, or the check is a money order, traveler's check, or third-party check.

Non-Reporting OTC Endpoints Report - A business report that allows you to view OTC Endpoints that have not reported a deposit.

O

Open Batch Status - Indicates the batch is open and accepting new checks.

Organization - The location or level within a Federal Program agency.

Organization Hierarchy - The structure of a Federal Program agency as defined in OTCnet.

Organization Hierarchy Report - A check processing business report that allows you to view the target OTC Endpoint within the context of the current OTC Endpoint.

OTC Collections - Receipts that contain cash, checks, and/or money orders that are collected over-the-counter by organization endpoints in exchange for goods or services.

OTC Endpoint - The endpoint (location) that collects over-the-counter (OTC) receipts and deposits them to the Treasury's General Account.

OTC Endpoint (CHK) - The endpoint (location) setup in OTCnet to use check capture.

OTC Endpoint (TGA) - The endpoint (location) setup in OTCnet to use Deposit Reporting.

OTC Endpoint Mapping - The assignment of accounting codes to an agency's OTC Endpoint, for which a deposit amount can be allocated.

OTCnet Offline - Refers to the over the counter application that provides Check Capture functionality to end users with limited internet activity, and provides the capability to upload offline-captured batches to the Online OTCnet application for processing.

OTCnet Online - Refers to the web-based over the counter application that provides Check Capture, Check Processing and Deposit Processing functions to end users (that have constant internet activity).

Over the Counter Channel Application (OTCnet) - Refers to the over the counter application that provide Check Capture and Deposit Reporting to end users.

P

Personal Item Type - Indicates that the name on check is an individual's name, not acting as a business.

Primary Local Security Administrator (PLSA) - An agency or financial institution/federal reserve bank user who has authorization to maintain user access to an organization, including assigning/removing user roles and assigning/removing organization hierarchy access. This user is also able to request and create users for the organization.

Processing Options - User-defined parameters for the deposit and adjustment processes.

Processing Options by OTC Endpoints Report - A business report that allows you to view processing options defined for endpoints within the organization.

Q

Queue Interface – Used by military agencies that utilize the Deployable Disbursing System (DDS) database bridge. It provides a single transaction input point, prevents data entry errors, and discrepancy between both systems.

R

Received - The agency has sent this transaction through OTCnet. No settlement has been performed for this transaction yet.

Received Date - The date the check was received by web-based OTCnet.

Rejected - A deposit that is returned by a financial institution or FRB to the Deposit Preparer to create a new deposit.

Represented - This transaction was returned with a reason code that allows for another collection attempt to be made (see Appendix Chapter of the Participant User Guides for Reason Codes). Depending on an agency's policy, the item is reprocessed in an attempt to collect the funds from the check writer. Items with this status are in-process of collection.

Retired - This transaction was unable to be collected. The agency receives an SF5515 Debit Voucher Report with a debit processed to Debit Gateway, the effective date and debit voucher number. The offset to the agency's debit is an ACH return or a paper return (Check 21) received from the check writer's financial institution. This transaction cannot be processed again through OTCnet.

Return Reason Codes - Represent the numeric codes used in the ACH and paper return processing, which specify the reason for the return of the transaction and Check 21 codes.

Return Settlement Date - The effective date of settlement of the returned check item.

Returned Item - A check that was originally part of an OTCnet deposit but returned to the financial institution for non-sufficient funds, closed account, etc.

Routing Transit Number (RTN) - (also known as **American Bankers Association (ABA) Number or Bank Routing Number**) - The nine-digit number used to identify a financial institution.

S

Save as Draft - An option that allows a Deposit Preparer to save a deposit for modification at a later date.

Save for Approval - An option that allows a Deposit Preparer to save a deposit for a Deposit Approver to submit to a financial institution.

Send Error Batch Status – Indicates the batch was transmitted and fully processed by the OTCnet server without error.

Sent Batch Status – Indicates the batch was uploaded online without error.

Separation of Duties - A concept used to ensure there are typically separate personnel with authority to authorize a transaction, process the transaction, and review the transaction.

Settle Best Method - The option that allows OTCnet to decide the best settlement method for personal and non-personal checks.

Settled - This transaction is complete and the funds have been credited to the agency's Treasury General Account. The effective date of the deposit and the SF215 Deposit Ticket Report deposit ticket number are provided.

Settlement Date - The date the deposit is credited to the Treasury General Account.

SF215 Deposit Ticket Report - The report presented to a financial institution by a U.S. government agency with checks and other payment instruments to make a manual deposit. This report is manually generated for Deposit Reporting and auto-generated for Check capture. The report is available in OTCnet for 45 calendar days.

SF5515 Debit Voucher Report - The report used to debit the Treasury General Account (TGA) to decrease the amount of a deposit made to that account. This report is manually generated for Deposit Reporting and auto-generated for Check capture. The report is available in OTCnet for 45 calendar days.

Share Accounting Module (SAM) - The application that facilitates the process of validating or deriving Treasury Account Symbol (TAS) and Business Event Type Code (BETC) combinations to assist CARS/GWA in classifying financial transactions as they occur.

Short Name/Code - The user-defined text describing an organization. Short Names/Codes must be unique within an organization hierarchy.

Submit - An option that allows a Deposit Approver to submit a deposit to a financial institution.

Submitted - A deposit that is submitted and waiting deposit confirmation by a Deposit Confirmer.

Suspend - Indicates that an individual's record is set to a predetermined suspension period. During this time, OTCnet prevents an individual from processing a check through OTCnet. The individual's database record has a Trade Status of Suspend and the expiration date is set until a specific date.

T

Terminal ID - The unique number assigned to the workstation where a user performs functions in OTCnet.

Trade Status - Represents the status of the verification records. There are four possible trade statuses in the system: Blocked, Denied, Suspended, and Cleared. The Trade Status D-Suspended or D-Denied is assigned to auto generated Dynamic records.

Transaction History - Defines the time range that a Deposit Confirmer will be able to view the historical deposit transactions for his or her financial institutions. For example, if the transaction history is set at 45 days, the Deposit Confirmer will be able to view all the deposits that he or she has confirmed for the past 45 days.

Transaction Reporting System (TRS) - A collections reporting tool, supplying the latest information on deposits and detail of collections transactions to federal agencies. The system will allow financial transaction information from all collections systems and settlement mechanisms to be exchanged in a single system.

Treasury Account Symbol (TAS) - The receipt, expenditure, appropriation, and other fund account symbols and titles as assigned by Treasury.

U

Universal Serial Bus (USB) - A connection port on a computer that is universally compatible with many types of devices, such as printers, speakers, mouse, flash drives, etc.

US Dollar Equivalent (USE) - The deposit amount, in United States currency, which is equal to the foreign currency for which it is being exchanged.

US Treasury - The executive department and the Treasury of the United States federal government.

User Defined Field (UDF) - A user-defined text that describes deposit activity or deposit accounting activity.

User Information Report - A security report allows that you to view a user's contact information.

Users by Access Group (FI) Report - A security report that allows you to view users by financial institution.

Users by Access Group (FPA) Report - A security report that allows you to view users by OTC Endpoint.

Users by Role (FI) Report - A security report that allows you to view users by role for your financial institution.

Users by Role (FPA) Report - A security report that allows you to view users by role for your OTC Endpoint.

V

View CA\$HLINK II File Status Report - An administration report that allows you to view the status of deposit report files that have been processed by CA\$HLINK II or are ready for CA\$HLINK II to process.

View FRB CA\$HLINK File Status Report - An administration report allows you to view the status of deposit files that have been sent to FRB CA\$HLINK.

View TRS File Status Report - An administration report allows you to view the status of TRS files that have been processed by Transaction Reporting System (TRS) or are ready for TRS to process.

View Vouchers Completed Report - An administration report allows you to view the status of deposit and adjustment vouchers that have completed processing through the FI System To System Interface in the past 36 hours.

View Vouchers in Progress Report - An administration report allows you to view the status of deposit and adjustment vouchers in progress.

Viewer - A user who has authorization to view OTCnet information and produce reports from it.

Voucher Date - The financial institution business date a deposit will be presented or the calendar date the deposit will be mailed to the financial institution.

Voucher Number - The number assigned to a deposit by OTCnet.

Index

Batch ID.....	9	Item Type	7
Capture Date.....	10	Master Verification Database.....	i, iii, iv, 12, 37
Check 21	i, 18, 19, 20	MVD Viewer	iii, 5
Check Capture Administrator.....	iii	Password	i, iv, 3
Check Capture Lead Operator.....	iii	Received	19
Check Capture Operator	iii	Represented	19
Check Capture Supervisor.....	iii	Retired	19, 20
Equipment	i, iv, 14	Search Criteria Fields	8, 10
Failed.....	i, 4, 19		