

Merchant
User Guide

eCheck Processing

June 17, 2013

| Version 10

CHASE ™
Paymentech

4 Northeastern Blvd.
Salem, NH 03079-1952
603.896.6000

www.chasepaymentech.com

CHASE ™
Paymentech

eCheck Processing

U.S. and Canada

A Merchant User Guide



© Chase Paymentech Solutions, LLC – 2006 – 2013, All rights reserved

14221 Dallas Parkway
Dallas, TX 75254
www.chasepaymentech.com

This document contains confidential and proprietary information of Chase Paymentech Solutions, LLC and Paymentech, LLC (collectively referred to as "Chase Paymentech"). No disclosure or duplication of any portion of these materials may be made without the express written consent of Chase Paymentech. These materials must be used solely for the operation of Chase Paymentech programs and for no other use.

DISCLAIMER

Chase Paymentech presents these materials for general informational purposes only, because we cannot make recommendations on rules, laws and regulations specific to you and your business.

PLEASE NOTE: We make no representations regarding the accuracy or completeness of the materials presented. The information provided contains summaries of NACHA rules and ACH requirements and may omit specific requirements that were, in our judgment, too detailed to fit within the intended scope of this document or too specific or narrowly tailored to be of interest to the majority of merchants.

Furthermore, NACHA rules and ACH requirements as well as any applicable codes, statutes and legislation are subject to frequent change and revision. You should not rely on these summaries alone. Please consult with your legal counsel and review the actual NACHA rules and applicable laws, codes, statutes, or legislation before making any decisions relating to your eCheck Program.

Revision History

Date	Revision Summary		Page(s)
11/26/08	Updated Supported Features		3-5
	Updated process maps		6-10
	FAQs added		70-78
	Changed Chase Paymentech Solutions to Chase Paymentech		All
12/10/08	Updated Response Codes		17
08/06/09	Added disclaimer		i
	Updated Supported features: PPD		4
	Updated Validation response codes		13 - 17
	Updated U.S. ECP return codes		27
	Updated Canadian ECP return codes		28
	Added ACH Operator Codes table		29
	Added Removing Accounts from the CPS Internal Negative File and SCAN		30 - 31
	Updated Guidelines for Authorization Methods		59 - 61
	Updated Debit authorization rules		65 - 66
	Updated Other relevant rules and regulations		67 - 68
	Updated FAQ's – ECP Processing and Implementation		80 - 83
	Added FAQ's – ECP Authorization Methods		84 – 85
09/21/2009	SCAN contact information updated		17, 31
10/13/2009	Special Note added		22
08/25/2010	Added Disclaimer		i
	Removed FAQs to separate document		
	Updated:	eCheck Solution Supported Features & added Special Note	3-5
		Transaction Processing	11-12
		Validation (US & Canadian ECP)	14-16
		Verification (US Only)	16
		Validation, Verification & Deposit Flows via Chase Paymentech	19
		Returns	22
		Return Codes, Dishonor Codes, & Response Actions (US ECP Only)	23-25
		Removing Accounts from SCAN File	32
	Added:	Communicating Negative Information	17
		Decline Notice Language	17-18
		ACT-0002 Report	34-37

Continued on next page

Table of Contents, Continued

Revision History, Continued

Date	Revision Summary	Page(s)
09/06/2011	Updated for ECP Compliance Program changes and incorporation of multiple processing platforms in one manual	Various
	Updated PTO Report Samples	35-48 & 65-67
	Added ROL Report Samples	55-62 & 68-69
10/22/2012	Updated Disclaimer	i
06/17/13	Reformatted Guide to new standard, removed ROL samples as not applicable to this manual	All

Table of Contents

<i>DISCLAIMER</i>	<i>i</i>
<i>Revision History</i>	<i>ii</i>
Table of Contents	iv
<i>Introduction</i>	<i>1</i>
<i>How eChecks are Processed</i>	<i>1</i>
<i>Why Implement an ACH Program?</i>	<i>1</i>
<i>The Chase Paymentech eCheck Solution</i>	<i>2</i>
<i>Summary of Chase Paymentech Supported ACH Entry Classes and Usage</i>	<i>4</i>
<i>How Does ECP Work?</i>	<i>5</i>
1. Acquisition of Customer Debit Authorization	<i>5</i>
2. Accounts Receivable (Check) Conversion (ARC).....	<i>6</i>
3. Point of Purchase (Check) Conversion (POP)	<i>7</i>
4. Telephone Initiated Payments (B2C) and Cash Concentration and Disbursement (B2B)	<i>8</i>
5. Internet Initiated Payments (B2C) and Cash Concentration and Disbursement (B2B)	<i>9</i>
<i>Transaction Processing</i>	<i>9</i>
<i>Preferred Delivery Method</i>	<i>10</i>
<i>Validation (U.S. and Canadian ECP)</i>	<i>11</i>
Phase 2 – Proprietary Databases and Negative Files	<i>12</i>
<i>Verification (U.S. Only)</i>	<i>14</i>
<i>Communicating Negative Information</i>	<i>14</i>
<i>Decline Notice Language</i>	<i>15</i>
<i>Validation, Verification and Deposit Flows via Chase Paymentech</i>	<i>16</i>
<i>Prenotification (U.S. ECP only)</i>	<i>17</i>
<i>Deposits</i>	<i>17</i>
<i>Facsimile Drafts (U.S. ECP only)</i>	<i>18</i>
Returns and Rejects	19
<i>Introduction</i>	<i>19</i>
<i>Returns</i>	<i>19</i>
<i>Returns, Redeposit and Dishonor Rules and Regulations</i>	<i>20</i>
<i>Redeposit of Returns for NSF and Uncollected Funds</i>	<i>24</i>
<i>Return Codes, Dishonor Codes and Response Actions (U.S. ECP Only)</i>	<i>24</i>
<i>Return Codes and Response Actions (Canadian ECP only)</i>	<i>26</i>
<i>Return Codes Used by ACH Operators</i>	<i>27</i>
<i>Removing Accounts from the CPS Proprietary Negative File</i>	<i>28</i>
<i>Removing Accounts from the Certegy Distributed Negative File</i>	<i>29</i>

Table of Contents, Continued

ECP Financial Reporting	30
<i>Introduction.....</i>	<i>30</i>
PTO ECP Financial Reporting.....	31
<i>Exception Detail (ACT-0002).....</i>	<i>31</i>
Field Definitions	32
<i>Deposit Activity Summary (FIN-0010)</i>	<i>34</i>
Field Definitions	35
<i>Service Charge Detail (FIN-0011).....</i>	<i>38</i>
Field Definitions	39
<i>ECP Returns Received (PDE-0022)</i>	<i>41</i>
Field Definitions	41
<i>ECP Return Activity (PDE-0018)</i>	<i>43</i>
Field Definitions	45
Notification of Change	47
<i>Introduction.....</i>	<i>47</i>
<i>eCheck Deposit Matching (Repairs).....</i>	<i>48</i>
<i>ECP Notification of Change (ACT-0019).....</i>	<i>49</i>
Field Definitions	50
eCheck Funds Transfer Options.....	52
<i>Available Options</i>	<i>52</i>
eCheck Rules and Regulations	53
<i>Regulatory Compliance</i>	<i>53</i>
<i>ACH Security Framework.....</i>	<i>54</i>
Summary:.....	54
Background:	54
KEY COMPONENTS OF RULE AMENDMENT	54
Protection of Sensitive Data and Access Controls	54
<i>Guidelines for Authorization Methods</i>	<i>55</i>
<i>Regulations and Industry Standards for U.S. ECP.....</i>	<i>58</i>
<i>Debit Authorization Rules.....</i>	<i>60</i>
<i>Other Relevant Rules and Regulations</i>	<i>61</i>
<i>Uniform Commercial Code</i>	<i>64</i>
<i>Uniform Commercial Code – Industry Best Practices</i>	<i>65</i>
<i>Regulations and Industry Standards for Canadian ECP.....</i>	<i>67</i>
Appendix A	68
<i>Overview.....</i>	<i>68</i>
<i>Supported Entry Classes</i>	<i>69</i>
<i>Components of a Personal Check.....</i>	<i>70</i>

Table of Contents, Continued

<i>Components of a Business Check – Parsing the MICR Line Data</i>	70
<i>Business Checks Ineligible for Conversion</i>	71
Appendix B	73
<i>Overview</i>	73
<i>Positive Reason Codes</i>	74
<i>Authorization Declines</i>	74
Best Practice FAQs	75
<i>Rules and Regulations – Unauthorized Returns</i>	75
<i>ECP Processing and Implementation</i>	80
<i>ECP Authorization Methods</i>	83
Glossary	84

Introduction

Electronic Check Processing (commonly referred to as eCheck or ECP) is an electronic payment solution designed to streamline payments in the U.S. and Canada. eCheck processing directly debits bank accounts for payment of goods and/or services. This User Guide explains Chase Paymentech's eCheck solutions and presents an overview of the rules and regulations governing eCheck transactions. A separate User Guide details our European eCheck solution, European Direct Debit.

How eChecks are Processed

eChecks are processed in one of two ways for U.S. Dollar transactions:

- Using the Automated Clearing House (ACH) network when the bank is a member, or by
- Generating a facsimile draft at the direction of the merchant or when the consumer's bank is not a participant of the ACH network

For Canadian currency processing, eChecks are processed by

Utilizing the Canadian Payments Association (CPA) to directly debit the consumer's account

Web Link: www.cdnpay.ca

Canadian eCheck processing is not available to Retail merchants.

For Euro and British Pound Sterling currencies, eCheck transactions are processed by

Accessing bank clearing systems in each country to directly debit the consumer's account. BACS and ELV are some of the popular European Direct Debit payment methods supported. (See the *European Direct Debit Processing User Guide*).

Why Implement an ACH Program?

Implementing an eCheck program can benefit a merchant by offering

- a lower cost method of payment (compared to bankcard interchange)
- a new customer acquisition tool (e.g. the credit challenged, under banked, or those who simply do not wish to pay with a bankcard), and
- a customer retention tool (e.g. recurring, continuity billing programs)

Continued on next page

Why Implement an ACH Program?, Continued

Facts

- The 18–34 age group has demonstrated a decided preference for debit payments over credit. This demographic is highly-evolved toward Internet use (e.g., 60% are online bankers and expect debit account access wherever they transact)
- Statistics show that 92% of high school graduates are Internet literate; growing numbers are registering for new payment types.
- A new population “bubble” is moving through the marketplace with unprecedented willingness to shop their primary debit account to institutions who offer the Internet and wireless services and access they demand
- Online merchants also realize that offering more payment options pays off

The Chase Paymentech eCheck Solution

The Chase Paymentech eCheck product is designed to provide merchants with a robust suite of eCheck services, and risk and exception management tools; all of which are critical to operating a profitable and efficient eCheck program. The following table details the product’s primary features and functionality:

Supported Features	Functions	Benefits
Validation	<ul style="list-style-type: none"> • Validation is mandatory for the merchant • Notification of Change (NOC) File: looks for changes made to any account data • Accuity File: ensures that the routing number belongs to a legitimate financial institution and that they participate in ACH • Internal Proprietary Negative File: looks for negative account history and/or updated account information provided by the customer’s bank 	<ul style="list-style-type: none"> • Complies with NACHA rules and regulations • Mitigates the risk of returns, rules violations and/or fines • Avoids re-entry of previous detected Negative Status Account.
Verification	<ul style="list-style-type: none"> • Verification is optional for the merchant. • Certegy Distributed Negative File: checks the account for: <ul style="list-style-type: none"> • current, unresolved NSF activity in the system • account closures • accounts that have a history of bad checks outstanding 	<ul style="list-style-type: none"> • Determines the likelihood of a ‘problem’ account • Excellent fraud prevention tool • Used primarily in situations where there is no pre-existing relationship with the customer

Continued on next page

The Chase Paymentech eCheck Solution, Continued

Supported Features	Functions	Benefits
Internet Payments (WEB)	<ul style="list-style-type: none"> Supports one time and recurring internet payments Supports debit entries authorized and/or initiated via Wireless Networks in accordance with WEB SEC Code guidelines. 	Accept eCheck payments from your customers via the WEB or wireless device
IVR and Call Center Payments (TEL)	<ul style="list-style-type: none"> Supports one time and recurring debit payments from a merchant's Call Center. An IVR system that only supports touch-tone response is not sufficient as a standalone authorization tool and must be accompanied with an oral authorization. 	Accept eCheck payments from your customers via the Call Center
Accounts Receivable Conversion (ARC)	Supports the conversion of checks received via U.S. mail into a merchant's unattended lockbox for single entry debits.	<ul style="list-style-type: none"> Quicker funds availability and returns data Electronification of paper adds greater automation and efficiency to back-office operations <p>Improved cash flow</p>
Point of Purchase Conversion (POP)	Supports single entry debits used at the point of purchase.	<ul style="list-style-type: none"> Quicker funds availability and returns data Electronification of paper adds greater automation and efficiency to point of purchase operations Improved cash flow
Corporate Credit or Debit (CCD)	<ul style="list-style-type: none"> Supports the use of ACH debits and credits in B2B transactions. MUST be used for all business to business transactions with the exception of POP and ARC. Supports the use of ACH debits and credits as a means of electronically paying corporate invoices 	<ul style="list-style-type: none"> Consolidates cash deposits from various divisions/affiliates into a central bank account Simplifies internal cash and treasury management Lower cost means of electronically paying vendor invoices
Single and Recurring Payments (PPD)	<ul style="list-style-type: none"> Supports a merchant's recurring billing programs Supports merchant credit and debit transactions. PPD must be used for all CREDIT transactions regardless of how the original debit authorization was taken. 	Lower cost means of collecting recurring payments from your existing customers

Continued on next page

The Chase Paymentech eCheck Solution, Continued

Supported Features	Functions	Benefits
Orbital Gateway and Virtual Terminal	Web services API and browser based 'virtual' terminal. Supports POP, ARC, WEB, TEL, PPD and CCD payments).	Expedited integration into the Chase Paymentech platform
GLBA Compliant Encryption (Gramm-Leach Bliley Security Compliance)	Supports the exchange of encrypted data with participating financial institutions	<ul style="list-style-type: none"> • Insures security and confidentiality of customer information • Protects against anticipated threats or hazards to the security or integrity of such information • Protects against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer
Automated Reporting and Exceptions Management	Supports Web based, or Tab, Comma Delimited (Electronic) File Formats for eCommerce CNP and Retail merchants.	Automated and simplified reconciliation of settlement proceeds, returns and exceptions

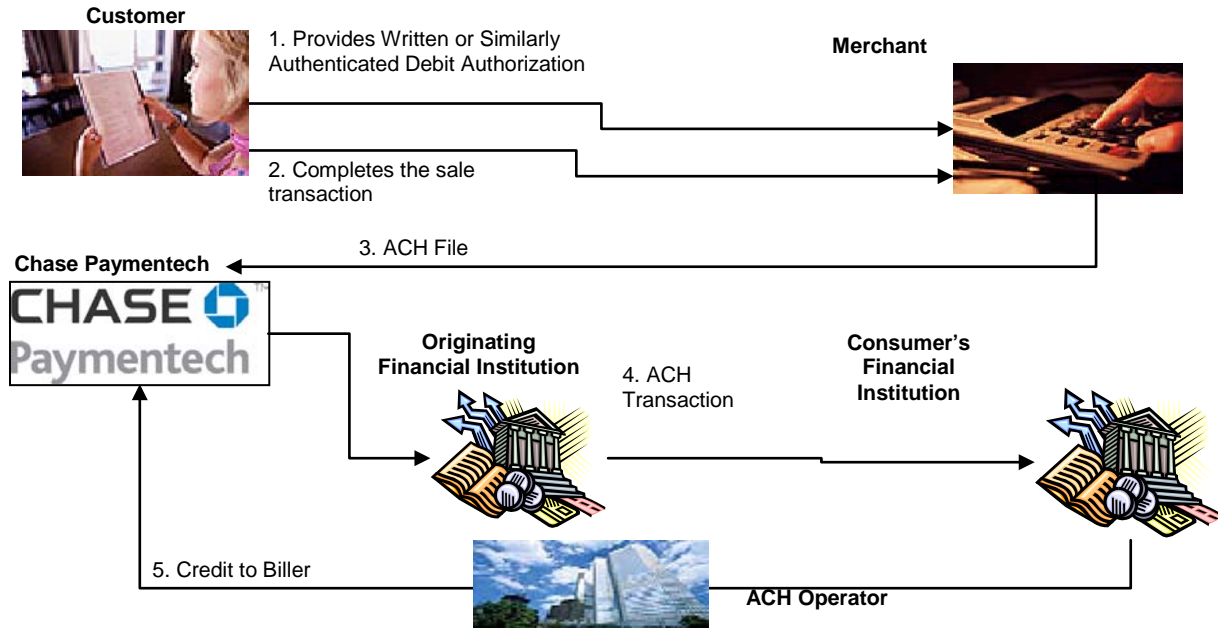
If merchants intend to electronically collect a service charge for transactions returned for insufficient funds, the merchant must CLEARLY DISCLOSE THE AMOUNT OF THE CHARGE, obtain the proper authorization from the consumer, as well as communicate the appropriate notice via written or verbal method prior to the transaction as per NACHA Rules and Regulations. The service charge fee must be transmitted as a separate transaction from the sale transaction.

Summary of Chase Paymentech Supported ACH Entry Classes and Usage

	B2C					B2B CCD
	ARC	POP	PPD	TEL	WEB	
Mail Drop Box	Y					
Telephone (person)			Y	Y		Y
Telephone (IVRU)			Y	Y		Y
Walk-In (Retail)						Y
Internet			Y		Y	Y
Other Electronic Devices (e.g., POS)		Y				
Direct Payment (recurring debit)			Y		Y	Y

How Does ECP Work?

1. Acquisition of Customer Debit Authorization

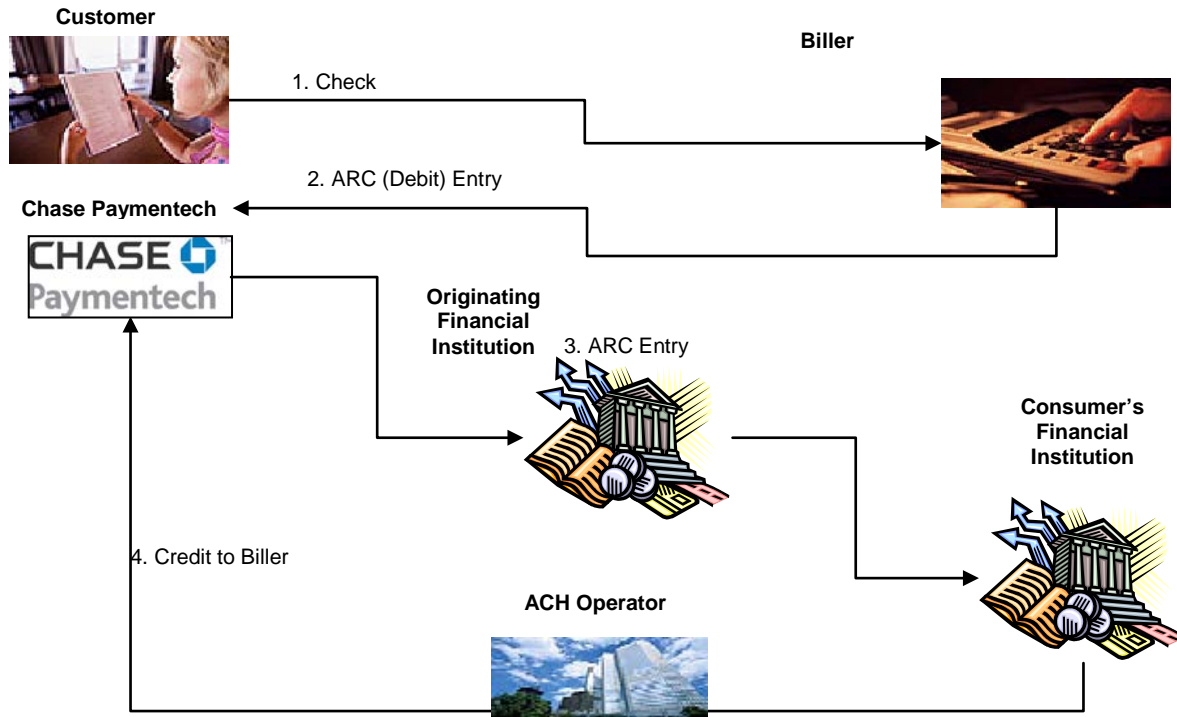


- Merchant must obtain debit authorization from the customer, prior to originating ACH debits to the customer's account.
- For a quick reference summary of the Debit Authorization Rules and Regulations, by Standard Entry Class, please refer to the ACH Authorization Authentication Guidelines in the Appendix of this document.

Continued on next page

How Does ECP Work?, Continued

2. Accounts Receivable (Check) Conversion (ARC)

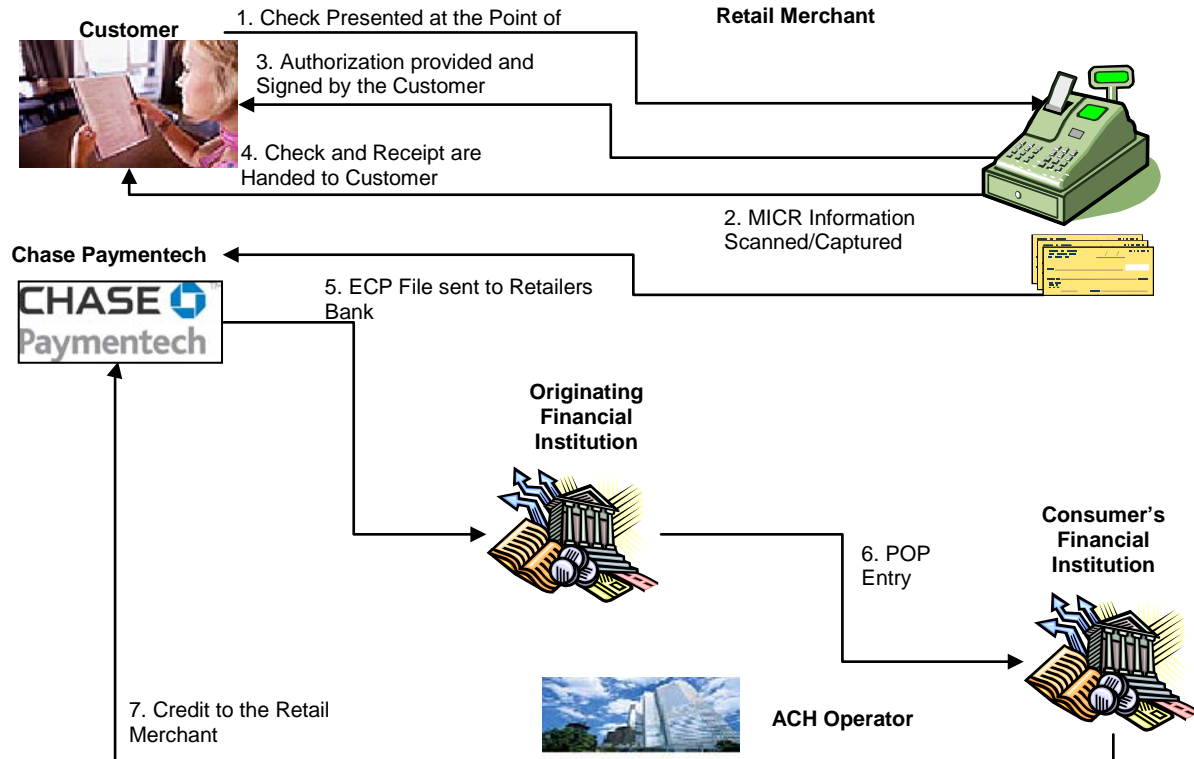


- Merchant opens the envelope with check/coupon, captures/archives check image, and posts bill data to Accounts Receivable.
- Merchant creates the ARC entry from the MICR information on the checks and transmits the data to Chase Paymentech.
- Chase Paymentech transmits the ARC entry to the originating financial institution that then transmits the entry to the ACH Operator for distribution to the consumer's financial institution.
- Consumer's financial institution debits the customer's account and sends a credit to the merchant account via the ACH Operator.
- Receipt of the paper check by the merchant serves as written debit authorization from the customer and is the source document for the transaction.

Continued on next page

How Does ECP Work?, Continued

3. Point of Purchase (Check) Conversion (POP)

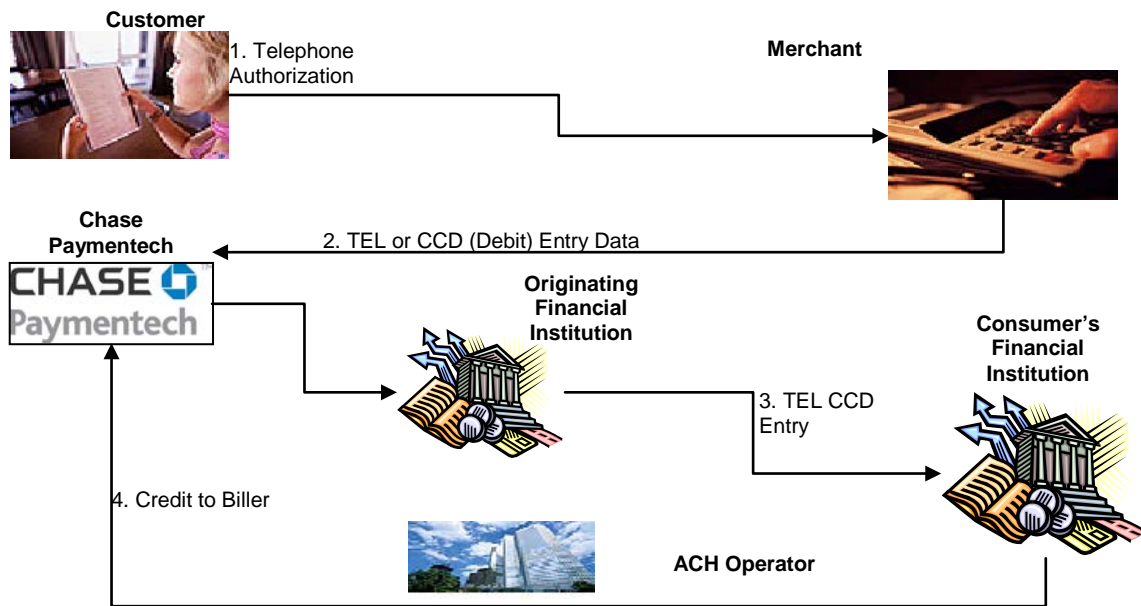


- Retail Merchant receives the check from the customer at the point of sale.
- Check is then scanned into a hardware device and the MICR information is captured. The device then voids the check and prints an authorization form. The check is not negotiated; it becomes the source document required to create the ACH transaction.
- Amount of the check is entered manually.
- Customer then signs the written authorization allowing the point of purchase debit to be processed against their account.
- Retail Merchant returns the voided check to the customer, along with a copy of the customers signed authorization and receipt containing:
 - Company name
 - Date of transaction
 - Amount of transaction
 - Serial number of check
 - Company or terminal ID
 - Terminal city
 - Terminal state
- Retail Merchant sends the ACH file to Chase Paymentech for clearing.
- Consumer's financial institution debits the customer's account and sends a credit to the retail merchant account via the ACH Operator.

Continued on next page

How Does ECP Work?, Continued

4. Telephone Initiated Payments (B2C) and Cash Concentration and Disbursement (B2B)

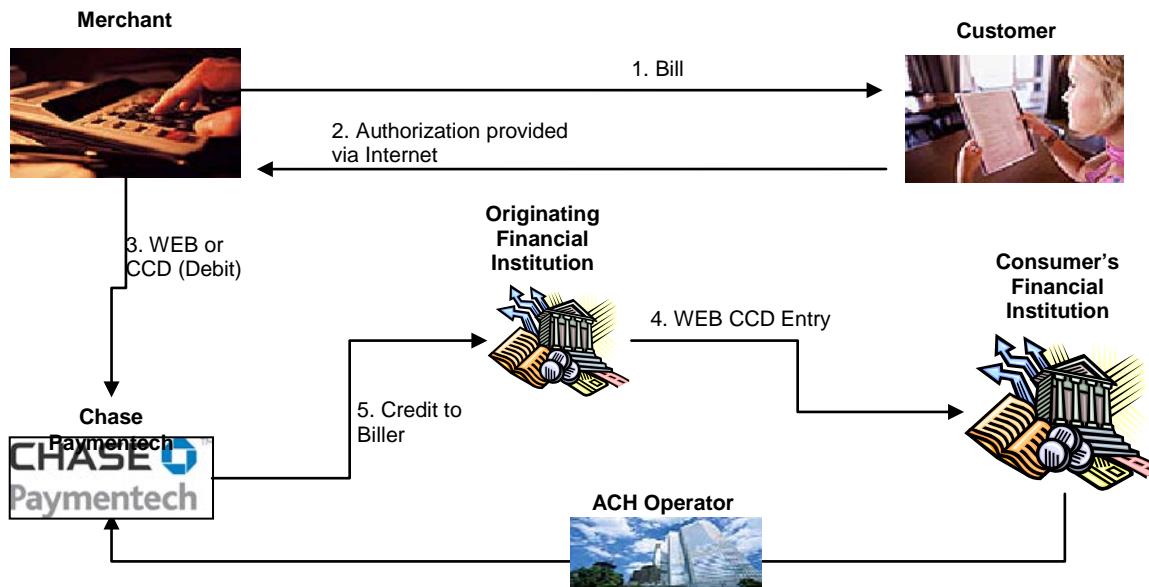


- Customer calls the merchant and provides debit authorization (written, or tape recorded) and bank account information.
- Merchant (or agent) initiates the debit transaction to the customer's account via the merchant financial institution.
- Chase Paymentech transmits the entry to the originating financial institution.
- Originating financial institution then transmits the ACH entry to the ACH Operator for distribution to the customer's financial institution.
- Customer's financial institution debits the customer's account and sends a credit to the merchant's account via the ACH Operator.

Continued on next page

How Does ECP Work?, Continued

5. Internet Initiated Payments (B2C) and Cash Concentration and Disbursement (B2B)



- Consumer visits merchant web site to perform transaction (business or consumer).
- Customer connects to the merchant website and provides debit authorization (per NACHA authorization requirements).
- Chase Paymentech transmits the entry to the originating financial institution who then creates an ACH entry to charge (debit) the customer's account via the ACH operator.
- Customer's financial institution debits the customer's account, and provides the funds to the merchant.

Transaction Processing

ECP transactions can be submitted for deposit to Chase Paymentech in the same file and using the same transaction division number (Merchant number) as credit card transactions. There are, however, preliminary steps which occur during the submission processing cycle prior to ECP transactions being deposited:

- Validation – mandatory for all ECP transactions and done with every deposit/prenote and verification request.
- Verification – optional and available for U.S. ECP only
- Pre-notification – optional and available for U.S. ECP only

Continued on next page

Transaction Processing, Continued

These preliminary steps are designed to provide a degree of confidence in the checking account information provided by your customer. They indicate if the information can be processed and/or if there is any negative history associated with the customer's account.

Validation occurs on every ECP transaction submitted to Chase Paymentech. The validation process includes format and data edit checks, bank routing number checks and comparison to Chase Paymentech proprietary internal negative file to prepare the transaction for a successful deposit.

The Chase Paymentech negative file contains millions of unique bank accounts.

Validation is designed to help merchants comply with NACHA rules and regulations by ensuring that there is no reported negative activity with that routing/bank account number: In addition, Validation can mitigate the risk of submitting bad ACH entries into the system, administrative type returns and financial losses.

	Notification of Change Database	Accuity File	Chase Paymentech Internal Negative File
Description	Looks for account information changes from the customer's bank	Determines whether the RDFI is legitimate and participates in ACH	Checks for routing and bank account numbers for negative and/or merchant specific returns history
Value Proposition	Chase Paymentech repairs the item before it is presented to the ACH	<ul style="list-style-type: none"> • Checks the validity of the routing number the customer provided • Determines whether Chase Paymentech will create a paper draft for straight through processing 	Mitigates the risk of ACH returns, rules violations, and fines

Preferred Delivery Method

For U.S. eCheck Processing, the merchant has a choice of the Preferred Delivery Methods listed below. Regardless of the delivery method used, if the transaction fails either Validation or optional Verification, it will be rejected and returned to the merchant.

- **ACH** – the attempt will be made to deposit the transaction via the ACH.
- **Facsimile Draft** – the transaction will be deposited as a facsimile (paper) draft
- **Best Possible** – the transaction will be deposited through the ACH system unless the consumer's bank is not an ACH participant at which time a facsimile draft will be created and deposited on behalf of the merchant. Refunds must be processed through the ACH system.

For Canadian eCheck Processing, Electronic Funds Transfer (EFT) is the only possible delivery method for all transactions.

Validation (U.S. and Canadian ECP)

The **validation** process, designed to reduce the number of returns, consists of two phases:

Phase 1 – Format and Data – If the format and data cannot be validated, the transaction will be returned to you with one of the following response codes:

Code	Description	Means...
100	Approved	Successfully approved
101	Validated	Account passed Paymentech negative file and data edit checks
102	Verified	Account passed external negative file
103	Pre-noted	Up front validation test
202**	Bad Amount Non-numeric Amount	Amount sent was zero, unreadable, over ceiling limit, or exceeds maximum Allowable amount.
203**	Zero Amount	Amount sent was zero
204**	Other Error	Unidentifiable error
238**	Invalid Currency	Currency does not match Paymentech merchant setup for division
239**	Invalid MOP for Division	Method of payment is invalid for the division
241**	Illegal Action	Invalid action attempted
244**	Invalid Encryption Format	Invalid encryption flag. Data is inaccurate.
247**	Check Conversion Data Error	Proper data elements were not sent for POP/ARC transactions
248**	Blanks Not Passed in Reserved Field	Blanks not passed in Reserved Field
253**	Invalid Transaction Type	Invalid transaction type for this order
519	On Negative File	Account number appears on SCAN negative file
750	Invalid Transit Routing Number	ABA transit routing number is invalid, fails check digit
751	Transit Routing Number Unknown	Transit routing number not on list of current acceptable numbers
752	Missing Name	Pertains to deposit transactions only
753	Invalid Account Type	Pertains to deposit transactions only
754	Account Closed	Bank account has been closed For PayPal – the customer's PayPal account was closed/restricted
755	No Account/ Unable to Locate	Does not match any account for the customer at the bank
756	Account-Holder Deceased	Customer or accountholder has died
757	Beneficiary Deceased	Beneficiary on account has died
758	Account Frozen	Transaction posting to account prohibited
759	Customer Opt-out	Customer has refused to Allow transaction For PayPal – the customer's billing agreement was cancelled
760	ACH Non-Participant	Banking institution does not accept ACH transactions
763	Invalid Account Number	Account number is incorrect
764	Authorization Revoked by Consumer	Customer has notified their bank not to accept these transactions

Continued on next page

Validation (U.S. and Canadian ECP), Continued

Code	Description	Means...
765	Customer Advises Not Authorized	Customer has not authorized bank to accept these transactions
766	Invalid CECP Action Code	Canadian ECP only Note: Invalid Action Code Valid Action Codes are: FPO start Refund Validate only Validate and Deposit
767	Invalid Account Number Format	Formatting of account number is incorrect (Canadian ECP only)
769	Account Non Convertible	Account is not eligible for ACH conversion and would include IAT (International ACH) Accounts
768	Bad Account Number Data	Invalid characters in account number
834	Unauthorized User	Method of payment is invalid for the division

**Available only on Paymentech Online Reporting

Phase 2 – Proprietary Databases and Negative Files

For **U.S. ECP**, the transaction is compared to the Federal Reserve and Accuity EpicWare File that contains records of all financial institutions in the United States assigned transit and routing numbers. This database is housed at Chase Paymentech and is updated monthly. The file serves as a filter to identify all inaccurate or unknown routing and transit number information submitted in the transaction file.

For **Canadian ECP**, the transaction is compared to the CPA Financial Institution File that contains a record of all deposit-taking financial institutions in Canada. This database is housed at Chase Paymentech and is regularly updated.

For **U.S. ECP**, the transaction is compared to Chase Paymentech's proprietary negative file. In doing so we are able to reject up-front those transactions most likely to be returned by the customer's bank because Chase Paymentech has previously seen a hard return on the account. This database is housed at Chase Paymentech and is updated daily.

If the transaction cannot be validated at this point, the transaction will be returned to you with one of the following reject response codes:

Continued on next page

Validation (U.S. and Canadian ECP), Continued

Code	Description	Means...	Related Return Code
751	Transit Routing Number Unknown	Transit routing number not on list of current acceptable numbers	N/A
754	Account Closed	Bank account has been closed For PayPal – the customer's PayPal account was closed/restricted	R02
755	No Account/ Unable to Locate	Does not match any account for the customer at the bank	R03
756	Account-Holder Deceased	Customer or accountholder has died	R15
757	Beneficiary Deceased	Beneficiary on account has died	R14
758	Account Frozen	Transaction posting to account prohibited	R16
759	Customer Opt-out	Customer has refused to Allow transaction For PayPal – the customer's billing agreement was cancelled	R10
760	ACH Non-Participant	Banking institution does not accept ACH transactions	N/A
763	Invalid Account Number	Account number is incorrect	R04

Additional Response Codes for transactions that cannot be validated are listed below:

Code	Description	Means...	Related Return Code
764*	Authorization Revoked by Consumer	Customer has notified their bank not to accept these transactions	R07
765*	Customer Advises Not Authorized	Customer has not authorized bank to accept these transactions	R10

* These Returns are merchant specific and are not shared by all merchants.

Verification (U.S. Only)

Once a U.S. ECP transaction has been Validated, **Verification** will be performed if requested. Verification is the process of electronically matching the routing number and account number information against the Certegy Distributed Negative File (DNF) . This file is owned by Certegy Check Services and hosted in the Chase Paymentech system which is updated daily.

Verification determines the following information:

- Any account which have unpaid checks outstanding
- Accounts that have been closed for cause by the customer's financial institution

Transactions that cannot be verified will be returned to you with the following response code:

Code	Description	Means...
519	On Negative File	Account number appears on Certegy DNF

Communicating Negative Information

Under the Fair Credit Reporting Act (FCRA), if the verification is negative merchants are required to politely and discreetly provide adverse notice to consumers who have been declined check processing. Consumers should be directed to contact Certegy Check Services directly per the instructions below to resolve any outstanding dispute and/or obtain additional detail regarding their check status.

Decline Notice Language

Content of Decline Notice:

Decline Notice

We're sorry, but we are unable to proceed with your transaction. Our decision was based in whole or in part on information obtained from Certegy Check Services, Inc. ("Certegy"). Certegy provides authentication and risk management services to merchants and businesses nationwide.

Certegy is unable to tell you the specific reasons for the denial decision made by us, but can give you the information contained in Certegy's file.

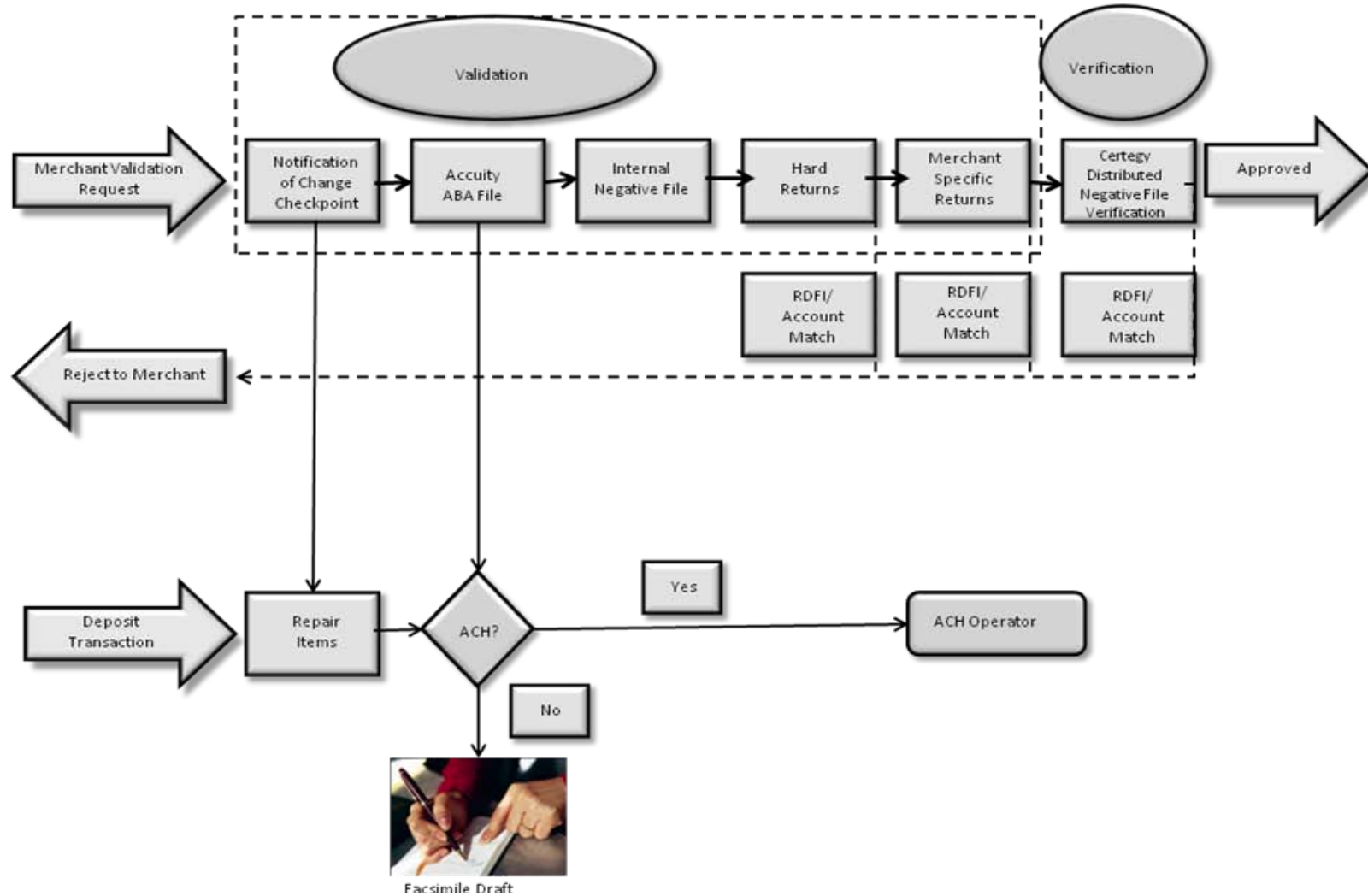
Under the Fair Credit Reporting Act, you have the right to obtain a free copy of your information held in Certegy's file, if you request it no later than 60 days after you receive this notice. In addition, if you find that any information in Certegy's file is inaccurate or incomplete, you have the right to dispute it with Certegy.

You may reach Certegy at www.askcertegy.com; toll free at 1-800-237-4851, or write to Certegy Check Services, Inc., P.O. Box 30046, Tampa, FL 33630-3046. If you contact Certegy, please provide the following information so they can respond promptly to your request:

- Full Name
- Driver's License Number and State
- Current Address
- Home Telephone Number
- Date Declined
- Date of Birth
- Dollar Amount
- Check/Draft/Transfer Number
- Merchant Name
- Checking Account Number
- Name of Financial Institution

Based on the Standard Entry Class Codes you may be utilizing, it is a requirement as per FCRA and your ECP Amendment that you incorporate the verbiage above in your telephone scripts, web sites and/or printed receipts in order to ensure you are in compliance with FCRA rules and communicating the appropriate adverse notice information to any consumer who has been denied check processing. FCRA states that declined consumers must be provided the Adverse Action notice in oral, written or electronic notice.

Validation, Verification and Deposit Flows via Chase Paymentech



Continued on next page

Prenotification (U.S. ECP only)

A **prenotification** or **prenote** is an optional non-dollar transaction sent through the ACH network by the Originating Depository Financial Institution (ODFI) to the Receiving Depository Financial Institution (RDFI) to verify the accuracy of the account data. As per NACHA rules, if a prenote is used, the live dollar entry cannot be sent through the ACH network until at least 6 banking days following the settlement date of a prenote entry.

The data in a prenote is identical to what will be contained in potential ECP transactions, with the exception of the dollar amount and the transaction type.

By regulation, merchants are not required to submit a prenote for preauthorized debits to a customer's account prior to submitting a live dollar transaction through the ACH system. A merchant may choose the prenote process as a way of determining the validity of the account.

Caution: Although NACHA rules require an RDFI (customer's bank) to provide returns and notification of change details on a prenote transaction, in practice not all RDFI's provide responses. Hence, the absence of a reply is not always indicative of a 'good account.' Please consider this market dynamic when evaluating the implementation of a prenote program.

Deposits

It is Chase Paymentech's goal to process transactions in the most efficient and cost-effective manner. The preliminary steps insure that the electronic check transactions presented for deposit conform to current processing standards and regulations in both the United States and Canada.

NACHA Operating Rules state that it is mandatory that all prenote and deposit transactions with the exception of POP must contain the customer's name in order to be processed by Chase Paymentech and must be a zero dollar transaction.

Facsimile Drafts (U.S. ECP only)

A **facsimile draft** is a document created by Chase Paymentech upon the request of a merchant and/or when the receiving bank is not a participant of an ACH association. The facsimile draft flows through the Federal Reserve's check clearing process rather than through the ACH network.

Facsimile drafts can be used for deposit transactions in the following situations:

- if the merchant has chosen "Facsimile Draft" (F) as the Preferred Delivery Method

OR

- if the customer's bank is not a participant in the ACH system and the merchant has chosen "Best Possible" (B) as the Preferred Delivery Method

A facsimile draft contains the same information as appears on the customer's check:

- ABA number of the customer's financial institution
 - the customer's account number
 - the customer's name
 - the name and address of the customer's financial institution
 - the date of the transaction
 - the amount of the transaction
 - the payee's (merchant's) name
-

Returns and Rejects

Introduction

As a merchant, you do all you can to insure the customer information transmitted to Chase Paymentech is correct and up-to-date. Even with all your efforts, certain transactions cannot be processed. These transactions, which are returned to the merchant, fall into the following two categories:

- **Returns** are generated by Chase Paymentech on the initial transmission of the file. Returns occur when a transaction fails front-end edit checks.
- **Rejects** (chargebacks) are generated by the customer's bank. The bank may return an item for a variety of reasons. There are, however, certain regulations with which the customer's bank must comply in order to return an item unpaid.

Returns

Electronic check returns are received by Chase Paymentech on a daily basis, usually within a few days of the initial transaction. NACHA rules state that an RDFI (issuing bank) can take up to 48 hours from the receipt of a transaction to return the entry for a valid return reason code.

ACH bank returns activity and any associated fees are reported on the standard, web-based financial reports, or in an electronic file format.

Refer to the ECP Financial Reporting section of this user guide for a discussion of these reports.

Returns, Redeposit and Dishonor Rules and Regulations

Item	ARC	POP	WEB, TEL, PPD, CCD
Timing of administrative hard returns	The RDFI must provide the return to the ODFI no later than the opening of business on the second banking day following the settlement date of the transaction.	The RDFI must provide the return to the ODFI no later than the opening of business on the second banking day following the settlement date of the transaction.	The RDFI must provide the return to the ODFI no later than the opening of business on the second banking day following the settlement date of the transaction.
Extended return deadlines for unauthorized Consumer and Corporate Debits	<p>ARC entries may be returned by the RDFI for up to 60 days following the settlement date of the original entry, for the following reasons:</p> <ol style="list-style-type: none"> 1. A stop payment order was placed on the source document. 2. Notice was not provided to the consumer in accordance with NACHA rules. 3. The source document was previously presented for payment. 4. The amount of the ARC entry was not accurately obtained from the source document. 	<p>POP entries may be returned by the RDFI for up to 60 days following the settlement date of the original entry, for the following reasons:</p> <ol style="list-style-type: none"> 1. Improper Source Document (not drawn on a consumer account). 2. Consumer did not authorize the debit. 3. The source document was previously presented for payment. 	<p>Unauthorized Consumer Entries (R07 and R10) Debit entries returned for response code R07 or R10 must be returned by the RDFI to the ACH Operator no later than the opening of business on the banking day following the 60th calendar following the settlement date of the original entry. If a consumer provides the RDFI with a "Written Statement" (WS), stating an ACH transaction was not authorized, or that authorization was revoked, the RDFI may transmit an adjustment entry (return) to the ODFI, no later than the opening of business on the banking day following the 60th calendar day following the settlement date of the original entry.</p> <p>Unauthorized Corporate Entries (R29) Corporate debit entries returned for response code R29 must be returned by the RDFI to the ACH Operator no later than the opening of business on the banking day following the 2nd calendar following the settlement date of the original entry.</p>

The 60 day right of return for consumer entries offers an automated process to return unauthorized debits through the ACH network but is in addition to, not in lieu of, the liabilities established under the warranty. Hence, the liability is not limited to the 60 day return time but limited only by the statute of limitations for breach of contract claims under the applicable state law which can be up to 7 years in some states.

(The right of return provides a means to simplify and automate the recovery of funds. However, ODFIs must understand that the warranty language within the Rules is broad and does not limit itself to the period of time in which an RDFI can recover funds through the ACH network. The ODFIs potential liability under the NACHA Rules for a breach of warranty is not limited to the returns time frame, but is instead, limited only by the statute of limitations for limitations for breach of contract claims under the applicable state law.)

Liability can potentially be less if provided so by relevant State Laws.

Continued on next page

Returns, Redeposit and Dishonor Rules and Regulations, Continued

Item	ARC	POP	WEB, TEL, PPD, CCD
Acceptable returns volumes			<p><i>On March 22, 2008, NACHA implemented new reporting requirements which require Originating Deposit Financial Institutions (ODFIs) to provide, when requested by NACHA, certain information about Originators that have return rates for unauthorized entries in excess of one percent. This rule also requires ODFIs to reduce the returns rate for any Originator to a rate below one percent within sixty days after receipt of the National Associations written request for information and maintain that return rate below one percent for an additional, 180 days. This amendment applies to all SEC codes.</i></p> <p><i>NACHA states that if a merchant exceeds a 1% threshold for ECP unauthorized returns in a 60 day window, the merchant is then subject to a "detail process" that NACHA has outlined they must follow to then prove that the return rate will be reduced in the future via steps and timelines outlined by NACHA.</i></p>

Continued on next page

Returns, Redeposit and Dishonor Rules and Regulations, Continued

Item	ARC	POP	WEB, TEL, PPD, CCD
<p>Dishonors</p>	<p>A return can be dishonored to the RDFI, if it was untimely and the ODFI or the merchant suffered a loss due to the untimely return, or if the return contained incorrect or incomplete information.</p> <p>Dishonored returns must be sent back to the customer's bank within 5 days of the settlement date of the return.</p> <p>The customer's bank may react to a dishonored item by</p> <ul style="list-style-type: none"> • Accepting the dishonor • Contesting the dishonor, or • Correcting the information and resubmitting the item <p>This sequence can occur <u>only</u> once.</p> <p>There is no additional recourse available to the parties within the ACH system once the cycle has been completed. Any disputes beyond this point must be handled outside of the ACH system. Arbitration, Collection and Compliance opportunities do not exist for ACH transactions.</p>	<p>A return can be dishonored to the RDFI, if it was untimely and the ODFI or the merchant suffered a loss due to the untimely return, or if the return contained incorrect or incomplete information.</p> <p>Dishonored returns must be sent back to the customer's bank within 5 days of the settlement date of the return.</p> <p>The customer's bank may react to a dishonored item by</p> <ul style="list-style-type: none"> • Accepting the dishonor • Contesting the dishonor, or • Correcting the information and resubmitting the item <p>This sequence can occur <u>only</u> once.</p> <p>There is no additional recourse available to the parties within the ACH system once the cycle has been completed. Any disputes beyond this point must be handled outside of the ACH system. Arbitration, Collection and Compliance opportunities do not exist for ACH transactions.</p>	<p>A return can be dishonored to the RDFI, if it was untimely and the ODFI or the merchant suffered a loss due to the untimely return, or if the return contained incorrect or incomplete information.</p> <p>Dishonored returns must be sent back to the customer's bank within 5 days of the settlement date of the return.</p> <p>The customer's bank may react to a dishonored item by</p> <ul style="list-style-type: none"> • Accepting the dishonor • Contesting the dishonor, or • Correcting the information and resubmitting the item <p>This sequence can occur <u>only</u> once.</p> <p>There is no additional recourse available to the parties within the ACH system once the cycle has been completed. Any disputes beyond this point must be handled outside of the ACH system. Arbitration, Collection and Compliance opportunities do not exist for ACH transactions.</p>

Redeposit of Returns for NSF and Uncollected Funds

Chase Paymentech can auto re-deposit (on a merchants behalf) returns for non-sufficient (R01) or uncollected funds (R09). The redeposit is based on the specific requirements of the merchant.

To provide a merchant greater flexibility in customizing the redeposit process, the redeposit time frame parameter can be set at the transaction division level and may have a value up to 99 calendar days, although Chase Paymentech recommends 5 banking days.

If the redeposit parameter is set to...	Redeposit will occur...
Blank	Never (the item will be returned to the merchant)
1	1 day after receipt of the returned item
2	2 days after receipt of the returned item
3	3 days after receipt of the returned item
↓	↓
Up to 99	Up to 99 days after receipt of the returned item

The Chase Paymentech system default parameter is 1 day. If the merchant does not opt to select another parameter, all initial returns for NSF (R01) and Uncollected Funds (R09) will be redeposit the next day. Please contact your Chase Paymentech Account Manager to modify your redeposit parameters.

If the redeposit parameter is set to 1 or above, Chase Paymentech will redeposit once those transactions returned for Insufficient Funds or Uncollected Funds.

Transactions that are returned a second time will be sent to you to seek an alternative method of payment.

Return Codes, Dishonor Codes and Response Actions (U.S. ECP Only)

The table below lists the Return Codes (shown with an R before the code), the Description indicating the reason for the original return, and the Response Actions applicable to the Return Codes.

Possible Response Actions for U.S. ECP Returns:

Continued on next page

Return Codes, Dishonor Codes and Response Actions (U.S. ECP Only), Continued

*The Response Action listed in the table below pertain to ACH Return Codes

A – Item will be automatically re-deposited once according to the prevailing value of the time frame parameter. If a merchant chooses not to redeposit these items (redeposit parameter set to blank), Response Action B will be followed.

B – Item will be returned to you to seek an alternate method of payment.

Return Code	Description	Response Action*
R01	Insufficient funds	A
R02	Account closed	B
R03	No account/unable to locate account	B
R04	Invalid account number	B
R05	Unauthorized debit to consumer account, using CCD entry class	B
R06	Returned per Originating Depository Financial Institutions request	B
R07	Authorization revoked by the customer	B
R08	Stop payment	B
R09	Uncollected balances	A
R10	Customer advises not authorized; (ARC, POP)- Notice not provided, Improper source document, Entry not accurately obtained from the source document	B
R11	Check truncation entry return (i.e., exceeds dollar limit, no match, stale dated check)	B
R12	Account sold to another financial institution	B
R14	Payee deceased or unable to continue in that capacity	B
R15	Beneficiary or account holder is deceased	B
R16	Account frozen	B
R17	File Record Criteria: Data edit causing processing error. Also used for an incorrectly coded IAT transaction.	B
R20	Non-transaction account	B
R23	Credit entry refused by the receiver	B
R24	Duplicate entry	B
R29	Corporate customer advises not authorized	B
R37	(ARC, POP) Source document presented for payment	B
R38	(ARC, POP) Stop payment received on source document	B

Continued on next page

Return Codes, Dishonor Codes and Response Actions (U.S. ECP Only), Continued

Return Code	Description	Response Action*
R39	(ARC, POP) Improper source document	B
R61	Misrouted return	B
R67	Duplicate return	B
R68	Untimely return	B
R69	Multiple errors	B
R70	Permissible return entry not accepted	B
R71	Misrouted dishonored returns	B
R72	Untimely dishonored return	B
R73	Timely original return	B
R74	Corrected return	B
R75	Original return not a duplicate	B
R76	No errors found	B

Return Codes and Response Actions (Canadian ECP only)

Return Codes and Response Actions for Canadian ECP returned items are listed below.

Possible Response Actions for Canadian ECP:

B – Item will be returned to you to seek an alternate method of payment.

Return Code	Description	Response Action*
R01	Insufficient funds	B
R02	Account closed	B
R03	No account/unable to locate account	B
R04	Invalid account number	B
R07	Agreement Revoked	B
R08	Stop payment	B
R09	Uncollected balances	B
R10	Customer advises not authorized; (ARC, POP)- Notice not provided, Improper source document, Entry not accurately obtained from the source document	B
R11	Check truncation entry return (i.e., exceeds dollar limit, no match, stale dated check)	B

Continued on next page

Return Codes and Response Actions (Canadian ECP only), Continued

Return Code	Description	Response Action*
R12	Account sold to another financial institution	B
R15	Beneficiary or account holder deceased	B
R16	Account frozen	B
R17	File Record Edit Criteria	B
R29	Not According to Agreement	B
R36	Return of Improper Debit Entry	B
R37	Source Document Presented for Payment	B
R38	Stop Payment on Source Document	B
R39	Improper Source Document	B

Return Codes Used by ACH Operators

Return Codes used by ACH Operators are listed below:

B – Item will be returned to you to seek an alternate method of payment.

Return Code	Description	Response Action*
R13	Invalid ACH Routing Number	B
R18	Improper Effective Entry Date	B
R19	Amount Field Error	B
R25	Addenda Error	B
R26	Mandatory Field Error	B
R27	Trace Number Error	B
R28	Routing Number Check Digit Error	B
R30	RDFI Not Participant in Check Truncation Program	B
R32	RDFI Non-Settlement	B
R34	Limited Participation DFI	B
R35	Return of Improper Debit Entry	B
R36	Return of Improper Credit Entry	B

Removing Accounts from the CPS Proprietary Negative File

In order to have an account removed from the CPS internal negative file, it is the responsibility of the merchant to request the removal of the account in writing and provide the necessary documentation to Merchant Services via FAX (see details below). It is a NACHA regulation that the documented request MUST come directly from the merchant and not from the bank to Chase Paymentech.

For merchant specific return codes on the internal negative file

- R07/Authorization Revoked,
- R10/Consumer Advises Not Authorized
- R29/Corporate Customer Advises Not Authorized

Step	Action
1	Merchant must obtain written authorization from the consumer indicating that the consumer is authorizing the removal of this hold on their account with the merchant.
2	Merchant must send a written request on company letterhead via FAX to Chase Paymentech Merchant Services at 603.896.8715 to have the account removed from the negative file. They must also provide a copy of the written authorization from the consumer which includes the following: <ul style="list-style-type: none">• Consumers name• Consumer's account number• RDFI (Routing and Transit Number) of the consumer's bank.
3	Merchant Services will follow up and make the necessary changes.

For the following return codes on internal negative file:

- R02/Account Closed
- R03/No Account/Unable to Locate
- R04/Invalid Account Number
- R14/Payee Deceased
- R15/Beneficiary or Account Holder Deceased
- R16/Account Froze

The following return codes will not appear on the Chase Paymentech's proprietary negative file:

- *R01/ Insufficient Funds*
- *R08/Stop Payment*
- *R09/Uncollected Funds*

Continued on next page

Removing Accounts from the CPS Proprietary Negative File, Continued

Step	Action
1	Merchant must contact the RDFI (issuing bank) and obtain written authorization that the hold has been released for that bank account.
2	Merchant must send a written request on company letterhead via FAX to Chase Paymentech Merchant Services at 603.896.8715 to have the account removed from the NEG file. They must also provide a copy of the written authorization from the consumer which includes the following: <ul style="list-style-type: none">• Consumers name• Consumer's account number• RDFI (Routing and Transit Number) of the consumer's bank.
3	Merchant Services will follow up and make the necessary changes.

Removing Accounts from the Certegy Distributed Negative File

To have an account removed from the Certegy Distributed Negative (CDN) File, the CONSUMER must contact Certegy directly for more detailed instructions. Please refer to the section on Verification eCheck Processing for full details:

You may reach Certegy at www.askcertegy.com; toll free at 1-800-237-4851, or write to Certegy Check Services, Inc., P.O. Box 30046, Tampa, FL 33630-3046. If you contact Certegy, please provide the following information so they can respond promptly to your request:

- Full Name
 - Driver's License Number and State
 - Current Address
 - Home Telephone Number
 - Date Declined
 - Date of Birth
 - Dollar Amount
 - Check/Draft/Transfer Number
 - Merchant Name
 - Checking Account Number
 - Name of Financial Institution
-

ECP Financial Reporting

Introduction

ECP deposit and return (and U.S. ECP dishonor) activity is reported on a variety of Chase Paymentech reports, the frequency of which can be customized to meet each merchant's need. Depending on which Chase Paymentech platform you are processing ECP (eCommerce or retail) you will be accessing the Paymentech Online (PTO) reporting tool to access your reports.

The table below describes these reports found in [Paymentech Online \(PTO\)](#), samples of which appear on the following pages.

Report ID	Report name	Page
ACT-0002	Exception Detail	31
FIN-0010	Deposit Activity Summary	34
FIN-0011	Service Charge Detail	37
PDE-0022	ECP Returns Received	41
PDE-0018	ECP Return Activity	43
ACT-0019	Notice of Change	50

PTO ECP Financial Reporting

Exception Detail (ACT-0002)



4 Northeastern Boulevard, Salem, NH 03079-1952
 Tel (603) 896-8333. Email: Merchant_Services@Chasepaymentech.com

Exception Detail (ACT-0002)

ABC Company, Inc. - CO# 123456

Currency Pair: Presentment: USD - U.S. Dollars/ Settlement: USD - U.S. Dollars

Reporting Period: From 08/10/XXXXthrough 08/10/XXXX

Submission Date/Time	Exception Type	PID #	PID Short Name	Submission #	Submission Status	Record #	Transaction Division #	Merchant Order #	RDFI #	Account #	Expiration Date
08/10/XXXX 11:03:00 AM	Rejected Transaction	#####	aaaa	#####	Accepted	#####	#####	#####		XXXXXXXXXXXXXXXXXXXX	
08/10/XXXX 12:30:49 PM	Rejected Transaction	#####	aaaa	#####	Accepted	#####	#####	#####		XXXXXXXXXXXXXXXXXXXX	
08/10/XXXX 02:03:57 PM	Rejected Transaction	#####	aaaa	#####	Accepted	#####	#####	#####		XXXXXXXXXXXXXXXXXXXX	
08/10/XXXX 05:19:06 PM	Rejected Transaction	#####	aaaa	#####	Accepted	#####	#####	#####		XXXXXXXXXXXXXXXXXXXX	
08/10/XXXX 07:07:09 PM	Rejected Transaction	#####	aaaa	#####	Accepted	#####	#####	#####		XXXXXXXXXXXXXXXXXXXX	
08/10/XXXX 07:07:09 PM	Rejected Transaction	#####	aaaa	#####	Accepted	#####	#####	#####		XXXXXXXXXXXXXXXXXXXX	
08/10/XXXX 07:07:23 PM	Rejected Transaction	#####	aaaa	#####	Accepted	#####	#####	#####		XXXXXXXXXXXXXXXXXXXX	
Total # Exception Transactions #				7							
Total Amount :				1,061.24							

Left Side of Report

Continued on next page

Exception Detail (ACT-0002), Continued

Exception #	Amount	MOP	Action Code	Auth Date	Auth Code	Auth Response Code	Consumer Bank Country Code	Trace Id	Reject Code
	57.44	??	AU						201
	20.00	??	AU						201
	584.53	??	AU						201
	171.81	??	AU						201
	75.82	??	AU						201
	75.82	??	AU						201
	75.82	??	AU						201

Right Side of Report

Field Definitions


Field	Definitions
Submission Date / Time	Date and time the submission containing the exception item was completely received by Chase Paymentech
Exception Type	Category of exception – Declined Deposit, Rejected Transaction or Canceled/On-hold item
PID# (Presenter ID)	Unique 6-digit number assigned by Chase Paymentech to a presenter for identification purposes
PID Short name	Name assigned to the PID by Chase Paymentech consisting of up to 6 characters. Used in conjunction with the PID # for identification purposes
Submission #	Unique number assigned to the submission when received by Chase Paymentech
Submission Status	Status of the submission – Accepted, Canceled or On-hold

Continued on next page

Exception Detail (ACT-0002), Continued

Field	Definitions
Record #	Sequential number of the exception item in the submission file
Transaction Division #	Number of the transaction division the exception item was processed under
Merchant Order #	Number assigned by the merchant and submitted to Chase Paymentech with the original sale transaction
RDFI #	Identification number of the Receiving Depository Financial Institution
Account #	Unique number identifying the consumer's account, i.e., Credit Card #, Checking or Savings Account #
Expiration Date	Date submitted by the merchant as to when the credit card expires
Amount	Amount of the exception item
MOP	Method of payment associated with the transactions, i.e., Visa, MasterCard, Discover, ECP, etc. A hyperlink to a HELP guide listing the full names of all MOPS
Action Code	Identifies the requested action for the transaction, i.e., A=Authorize, B=Conditional Deposit, D=Deposit, R=Refund, H=Validate and Deposit (ECP), etc.
Auth Date	Date the exception transaction was authorized
Auth Code	6-character Authorization code associated with the transaction
Auth Response Code	3-digit code indicating the reason for the declined authorization
Consumer Bank Country Code	Identifies the country in which the consumer's bank is located
Trace ID	6-digit number with a range of 000001 thru 999999 assigned on a rolling basis to identify a debit transaction
Reject Code	3-digit code assigned to rejected transactions that do not pass Chase Paymentech's front end edit routines

Deposit Activity Summary (FIN-0010)

 CHASE Paymentech						
4 Northeastern Boulevard, Salem, NH 03079-1952 Tel (603) 896-8333. Email: Merchant_Services@Chasepaymentech.com						
Deposit Activity Summary (FIN-0010)						
ABC Company, Inc. - CO# 12345						
Currency Pair: Presentation: USD - U.S. Dollars/ Settlement: USD - U.S. Dollars						
Reporting Period: From 08/10/XXXX through 08/10/XXXX						
Activity Summary						
	Submitted Transactions		Count	Amount		
Submissions Received = 2	CREDIT CARD AUTH ONLY		4,267	1,479,046.02		
Submissions Accepted = 2	Credit Card Deposits		4,257	1,528,225.84		
Submissions Cancelled = 0	ECP Ver/Val/Prenote		4	0		
	Rejected Items		4	811.99		
	Successful Deposits		4,257	1,528,225.84		
Financial Summary						
Successful Deposits	Sales Count	Sales Amount	Refund Count	Refund Amount	Total Deposit	Total Net Deposit
Total Successful Deposits	4,251	1,529,214.92	6	(989.08)	4,257	1,528,225.84
Settled Deposits						
VISA	3,115	990,409.91	5	(943.66)	3,120	989,466.25
MasterCard	1,010	374,475.66	1	(45.42)	1,011	374,430.24
ECP	4	750.00	0	0	4	750.00
Total Settled Deposits	4,129	1,365,635.57	6	(989.08)	4,135	1,364,646.49
Conveyed Deposits						
American Express	122	163,579.35	0	0	122	163,579.35
Total Conveyed Deposits	122	163,579.35	0	0	122	163,579.35
Fees & Adjustments Summary						
Total Settled Deposits Net Amount						1,364,646.49
Interchange & Assessment Fees						(23,638.21)
Paymentech Fees						(350.65)
Chargeback Adjustments						(265.68)

Continued on next page

Deposit Activity Summary (FIN-0010), Continued

Fees & Adjustments Summary						
ECP Return Adjustments						(1,500.00)
Total Fees & Adjustments						(25,754.54)
Net Financial Activity						1,338,891.95
Transfer Summary						
	FTI #	FT #	Net Activity Date Range	Effective Date	Transfer Amount	
Pending Transfers	#####	#####	08/09/XXXX thru 08/09/XXXX	08/11/XXXX	1,589,244.09	
	#####	#####	08/10/XXXX thru 08/10/XXXX	08/12/XXXX	1,338,891.95	
Effective Transfers	#####	#####	08/06/XXXX thru 08/06/XXXX	08/10/XXXX	1,428,675.69	
	#####	#####	08/07/XXXX thru 08/07/XXXX	08/10/XXXX	463,191.68	
	#####	#####	08/08/XXXX thru 08/08/XXXX	08/10/XXXX	292,563.90	
Total Effective Transfer						2,184,431.27

Field Definitions

Section	Field	Definitions
Activity Summary summary information on submissions received and submitted transactions	Submissions Received = x	Total number of submissions received by Chase Paymentech on behalf of the merchant
	Submissions Accepted = x	Total number of submissions received by Chase Paymentech that were accepted
	Submissions Cancelled = x	Total number of submissions received by Chase Paymentech that were cancelled
		Total count and amount of transactions in the submissions received by Chase Paymentech broken into the following categories: <ul style="list-style-type: none"> Credit Card Auth Only – transactions received via batch or online with an Action Code of A (Authorize Only) Debit Authorizations – transactions submitted for debit MOPs with an Action Code of A (Authorize Only) ECP/Ver/Val/Prenote – transactions that are verified, validated and/or prenoted as part of electronic check processing

Continued on next page

Deposit Activity Summary (FIN-0010), Continued

Section	Field	Definitions
Activity Summary summary information on submissions received and submitted transactions	Submitted Transactions	<ul style="list-style-type: none"> Rejected Transactions – transactions that failed to pass Chase Paymentech’s front-end edit checks Declined Deposits – transactions that received a negative authorization response from the card issuer Non-Financial Transactions – transactions, such as Gift Card, that have no financial impact Successful Deposits – Net amount of successfully deposited sale and refund transactions
	Financial Summary	
summary information on transactions received and processed successfully by Chase Paymentech during the reporting period	Total Successful Deposits	Summary totals of Sales Count and Amount, Refund Count and Amount, Total Deposit Count and Total Net Deposit Amount for all transactions successfully deposited with Chase Paymentech
	Settled Deposits	Summary totals by MOP (Method of Payment) of Sales Count and Amount, Refund Count and Amount, Total Deposit Count and Total Net Deposit Amount for all payment types settled by Chase Paymentech, i.e. Visa/Delta, MasterCard, Diners, JCB, Bill Me Later, Debit Cards and ECP
	Conveyed Deposits	Summary totals by MOP of Sales Count and Amount, Refund Count and Amount, Total Deposit Count and Total Net Deposit Amount for all conveyed transactions, i.e. AMEX, Discover/Novus, Diner’s/Carte Blanche
Summary of Fees and Adjustments includes totals of all fees and adjustments posted during the reporting period and the net financial activity for the reporting period	Total Settled Deposits Net Amount	Value of this field is same as that appearing on the Total Net Deposit Amount in the Activity Summary section of the report. This value is used in the calculation of the Net Financial Activity for the reporting period
	Interchange & Assessment Fees	Pass-through fees assessed by the card associations
	Chase Paymentech Fees	Fees assessed by Chase Paymentech for the processing of your transactions
	Chargeback Adjustments	Total of adjustments (both credit and debit) resulting from chargeback activity
	ECP Return Adjustments	Total of adjustments (both credit and debit) resulting from ECP return activity
	Debit Adjustments	Total of adjustments (both credit and debit) resulting from Debit return activity
	Other Adjustments	Total of other adjustments not related to chargebacks, ECP returns, or debit returns
	Total Fees & Adjustments	Total of all fees assessed and adjustments processed
	Net Financial Activity	Total Settled Deposits Net amount minus total Fees and Adjustments for the reporting period

Continued on next page

Deposit Activity Summary (FIN-0010), Continued

Section	Field	Definitions
Transfer Summary for the following categories: Pending Transfers Effective Transfers Total Effective Transfer	FTI#	Funds Transfer Instruction ID # - number for each transfer line item
	FT#	Funds Transfer # - unique funds transfer number assigned to each separate transfer
	Net Activity Date Range	Merchant activity date range for the financial events included in the transfer
	Effective Date	Date the transfer will reach the merchant's bank account
	Transfer Amount	Amount of each transfer
Transfer Summary (Row Labels and definitions)	Effective Transfers	Total value of funds transfers that have been confirmed and have a post date that falls within the reporting period
	Total Effective Transfers	Sum of all transfers that have been confirmed and have a post date that falls within the reporting period for the entity being reported on
	Pending Transfers	Total value of funds transfers in a "Ready", "In File", "Sent" or "Confirmed" status until the effective date has been reached

Service Charge Detail (FIN-0011)

Category/Description	Action Type	MOP	Interchange Qualification	Fee Schedule	Unit Quantity	Unit Fee	Amount	Rate	Total Charge
CHASE Paymentech 4 Northeastern Boulevard, Salem, NH 03079-1952 Tel (603) 896-8333. Email: Merchant_Services@Chasepaymentech.com									
Service Charge Detail (FIN-0011) ABC Company Inc. - CO# 12345									
Currency Pair: Presentation: USD - U.S. Dollars/ Settlement: USD - U.S. Dollars Reporting Period: From 08/10/XXXX through 08/10/XXXX									
Interchange & Assessment Fees									
MasterCard NABU Fee	Sale	MasterCard	M021	23695966	153	0.018500000	86,078.16	0.000000000	(2.83)
MasterCard NABU Fee	Sale	MasterCard	M68A	23695966	7	0.018500000	12,821.56	0.000000000	(0.13)
MasterCard NABU Fee	Sale	MasterCard	M68C	23695966	1	0.018500000	305.08	0.000000000	(0.02)
MasterCard NABU Fee	Sale	MasterCard	M781	23695966	89	0.018500000	34,844.66	0.000000000	(1.65)
MasterCard NABU Fee	Sale	MasterCard	MCH1	23695966	5	0.018500000	5,209.15	0.000000000	(0.10)
MasterCard NABU Fee	Sale	MasterCard	MCSA	23695966	15	0.018500000	12,274.69	0.000000000	(0.28)
MasterCard NABU Fee	Sale	MasterCard	MEMD	23695966	454	0.018500000	76,799.02	0.000000000	(8.40)
MasterCard NABU Fee	Sale	MasterCard	MRP1	23695966	104	0.018500000	40,852.77	0.000000000	(1.93)
MasterCard NABU Fee	Sale	MasterCard	MUC1	23695966	115	0.018500000	55,473.39	0.000000000	(2.13)
MasterCard NABU Fee	Sale	MasterCard	MWBI	23695966	64	0.018500000	48,040.58	0.000000000	(1.18)
MasterCard NABU Fee	Refund	MasterCard	MRD1	23695966	1	0.018500000	(45.42)	0.000000000	(0.02)
Visa Acquiring Processing Fee (APF)	Sale	VISA	NONE	23695966	3,158	0.019500000	1,024,075.70	0.000000000	(61.73)
Visa Interregional IAF fee (standard MCC)	Sale	VISA	V901	23695966	5	0.000000000	2,731.84	0.004500000	(12.29)
Visa Interregional IAF fee (standard MCC)	Sale	VISA	V905	23695966	1	0.000000000	89.71	0.004500000	(0.40)
Visa Interregional IAF fee (standard MCC)	Sale	VISA	V947	23695966	2	0.000000000	987.76	0.004500000	(4.44)
Total Interchange & Assessment Fees									(23,638.21)
Paymentech Fees									
Authorization Fees									
Online Authorization	Sale	VISA		23695966	3,158	0.025000000	1,024,075.70	0.000000000	(79.46)
eCheck Verification	Sale	ECP		23695966	4	0.060000000		0.000000000	(0.24)
Online Authorization	Sale	MasterCard		23695966	1,013	0.020000000	382,031.24	0.000000000	(20.73)
Online Authorization	Sale	American Express		23695966	96	0.020000000	92,939.08	0.000000000	(1.92)
Rejected Transact	Sale			23695966	4	0.025000000	811.99		(0.12)
Sub Total									(107.47)
Chargeback/ECP Return/Debit Adjustment Fees									
Chargeback Fee	Sale	VISA		23695966	1	5.000000000	(265.68)	0.000000000	(5.00)
Returns ACH Fee	Sale	ECP		23695966	1	1.500000000	(1,500.00)	0.000000000	(1.50)
Sub Total									(6.50)
Deposit Fees									
Settled Dep. Fee	Sale	VISA		23695966	3,115	0.035000000	990,409.91	0.000000000	(109.06)
Settled Dep. Fee	Refund	VISA		23695966	5	0.035000000	(943.66)	0.000000000	(0.18)
eCheck Deposit (ACH)	Sale	ECP		23695966	4	0.070000000	750.00	0.000000000	(0.28)
Settled Dep. Fee	Sale	MasterCard		23695966	1,010	0.035000000	37,417.50	0.000000000	(33.12)
Settled Dep. Fee	Refund	MasterCard		23695966	1	0.035000000	(45.42)	0.000000000	(0.04)

Continued on next page

Service Charge Detail (FIN-0011), Continued

Category/Description	Action Type	MOP	Interchange Qualification	Fee Schedule	Unit Quantity	Unit Fee	Amount	Rate	Total Charge
Paymentech Fees									
Deposit Fees									
Conveyed Dep. Fee	Sale	American Express		23695966	122	0.030000000	163,579.35	0.000000000	(3.66)
Sub Total									(148.64)
Other Fees									
Gateway Transaction Fee	Sale	VISA		23695966	3,158	0.020000000	1,024,075.70	0.000000000	(63.16)
Gateway Transaction Fee	Refund	VISA		23695966	5	0.020000000	(943.66)	0.000000000	(0.10)
Gateway Transaction Fee	Sale	ECP		23695966	4	0.020000000		0.000000000	(0.08)
Gateway Transaction Fee	Sale	MasterCard		23695966	1,013	0.020000000	362,031.24	0.000000000	(20.26)
Gateway Transaction Fee	Refund	MasterCard		23695966	1	0.020000000	(45.42)	0.000000000	(0.02)
Gateway Transaction Fee	Sale	American Express		23695966	96	0.020000000	92,939.08	0.000000000	(1.92)
Sub Total									(85.54)
Funds Transfer Fees									
ACH Transfer Fee					1	2.500000000			(2.50)
Sub Total									(2.50)
Total Paymentech Fees									(350.65)
Total All Fees									(23,988.86)

Field Definitions


Section	Field	Definitions
Interchange & Assessment Fees	Action Type	Type of transaction processed – a sale or a refund
	MOP	Method of payment associated with the transactions, i.e. Visa, MasterCard, Discover, ECP, etc. Hyperlinks to a HELP guide listing full names of all MOPS
Fees assessed by the card associations and passed through to the merchant by Chase Paymentech	Interchange Qualification	Interchange rate at which the transaction was qualified or the rate assessed for back-end downgrades, i.e. VRF, VCS, VPDM, MM1, MUCS, etc. Hyperlinks to a HELP guide listing all Interchange Qualifications
	Fee Schedule	Identification number assigned to the particular schedule of fees associated with the items
	Unit Quantity	Number of items processed during the reporting period that are being assessed the unit fee

Continued on next page

Service Charge Detail (FIN-0011), Continued

Section	Field	Definitions
Interchange & Assessment Fees Fees assessed by the card associations and passed through to the merchant by Chase Paymentech	Unit Fee	Fee per item (for the applicable Interchange rate) that is applied to the unit quantity in the calculation of the total charge for the line item
	Amount	Monetary value of the transactions included in the line item
	% Rate	Percentage applied to the amount (if applicable)
	Total Charge	Total of all Interchange & Assessment Fees assessed during the reporting period. Total charge equals: Unit Quantity x Unit Fee or Amount x % Rate or Unit Quantity x Unit Fee plus Amount x % Rate, if both are applicable
Chase Paymentech Fees Transaction and non-transaction fees assessed by Chase Paymentech. Individual fee categories are subtotaled within their section. A grand total of all fees appear at the end of the report. Fee Categories include: <ul style="list-style-type: none"> • Authorization Fees • Chargeback/ECP Return Fees • Deposit Fees • Equipment Fees • Funds Transfer Fees • Monthly Fees • PTI Non-Transaction Fees • Other (Miscellaneous) Fees 	Action Type	Type of transaction processed – a sale or a refund
	MOP	Method of payment associated with the transactions, i.e. Visa, MasterCard, Discover, ECP, etc. Hyperlinks to a HELP guide listing full names of all MOPS
	Fee Schedule	Identification number assigned to the particular schedule of fees associated with the items
	Unit Quantity	Number of items processed during the reporting period that are being assessed the unit fee
	Unit Fee	Fee per item (as indicated in the merchant's fee contracted fee schedule) that is applied to the unit quantity in the calculation of the total charge for the line item
	Amount	Monetary value of the transactions included in the line item
	% Rate	Percentage applied to the amount (if applicable)
	Total Charge	Total of all Interchange & Assessment Fees assessed during the reporting period. Total charge equals: Unit Quantity x Unit Fee or Amount x % Rate or Unit Quantity x Unit Fee plus Amount x % Rate, if both are applicable

ECP Returns Received (PDE-0022)

CHASE 		Paymentech		4 Northeastern Boulevard, Salem, NH 03079-1952 Tel (603) 896-8333. Email: Merchant_Services@Chasepaymentech.com									
ECP Returns Received (PDE-0022)													
ABC COMPANY, INC - CO#123456													
Currency Pair: Presentment: USD - U.S. Dollars/ Settlement: USD - U.S. Dollars													
Reporting Period: From 08/10,XXXX through 08/10/XXXX													
Sequence #	TD #	MOP Code	Consumer Bank Country Code	Merchant Order #	RDFI	Account #	Consumer Name	Reason Code	Original Transaction Date	Return Date	Activity Date	Return Amount	Return Cycle
#####	#####	EC		#####	#####	XXXXXXXXXXXX	NAME*ANY	R01	08/06/XX	08/10/XX	08/10/XX	1,500.00	1
Totals:											1	1,500.00	

Field Definitions

Field	Definitions
Sequence #	Number assigned by Chase Paymentech to the return transaction
TD #	Transaction Division number
MOP Code	Method of payment associated with the transactions, i.e. Visa, MasterCard, Discover, ECP, etc.
Consumer Bank Country Code	Identifies the country in which the consumer's bank is located
Merchant Order #	Order number assigned by the merchant and submitted to Chase Paymentech with the original sale transaction
RDFI	Identification number of the Receiving Depository Financial Institution
Account #	Consumer's checking or savings account number associated with the return
Consumer Name	Name on account associated with the return
Reason Code	Code indicating the reason the transaction was returned. Hyperlink to the ECP Return Codes Help Guide that lists all Return Codes and their descriptions

Continued on next page

ECP Returns Received (PDE-0022), Continued

Field	Definitions
Original Transaction Date	Date the original sale transaction was deposited with Chase Paymentech
Return Date	Date the return transaction was received by Chase Paymentech from the issuer
Activity Date	Date that action was taken to return item to merchant
Return Amount	Amount of the transaction being returned.
Return Cycle	Code that identifies the item as a first or second return

ECP Return Activity (PDE-0018)

		FINANCIAL SUMMARY	
		Return Count	Return Amount
BEGINNING WORK IN PROCESS		0	0.00
FINANCIAL ADJUSTMENTS		Return Count	Return Amount
Received	+	1	1,500.00
Re-Presented	-	0	0.00
Paymentech Adjustments	-	0	0.00
Subtotal		1	1,500.00
NON-FINANCIAL ADJUSTMENTS			
Returned to Merchant	-	0	0.00
Recourse	+	0	0.00
Subtotal		0	0.00
TOTAL WORK IN PROCESS ADJUSTMENT:		1	1,500.00
ENDING WORK IN PROCESS		1	1,500.00

Continued on next page

ECP Return Activity (PDE-0018), Continued

CHASE Paymentech												
4 Northeastern Boulevard, Salem, NH 03079-1952 Tel (603) 896-8333. Email: Merchant_Services@Chasepaymentech.com												
ECP Return Activity (PDE-0018)												
ABC Company, Inc. - CO# 12345												
Currency Pair: Presentment: USD - U.S. Dollars/ Settlement: USD - U.S. Dollars												
Reporting Period: From 08/10/XXXX through 08/10/XXXX												
DETAIL - RECEIVED												
Sequence #	TD #	MOP Code	Consumer Bank Country Code	Merchant Order #	RDFI	Account #	Consumer Name	Reason Code	Original Transaction Date	Return Received Date	Activity Date	Amount
#####	#####	EC		#####	#####	XXXXXXXXXXXXXXXXXX	NAME*ANY	R01	08/06/XX	08/10/XX	08/10/XX	1,500.00
RECEIVED TOTALS:											1	1,500.00
DETAIL - ENDING INVENTORY												
Sequence #	TD #	MOP Code	Consumer Bank Country Code	Merchant Order #	RDFI	Account #	Consumer Name	Reason Code	Original Transaction Date	Return Received Date	Activity Date	Amount
#####	#####	EC		#####	#####	XXXXXXXXXXXXXXXXXX	NAME*ANY	R01	08/06/XX	08/10/XX	08/10/XX	1,500.00
ENDING INVENTORY TOTALS:											1	1,500.00

Continued on next page

ECP Return Activity (PDE-0018), Continued

Field Definitions

Section	Field	Definitions
Financial Summary summarizes the financial impact to the ECP Returns Inventory for the reporting period	Beginning Work in Process	Lists the Return Count and Return Amount in Inventory at the beginning of the reporting period
	Financial Adjustments	Provides summarized totals for <ul style="list-style-type: none"> Returns Received by Chase Paymentech from issuers and added to Inventory during the reporting period Returns Re-Presented to the issuers by Chase Paymentech and deducted from Inventory during the reporting period Chase Paymentech Adjustments made during the reporting period Subtotal – net financial impact to Inventory due to the previous three line items. The impact to Inventory can be either positive or negative. The amount of the subtotal with the reversed sign (positive or negative) is indicated on the Deposit Activity Summary (FIN-0010) in the Financial Activity Section, on the ECP Return Adjustments line, and impacts the Net Activity amount for the reporting period.
	Non-Financial Adjustments	Provides summarized totals for <ul style="list-style-type: none"> Returns Returned to Merchant and deducted from Inventory, but with no financial impact to the merchant's Net Activity amount Recourse items – Previous Returned to Merchant items that the merchant is sending to Chase Paymentech for possible representment Subtotal – net impact to Inventory balance due to the previous two items. This amount does not impact the merchant's Net Activity amount for the reporting period.
	Total Work in Process Adjustments	Net amount of the Financial Adjustment Subtotal and the Non-Financial Adjustments Subtotal. This amount impacts the Inventory balance for the reporting period.
	Ending Work in Process	Lists the Return Count and Return Amount in Inventory at the end of the processing day. Ending Work in Process Count and Amount values are the sum total of the Beginning Work in Process and the Total Work in Process Adjustments line item amounts

Continued on next page

ECP Return Activity (PDE-0018), Continued

Section	Field	Definitions
Detail provides transaction-level detail of all return activity (Received, Re-presented, Returned to Merchant, Recourse and Ending Inventory) during the reporting period	Sequence #	Number assigned by Chase Paymentech to the return transaction <i>An "R" appearing before the Sequence # indicates a reversal of a previously processed transaction</i>
	TD #	Transaction Division number
	MOP Code	Method of payment associated with the transactions, i.e. Visa, MasterCard, Discover, ECP, etc.
	Consumer Bank Country Code	Identifies the country in which the consumer's bank is located
	Merchant Order #	Order number assigned by the merchant and submitted to Chase Paymentech with the original sale transaction
	RDFI	Identification number of the Receiving Depository Financial Institution
	Account #	Consumer's checking or savings account number associated with the return
	Consumer Name	Name on account associated with the return
	Reason Code	Code indicating the reason the transaction was returned. Hyperlink to the ECP Return Codes Help Guide that lists all Return Codes and their descriptions
	Original Transaction Date	Date the original sale transaction was deposited with Chase Paymentech
	Return Received Date	Date the return transaction was received by Chase Paymentech from the issuer
	Activity Date	Date that action was taken to return item to merchant
	Amount	Amount of the transaction being returned.
Return Cycle	Code that identifies the item as a first or second return	

Notification of Change

Introduction

A **Notification of Change (NOC)** is a non-dollar entry sent to Chase Paymentech by the consumer's bank. It is created in response to the bank receiving either a prenotification or a live dollar entry that contained incorrect information. The NOC instructs Chase Paymentech to change the information that is presented. The NOC serves the following purposes:

- to identify the entry that has been received by the bank
- to pinpoint the specific information on that entry that is incorrect
- to provide the correct information in a precise format so that the originator can make the necessary change or changes

Sources of incorrect information that result in a NOC can be

- obtained from the customer during the enrollment process, or
- changes made to the account by either the account-holder or their bank

A Notification of Change is informational. Receipt of an NOC does not prevent the transaction from being processed.

You will be notified of any Notifications of Change received by Chase Paymentech on your accounts via the ACT-0019 report.

Please update your records with the corrected information that appears on the Notification of Change Report to prevent problems with subsequent ECP transactions for your customers. If you choose not to make updates to your customer records, Chase Paymentech will update accounts found in our NOC database on your behalf and charge you a repair/deposit matching fee as per your Schedule A.

Correcting the information in your system will

- *ensure the efficient processing of subsequent ECP transactions*
- *minimize returns, and processing costs (repair fees)*

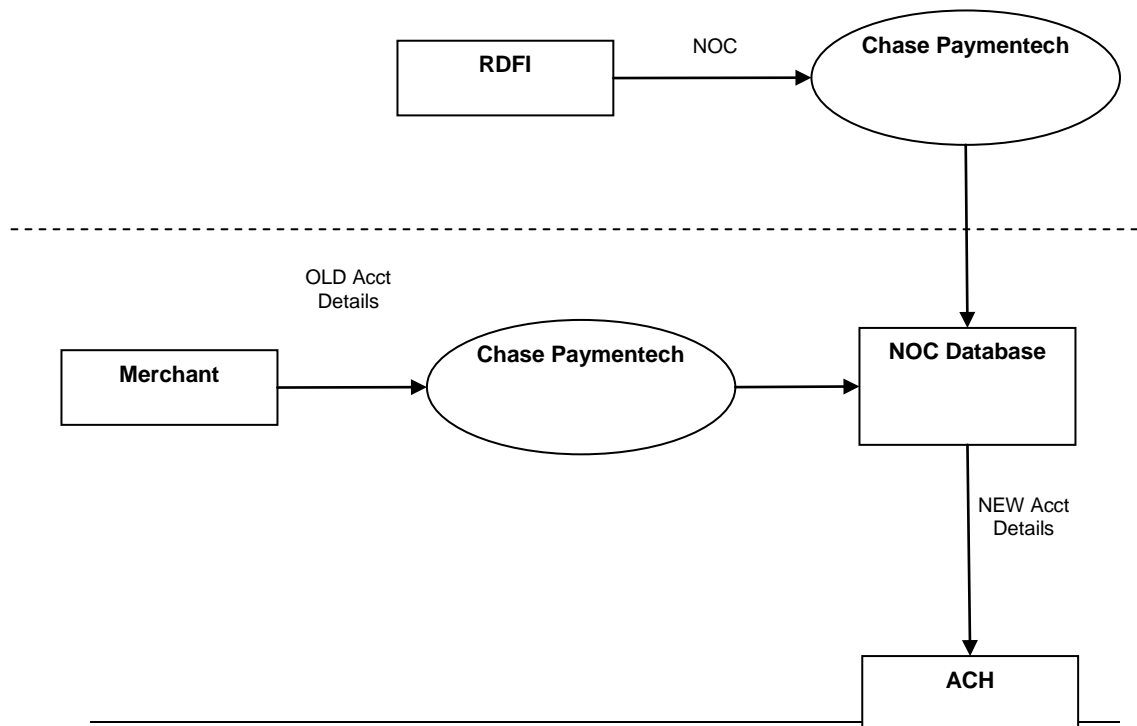
ARC	POP	WEB, TEL, PPD, CCD
Except for NOCs due to a bank merger, acquisition or other similar events, the RDFI must transmit the NOC within two (2) banking days of the settlement date of the entry to which the NOC relates.	Except for NOCs due to a bank merger, acquisition or other similar events, the RDFI must transmit the NOC within two (2) banking days of the settlement date of the entry to which the NOC relates.	Except for NOCs due to a bank merger, acquisition or other similar events, the RDFI must transmit the NOC within two (2) banking days of the settlement date of the entry to which the NOC relates.
Chase Paymentech will also make NOCs available to merchants within two banking days from the settlement date of the NOC.	Chase Paymentech will also make NOCs available to merchants within two banking days from the settlement date of the NOC.	Chase Paymentech will also make NOCs available to merchants within two banking days from the settlement date of the NOC.

Continued on next page

Introduction, Continued


All Notification of Change information is stored in our NOC database. Through the Deposit Matching (Repair) process, transaction information (account number, RDFI number, consumer name, account type) submitted by a merchant is matched to the information stored in the NOC database. Any necessary corrections are made so that the transaction will post correctly to the customer's account. A fee may be assessed for this matching service. Fines may be imposed for failure to respond to NOCs.

eCheck Deposit Matching (Repairs)



ECP Notification of Change (ACT-0019)

The Notification of Change Report (web-based or electronic file delivery) is non-financial in nature and consists of two sections. A sample NOC Report and its Field Definitions follow.

 4 Northeastern Boulevard, Salem, NH 03079-1952 Tel (603) 896-8333. Email: Merchant_Services@Chasepaymenttech.com										
ECP Notification of Change (ACT-0019) ABC Company, Inc. - CO# 123456										
Currency Pair: Presentation: USD - U.S. Dollars/ Settlement: USD - U.S. Dollars Reporting Period: From 06/09/XXXXthrough 06/09/XXXX										
TD # - ##### ABC-DIVISION-1										
Merchant Order #	Acct Type	RDFI #	Account Number	Consumer Name	Deposit Date	NOC Code	Change 1	Change 2	Change 3	Source
#####	CK	XXXXXXXX	XXXXXXXXXXXX	FIRST LAST	06/09/XX	C05	SV			Submission
#####	CK	XXXXXXXX	XXXXXXXXXXXX	FIRST LAST	06/09/XX	C02	#####			Submission
#####	CK	XXXXXXXX	XXXXXXXXXXXX	FIRST LAST	06/09/XX	C02	#####			Submission
#####	CK	XXXXXXXX	XXXXXXXXXXXX	FIRST LAST	06/09/XX	C01	#####			Submission
#####	CK	XXXXXXXX	XXXXXXXXXXXX	FIRST LAST	06/09/XX	C01	#####			Submission
#####	CK	XXXXXXXX	XXXXXXXXXXXX	FIRST LAST	06/09/XX	C02	#####			Submission
#####	CK	XXXXXXXX	XXXXXXXXXXXX	FIRST LAST	06/09/XX	C02	#####			Submission
#####	CK	XXXXXXXX	XXXXXXXXXXXX	FIRST LAST	06/09/XX	C01	#### - ####			Submission
#####	CK	XXXXXXXX	XXXXXXXXXXXX	FIRST LAST	06/09/XX	C01	#####			Submission
TD # - ##### ABC-DIVISION-2										
Merchant Order #	Acct Type	RDFI #	Account Number	Consumer Name	Deposit Date	NOC Code	Change 1	Change 2	Change 3	Source
#####	CK	XXXXXXXX	XXXXXXXXXXXX	FIRST LAST	06/09/XX	C02	#####			Submission
#####	CK	XXXXXXXX	XXXXXXXXXXXX	FIRST LAST	06/09/XX	C02	#####			Submission
#####	CK	XXXXXXXX	XXXXXXXXXXXX	FIRST LAST	06/09/XX	C02	#####			Submission
#####	CK	XXXXXXXX	XXXXXXXXXXXX	FIRST LAST	06/09/XX	C02	#####			Submission
#####	CK	XXXXXXXX	XXXXXXXXXXXX	FIRST LAST	06/09/XX	C02	#####			Submission
#####	CK	XXXXXXXX	XXXXXXXXXXXX	FIRST LAST	06/09/XX	C01	#####			Submission
TD # - ##### ABC-DIVISION-3										
Merchant Order #	Acct Type	RDFI #	Account Number	Consumer Name	Deposit Date	NOC Code	Change 1	Change 2	Change 3	Source
#####	CK	XXXXXXXX	XXXXXXXXXXXX	FIRST LAST	06/09/XX	C02	#####			Submission
#####	CK	XXXXXXXX	XXXXXXXXXXXX	FIRST LAST	06/09/XX	C01	#####			Submission
TD # - ##### ABC-DIVISION-4										
Merchant Order #	Acct Type	RDFI #	Account Number	Consumer Name	Deposit Date	NOC Code	Change 1	Change 2	Change 3	Source
#####	CK	XXXXXXXX	XXXXXXXXXXXX	FIRST LAST	06/09/XX	C02	#####			Submission
#####	CK	XXXXXXXX	XXXXXXXXXXXX	FIRST LAST	06/09/XX	C01	#####			Submission

Continued on next page

ECP Notification of Change (ACT-0019), Continued

Field Definitions

Field	Definitions
TD#/Name	TD# and name impacted by changes
Merchant Order Number	Order number assigned by the merchant and submitted to Chase Paymentech with the original sale
Account Type	Type of consumer's account: <ul style="list-style-type: none">• CK = Checking• CP = Corporate Checking• SV = Savings
RDFI	Receiving Depository Financial Institution – the bank where the transaction was sent
Account Number	Consumer's account number at the RDFI
Consumer Name	Consumer's name as provided in the original sale transaction
Deposit Date	Date the original transaction was processed by Chase Paymentech

Continued on next page

ECP Notification of Change (ACT-0019), Continued

Field	Definitions
NOC Code	3-digit code designating the reason the NOC was generated. <ul style="list-style-type: none"> • C01 Incorrect DFI Account Number • C02 Incorrect Routing Number • C03 Incorrect Routing Number and Incorrect DFI Account Number • C04 Incorrect Individual Name • C05 Incorrect Account Type • C06 Incorrect DFI Account Number and Incorrect Account Type • C07 Incorrect Routing Number, Incorrect DFI Account Number, and Incorrect Account Type • C61 Misrouted Notification of Change • C62 Incorrect Trace Number • C63 Incorrect Company ID • C64 Incorrect Individual ID Number • C65 Incorrectly Formatted Corrected Data • C66 Incorrect Discretionary Data • C67 Routing Number Not From Original Entry Data • C68 DFI Account Number Not From Original Entry Data • C69 Incorrect Transaction Code • C99 Miscellaneous
Change 1,2 and 3	Information the receiving bank is requesting to be changed to allow processing of the transaction in their system. Multiple changes are listed in Reason Code order
Source	Source of the NOC: <ul style="list-style-type: none"> • Returns = those returned from the receiving bank directly • Submission = those that are being changed by Chase Paymentech from previous NOC information stored in our database for the particular account
Entity Totals	Number of Changes in Submission and Returns categories

eCheck Funds Transfer Options

Available Options

The following funds transfer options are available for eCheck processing

Fed Wire:	1 day funds availability
ACH:	2 day funds availability
EFT (Canada):	2 day funds availability

eCheck Rules and Regulations

Regulatory Compliance

In order to implement a successful, ACH program, careful attention must be paid to regulatory compliance issues. The **Automated Clearing House (ACH)** network is subject to both federal regulation and industry rules and standards.

The legal framework:

- NACHA Operating Rules
- Electronic Funds Transfer Act & Regulation E
- Uniform Commercial Code; Article 4A (Paper Checks)
- Office of Foreign Asset Control
- Other State and Federal Laws

The **National Automated Clearing House Association (NACHA)** sets and governs the ACH industry rules and standards. **NACHA Operating Rules** recognize three acceptable authorization methods – Written, Internet (Web) and Telephone. Specific requirements for each method including the type of payment – single or recurring – appear below. ACH Authorizations must be obtained prior to debiting the consumer's account and must be retained by the merchant for a period of 2 years after the date of the final debit transaction.

Web Link: www.nacha.org

ACH Security Framework

Summary:

The ACH Security Framework Amendment which goes into effect September 2014, creates a framework within the *NACHA Operating Rules (Rules)* aimed at protecting the security and integrity of certain ACH data throughout its lifecycle. The Security Framework establishes minimum data security obligations for ACH Network participants to protect ACH data within their purview.

Specifically, the Framework:

- requires non-consumer Originators, Participating DFIs, Third-Party Service Providers and Third-Party Senders to establish, implement and, as appropriate, update security policies, procedures, and systems related to the initiation, processing and storage of Entries and resulting Protected Information;

Background:

Currently, the *NACHA Operating Rules* contain a number of data security and authentication requirements for ACH transactions that are generally based on individual Standard Entry Class (SEC) Codes and/or triggering events. The marketplace has changed since these security requirements were included in the *Rules* many years ago. Sound industry practices now reflect the understanding that certain financial data should be protected at all times – whether before, during or after transmission, and regardless of the form of transmission (e.g., by Internet or otherwise). By establishing minimum data security obligations, the ACH Security Framework changes will benefit the ACH Network by reducing the potential for both out-of-pocket losses experienced by ACH participants and their customers, and the damaging effect of data breaches on the reputation of the ACH Network and its participants.

KEY COMPONENTS OF RULE AMENDMENT

The ACH Security Framework amendment consists of three elements: (1) Protection of Sensitive Data and Access Controls; (2) Self-Assessment; and (3) Verification of Third-Party Senders and Originators.

Protection of Sensitive Data and Access Controls

The Security Framework requires all non-consumer Originators, Participating DFIs (as both ODFIs and RDFIs), Third-Party Service Providers, and Third-Party Senders to comply with specific security requirements with respect to the handling and storage of Protected Information. The security requirements will not apply directly to consumers, who can be Originators of CIE entries; however, such security requirements will apply to parties originating CIE Entries on behalf of consumers (i.e., the consumer's financial institution or a Third-Party Sender). Under this rule, non-consumer Originators, Participating DFIs, Third Party Service Providers, and Third-Party Senders will be required to establish, implement, and, as appropriate, update security policies, procedures, and systems related to the initiation, processing, and storage of entries. These policies, procedures, and systems must:

- (1) protect the confidentiality and integrity of Protected Information;
- (2) protect against anticipated threats or hazards to the security or integrity of Protected Information; and
- (3) protect against unauthorized use of Protected Information that could result in substantial harm to a natural person.

The security policies, procedures, and systems of ACH participants covered by the Security Framework must include controls on system access that comply with applicable regulatory guidelines. The impacted systems include all of those used by the ACH participant to initiate, process, and store entries must include controls on system access that comply with applicable regulatory guidelines.

Guidelines for Authorization Methods

Method	Code	Requirements
TEL – Single and Recurring ACH transfers	T	<p>TEL authorizations may be obtained orally via the telephone. If authorization is for a one time payment Originators are obligated to either tape record the consumer’s oral authorization OR to provide on advance of the settlement date of the entry, written notice to the consumer that confirms the oral authorization. If the authorization is for recurring transactions. Originators MUST provide BOTH a copy of the recording and a copy of the written confirmation message.</p> <p>A voice response unit (VRU) used to capture consumer information does not qualify as an oral authorization. A VRU may be used by the consumer to enter data provided that the actual authorization by the consumer is provided orally.</p> <p>If written notice is provided, the following 6 criteria MUST be included:</p> <ul style="list-style-type: none"> • Date consumer’s account will be debited • Amount of debit entry • Consumer’s name • Tel number available for customer inquires • Date of consumer’s oral authorization • Statement by the Originator that the authorization obtained from the receiver will be used to originate an ACH debit entry to the consumer’s account • Oral authorization must contain the following for both recurring and one-time TEL transactions: <ol style="list-style-type: none"> 1. Date on or after which the ACH debit will occur. 2. Amount of transaction or reference to the method of determining the amount of the transaction. 3. Receiver’s name or identity. 4. Account to be debited. 5. Telephone number for Receiver inquiries. 6. Date of Receiver’s oral authorization. 7. Statement that it’s a single entry (single authorizations only). <p>All authorizations must be retained by the Originator for a period of 2 years from the cancellation or revocation of the authorization for recurring or from the settlement date for 1 time.</p>
Debit Only		

Continued on next page

Guidelines for Authorization Methods, Continued

Method	Code	Requirements
Internet (Web) – Single and recurring transactions	I	<p>Authorization is obtained from the Receiver via the Internet. Must be identifiable as an ACH Debit authorization, clearly state the terms and provide (for recurring transactions) the method to revoke the authorization.</p> <ul style="list-style-type: none"> • Written authorization that is signed or similarly authenticated by the Receiver. • Be readily identifiable as an ACH debit authorization in clear concise language
Debit Only		<ul style="list-style-type: none"> • For recurring payments, must provide the Receiver with a method to revoke the authorization • Originator should prompt the consumer to print the authorization and retain a copy for their records.
Mobile	I	<p>All authorizations must be retained by the Originator for a period of 2 years from the cancellation or revocation of the authorization for recurring or from the settlement date for 1 time.</p> <ul style="list-style-type: none"> • NACHA has expanded the definition of WEB entries to include debit entries authorized and/or initiated via Wireless Networks in accordance with WEB SEC Code guidelines. • NACHA has revised the definition of “Unsecured Electronic Network” to include wireless networks in the case where an authorization is communicated from the Receiver to the Originator via the Internet or a Wireless Network. This does not include an authorization taken via an oral communication.
Debit Only		<ul style="list-style-type: none"> • Because SMS/Text messages do not include native encryption, their use of transmitting banking information to initiate an ACH debit would not be supported unless those messages were encrypted with a security technology that, at a minimum is equivalent to 128-bit RC4 encryption technology. • In the future, NACHA may develop a dedicated SEC Code to MOBILE debit entries when the volume can justify the investment. • Originators and Processors that do not already use the WEB SEC Code for MOBILE ACH debits could begin doing so as soon as possible, but must use WEB no later than the effective date of January 1, 2011.

Continued on next page

Guidelines for Authorization Methods, Continued

Method	Code	Requirements
PPD (Written) (Prearranged Payment and Debit) – Single and recurring transactions Credit and Debits	W	<p>Primarily used for recurring payments, but can also be used for single transactions. Requires one-time debit authorization to be provided by consumer. The following rules apply:</p> <ul style="list-style-type: none"> • Authorization may be obtained via telephone or in person. • Used for recurring or one time debit entries • Authorization must be by the consumer via a document that is signed or similarly authenticated. Copy MUST be sent to the consumer. • The authorization must clearly and conspicuously state its terms; I (consumer name) authorize (company name) to initiate debit entries monthly to checking account number indicated below). • Can be used for multiple non recurring debits where amounts and time frames vary. Originators need not obtain a written authorization for each debit provided they have established a written authorization up front that establishes that activity. <p>All authorizations must be retained by the Originator for a period of 2 years from the cancellation or revocation of the authorization for recurring or from the settlement date for 1 time.</p>
Retail Point of Purchase (POP) Single transactions Debit Only	P	<p>The physical check is written authorization and the source document for the transaction. The following conditions apply:</p> <ul style="list-style-type: none"> • The check has not been previously negotiated, voided, or used in a previous POP transaction • Is drawn on a consumer account and has an amount less than \$25,000 • Unacceptable source checks: <ul style="list-style-type: none"> – Checks or sharedrafts that contain an Auxiliary On – Us Field in MICR Line (effective 9/15/06) – Third Party – Credit Card – Cashiers Check, Money Order, Travelers Check, official checks) – Checks drawn on the U.S. Treasury, State and/or Federal Government – Non-U.S.\$ Currency – Checks drawn on an investment company as defined in the Investment Company Act of 1940 <p>All authorizations must be retained by the Originator for a period of 2 years from the date of the authorization</p>

Continued on next page

Guidelines for Authorization Methods, Continued

Method	Code	Requirements
Accounts Receivable Conversion (ARC) – Single transactions Debit Only	A	Used by merchants for the conversion of a consumers check received via U.S. Mail, or at an unattended lockbox location. The physical check is written authorization and the source document for the transaction. The following conditions apply; <ul style="list-style-type: none"> • The check has not been previously negotiated, voided, or used in a previous ARC transaction • Is drawn on a consumer account and has an amount less than \$25,000 • Unacceptable source checks: <ul style="list-style-type: none"> – Checks or share drafts that contain an Auxiliary On –Us Field in the MICR Line (effective 9/15/06) – Third Party – Credit Card – Cashier’s Check, Money Order, Travelers Check, official checks) – Checks drawn on the U.S. Treasury, State and/or Federal Government – Non-U.S.\$ Currency – Checks drawn on an investment company as defined in the Investment Company Act of 1940 All authorizations must be retained by the Originator for a period of 2 years from the date of the authorization.

Regulations and Industry Standards for U.S. ECP

The **Electronic Funds Transfer Act (Reg E)** states that preauthorized electronic fund transfers from consumer accounts must be authorized only by a writing signed or similarly authenticated by the consumer. A copy of the authorization must be supplied to the consumer.

Web Link: <http://www.federalreserve.gov>

Corporate to corporate electronic payments are not subject to Regulation E, however, NACHA rules state there must be an agreement between the parties.

Facsimile draft merchants may be subject to the Federal trade Commission’s Telemarketing Sales rule and/or the Uniform Commercial Code, Title 3.

Continued on next page

Regulations and Industry Standards for U.S. ECP, Continued

According to the Federal Trade Commission, the term telemarketing means a plan, program, or campaign which is conducted to induce the purchase of goods or services by use of one or more telephones and which involves more than one interstate telephone call.

The term telemarketing **does not include**:

- the solicitation of sales through the mailing of a catalog which
- contains a written description or illustration of the goods and services for sale
- includes the business address of the seller
- includes multiple pages of written material or illustrations, and
- has been issued not less frequently than once a year
- the solicitation of sales where the person making the solicitation does not solicit customers by outbound telephone calls, but only receives inbound calls initiated by customers in response to the catalog and during these calls only takes orders without further solicitation

The **Uniform Commercial Code (UCC), Title 3** applies to merchants choosing facsimile drafts that are exempt from the requirements of the FTC's Telemarketing Sales Rule. The UCC Rule states that it is legal and acceptable for an individual to verbally authorize a merchant to endorse a check or facsimile draft on his/her account.

Debit Authorization Rules

Item	Consumer Debit				
Debit Authorization	<p>Must be in writing, signed, or similarly authenticated; clear and conspicuous in terms and conditions</p> <ul style="list-style-type: none"> • TEL – either debit authorization must be tape recorded or a written notice must be provided to the consumer confirming the authorization. Recurring TEL entries always requires a written notice. • WEB – debit authorization must be obtained from the consumer over the Internet and similarly authenticated • PPD – written agreement is required via telephone or in person. Primarily used for recurring transactions. • ARC – notice equals authorization; no signed authorization is required. (The check is the source document) • POP – notice equals authorization; no signed authorization is required. (The check is the source document) • CCD – the receiver must have an agreement with the originator of the debit. All Business to Business transactions must be coded CCD with the exception of POP and ARC • Except for POP, ARC and single entry WEB and TEL payments, a merchant must provide the consumer with information on how to revoke debit authorization 				
Document Retention	<p>Minimally two years from the termination date for recurring, or the date of the debit transaction for 1 time.</p> <p>If the <u>amount</u> of the debit will change, the merchant must minimally provide 10 calendar days advance notice to the consumer of the new debit amount.</p> <p>If the date of the debit will change, the merchant must minimally provide the consumer 7 calendar days advance notice of the new date.</p> <table border="1" data-bbox="456 1150 1425 1667"> <tbody> <tr> <td data-bbox="456 1150 727 1440">ARC</td> <td data-bbox="727 1150 1425 1440">The source document is scanned/imaged and a copy of the source document must be retained for a period of 2 years from the settlement date. It is up to the merchant's discretion to determine how long to retain the original source document and to establish the appropriate policies and procedures to eventually destroy the original source documents. Merchants are encouraged to destroy source documents as soon as is reasonable to protect against the risk of fraud.</td> </tr> <tr> <td data-bbox="456 1440 727 1667">POP</td> <td data-bbox="727 1440 1425 1667">The source document is scanned and the original is returned to the consumer at the POS marked VOID; the Originator may not key enter the MICR information from the check – must be machine captured. The consumer signs a receipt giving authorization for the POP debit; authorization must be retained for two years from settlement date.</td> </tr> </tbody> </table>	ARC	The source document is scanned/imaged and a copy of the source document must be retained for a period of 2 years from the settlement date. It is up to the merchant's discretion to determine how long to retain the original source document and to establish the appropriate policies and procedures to eventually destroy the original source documents. Merchants are encouraged to destroy source documents as soon as is reasonable to protect against the risk of fraud.	POP	The source document is scanned and the original is returned to the consumer at the POS marked VOID; the Originator may not key enter the MICR information from the check – must be machine captured. The consumer signs a receipt giving authorization for the POP debit; authorization must be retained for two years from settlement date.
ARC	The source document is scanned/imaged and a copy of the source document must be retained for a period of 2 years from the settlement date. It is up to the merchant's discretion to determine how long to retain the original source document and to establish the appropriate policies and procedures to eventually destroy the original source documents. Merchants are encouraged to destroy source documents as soon as is reasonable to protect against the risk of fraud.				
POP	The source document is scanned and the original is returned to the consumer at the POS marked VOID; the Originator may not key enter the MICR information from the check – must be machine captured. The consumer signs a receipt giving authorization for the POP debit; authorization must be retained for two years from settlement date.				

Continued on next page

Debit Authorization Rules, Continued

Item	Consumer Debit	
Document Retention, continued	TEL	The tape recording and/or confirmation message must be retained by the Originator for a period of 2 years from the cancellation or revocation of the authorization for recurring or from the settlement date for 1 time.
	WEB	The authorization is obtained over the Internet and must be similarly authenticated. Originator should use commercially reasonable methods of authentication to verify the identity of the Receiver. The authorization proof must be retained by the Originator for a period of 2 years from the cancellation or revocation of the authorization for recurring or from the settlement date for 1 time.
	PPD	Written agreement must be retained for 2 years following termination or revocation of agreement.

Other Relevant Rules and Regulations

Item	Consumer Debit	
ARC	<ul style="list-style-type: none"> • Checks or sharedrafts that contain an Auxiliary On–Us Field in the MICR line • Less than \$25,000 in value • MICR line information must be machine read (scanned) • The check must contain a pre-printed check number • The payee name and check serial number must be submitted to ACH • A notice must be provided to the consumer that their check will be converted into an electronic payment, and funds could be deducted from their account as soon as same day • Checks drawn on an investment company as defined in the Investment Company Act of 1940 	
POP	<ul style="list-style-type: none"> • Checks or sharedrafts that contain an Auxiliary On – Us Field in the MICR line • No \$ amount limitation • MICR line information must be machine read (scanned) • The check must contain a pre-printed check number • The payee name is not required • The Terminal City and State ID must appear on the customer receipt and account statement • Notice must be provided to the consumer that their check will be converted into an electronic payment, and funds could be deducted from their account as soon as same day • Checks drawn on an investment company as defined in the Investment Company Act of 1940 	
WEB	<ul style="list-style-type: none"> • Consumer debits only • Consumer authorization must be obtained over the Internet and be similarly authenticated • Used for Single Entry and Recurring Payments 	

Continued on next page

Other Relevant Rules and Regulations, Continued

Item	Consumer Debit
WEB, continued	<ul style="list-style-type: none"> • Merchants must: <ul style="list-style-type: none"> ○ deploy fraud detection systems; ○ verify routing number (Chase Paymentech Validation) ○ verify consumer identity, and ○ maintain a secure Internet session with the consumer, minimally using 128-bit RC4 encryption • Perform periodic website security audits • Can be initiated against a consumer account only
TEL	<ul style="list-style-type: none"> • Consumer authorization must be tape recorded or the originator may choose to provide a written notice confirming the consumer's oral authorization for a single entry • Recurring entries require both a written notice sent to the consumer and tape recording .of the authorization. • Can occur when there is a pre-existing relationship with the customer; or there is no pre-existing relationship, but the consumer initiated the call to the merchant • Merchants must <ul style="list-style-type: none"> ○ deploy fraud detection systems; ○ verify routing number (Chase Paymentech Validation), and ○ verify consumer identity via some consumer authentication process
PPD (Prearranged Payment and Debit)	<ul style="list-style-type: none"> • Primarily used for recurring payments, but can also be used for single transactions; popular within the mortgage, insurance, and auto finance industries. Requires 1 time debit authorization in writing to be provided by consumer. • Also used for "credit" transactions to consumer accounts.
Proof of debit authorization	<p>Reg E rules allow the consumer and the consumer bank, to request proof of debit authorization from the merchant, up to two years from termination, or the date of the final transaction.</p> <p>Therefore, NACHA rules mandate that merchants must retain copies of authorization for up to 2 years from the termination or revocation of agreement. Failure to provide proof of debit authorization when requested is a violation of NACHA rules and a finable offense.</p>
Regulation E	<p>Reg E establishes the rights and liabilities of consumers and financial institutions regarding electronic funds transfers (EFT).</p> <ul style="list-style-type: none"> • Transfer of funds via an electronic terminal, telephone, computer, or magnetic tape, for the purposes of ordering, authorizing, or instructing a financial institution to debit/credit a bank account. <p>What activities are covered by this regulation?</p> <ul style="list-style-type: none"> • Check Conversion to ACH • Internet and Telephone ACH Payments • Prearranged Payments and Deposits (PPD) <p>Consumer Liability</p> <ul style="list-style-type: none"> • The customer is only liable if they were previously provided the required disclosures and their identity was verified • Limitation on liability for (consumer) unauthorized transfers: <ul style="list-style-type: none"> ○ \$50.00 or lesser amount if the customer notifies their bank within two days of learning of the loss

Continued on next page

Other Relevant Rules and Regulations, Continued

Item	Consumer Debit
Regulation E, continued	<ul style="list-style-type: none"> ○ Up to \$500.00 if they fail to notify their bank within two days of learning of the loss ○ The 60 day right of return offers an automated process to return unauthorized debits through the ACH network but is in addition to, not in lieu of, the liabilities established under the warranty. Hence, the liability is not limited to the 60 day return time but limited only by the statute of limitations for breach of contract claims under the applicable state law which can be up to 7 years in some states. <p><i>The right of return provides a means to simplify and automate the recovery of funds. However, ODFIs must understand that the warranty language within the Rules is broad and does not limit itself to the period of time in which an RDFI can recover funds through the ACH network. The ODFIs potential liability under the NACHA Rules for a breach of warranty is not limited to the returns time frame, but is instead, limited only by the statute of limitations for breach of contract claims under the applicable state law.</i></p> <p>Liability can potentially be less if provided so by relevant State Laws</p> <p>Consumer Disclosures</p> <ul style="list-style-type: none"> • Must be provided to consumers prior to the first transfer • A telephone number and address must be provided for customer inquiries and complaints • Consumer receipts must (minimally) contain the following details: <ul style="list-style-type: none"> ○ Amount ○ Date of Purchase, or on/after the debit will occur ○ Account Number ○ Merchant (terminal) location <p>Check Conversion (POP and ARC)</p> <ul style="list-style-type: none"> • Notice plus going forward = authorization (Reg E authorizes the merchant to process a check as a source document for EFT, by using the information on the check) • Merchants must provide disclosure to the consumer that their source document (check) will be converted to an electronic ACH transaction, and that funds may be debited for their account as soon as same day the merchant receives the payment • Obtaining a single authorization from the consumer is sufficient to convert multiple checks submitted after receiving an invoice or during a single billing cycle
Uniform Commercial Code impacts	<ul style="list-style-type: none"> • Governs the processing of Facsimile (paper) drafts • Facsimile Drafts are not subject to NACHA rules, or Regulation E. They are however subject to Uniform Commercial Code, Articles 3 and 4 • Merchants should only process Facsimile Drafts (via Chase Paymentech) if the bank is not a participant in the ACH system, or processing an item as ACH is a violation of NACHA rules (e.g. outbound telemarketing)

Uniform Commercial Code

The Uniform Commercial Code (UCC) consists of 10 Articles that outline regulations concerning commercial transactions. Articles 3 (Negotiable Instruments) and 4 (Bank Deposits and Collections) govern check processing and associated liability.

It is important to understand the legal ramifications of the UCC and the responsibilities it imposes upon your company.

UCC

Article 3 – Negotiable Instruments

Article 4 – Bank Deposits and Collection

UCC Index of all Articles

Who is Liable?

Although per UCC section 4–401 a bank is generally liable to its customer for checks it pays that are not “properly payable, changes to the UCC in 1990 place more responsibility for check fraud losses upon companies and not banks. Merchants generally will have more liability for check fraud losses than previously thought!

Generally, a check is not “properly negotiable” if a signature on it is forged or unauthorized. The following outlines the liable parties associated with check fraud. Caution: the following is not intended to be a complete compilation nor is it intended to be legal advice from Chase Paymentech

Forged Drawer’s Signature

Since a forged signature on a check, whether on a counterfeit or genuine check, is not an authorized signature the check would not be “properly negotiable”. If a bank clears a check with a forgery the bank is ultimately liable for the loss.

Altered Dollar Amount

Any check that is altered in dollar amount is also not negotiable. The customer is usually liable for up to the original amount of the check and the bank is liable for the amount in excess of the original amount.

Altered Payee

For checks with an altered payee, the bank and not the customer is generally held liable for losses.

Forged Endorsements

Forged endorsements create a check that is not properly negotiable. The depository bank is liable for losses because they should know their customer and they are responsible for verifying the payee’s signature.

Exceptions to the UCC Allocations Rules

Although under the general loss allocation rules the bank and not the customer assume losses from checks not properly payable, there are exceptions to the rules, which can shift liability for losses to the customer.

Continued on next page

Uniform Commercial Code, Continued

Failure to Exercise Ordinary Care

If a customer's failure to exercise "ordinary care" contributes to the forgery or alteration then the customer can be held liable for any losses.

Tardiness in Reporting

If a customer fails to promptly discover and report instances of forgery or alterations to its checks it can be held liable for losses. The UCC states that reporting of fraudulent items should occur within a reasonable time from the receipt of their bank statement, usually considered 30 days.

Imposters

The imposter rule imposes liability for losses on the party who was tricked by the imposter.

Fictitious Payee

If an employee writing checks creates a fictitious vendor, or employee, and deposits these checks into bank accounts under the name of the fictitious party then the merchant is liable for these checks.

Employee is Fraudulent Endorser

Companies are always better suited than banks to uncover fraud within their own companies. If an employee fraudulently endorses either the name of the company or of a third party, the endorsement is in essence effective.

Uniform Commercial Code – Industry Best Practices

Internal Corporate Controls

While each merchant's circumstances and operations are unique, controls must be implemented to increase the security of a company's assets and information. Adequate controls will minimize the risk of losses from check fraud.

Segregation of Duties

One recommendation is the segregation of operational activities- so that one individual doesn't have the ability to initiate and record check activity. Segregated roles for expense approval, record keeping, check-signing and account reconciliation must be maintained. Industry best practices suggest that minimally two employees should be involved in the check paying process.

Reconcile Bank Accounts

Per the UCC companies can be liable for check fraud losses if bank account reconciliation and fraud reporting do not occur within 30 days of receipt of the statement. Reconciliation is proven to be one of the best measures to identify fraudulent transactions.

Continued on next page

Uniform Commercial Code – Industry Best Practices, Continued

Timely Reporting of Fraud

The UCC states that to exercise ordinary care a company must discover and report unauthorized or altered checks within a reasonable period of time, no more than 30 days. A Company also has three years to discover and report forged endorsements.

Train Reconciliation Employees

Employees who perform the reconciliation process should be trained on how to identify fraud, from an accounting perspective as well as how to identify forged and altered checks. When reconciling, fan through the returned checks. A counterfeit check may stand out because it was printed on different colored check stock or the signature and fonts on the check may appear visually different than your authorized checks.

Periodic Audits

A party independent of the process should perform periodic audits of the check process (A/P, Payroll, etc.).

Securely Store Facsimile Signatures, Records, Documents

Bank account details, records and documentation should also be securely stored with limited access to such records.

Require Multiple Signatures for Large Dollar Checks

A threshold dollar amount should be established that requires two signers for all checks that meet or exceed that threshold.

Centralize Disbursement Operations

The headquarters location should control disbursement account, check processing and accounts reconciliation. With fewer individuals involved in the disbursement process, the lower the likelihood of unauthorized disbursements. Idle cash will also be reduced if excess cash is concentrated from local banks into centralized account(s).

Know Your Employees

It is important that you know the background of the employees who are responsible for cash related activities. Reference checking should be performed before hiring and for selected positions, further background checks may be warranted.

Electronic Payments

Moving paper based payments to electronic form is a great way to reduce check fraud. By reducing the distribution of checks, which contain all the information (account number, ABA number, etc.) a criminal needs to create fraudulent checks, you reduce the likelihood that this information will fall into the wrong hands. Automated Clearing House (ACH) electronic payments work very well for repetitive payee applications such as payroll or T&E (employees) and accounts payable (vendors). Working with your bank you can restrict ACH debit activity on your accounts.

Regulations and Industry Standards for Canadian ECP

The **Canadian Payments Association Rule H1 for Pre-Authorized Debits** is a continuing but revocable written authority given by the customer to the merchant that authorizes the merchant to issue preauthorized debits against the customer's account at the customer's bank and specifies whether such preauthorized debits are made for personal/household or business purposes.

A merchant must obtain written authorization from the customer prior to initiating a debit transaction through Chase Paymentech in order to be in compliance with the rules established by the Canadian Payments Association.

For Canadian EFT payments please refer to the H1 Rules for more details.

Appendix A

Overview

This Appendix contains the following:

- Supported Entry Classes
- ACH Authorization Authentication Guidelines
- Sample Debit Authorization
- Sample Web Authorization Page
- Sample Check Deposit Flow Chart for U.S. ECP
- Sample Check Deposit Flow Chart for Canadian ECP
- Sample Telemarketing Script for U.S. ECP
- Components of a Personal Check
- Components of a Business Check – Parsing the MICR line data
- Business checks ineligible for conversion

Continued on next page

Supported Entry Classes

Application Name	Entry Class Code	Description	B2B or B2C
Accounts Receivable Conversion	ARC	Single Entry (one time) debits initiated to convert a source document (a check) into an ACH debit. The source document must be delivered via the U.S mail, or at a drop box location. Examples: loan payments, credit card payments, utility payments...	B2C
Corporate Credit or Debit	CCD	Entries are single or recurring debits or credits used for corporate to corporate cash management purposes. Examples include company collection of funds from operating branches into a single account, or the payment of a single invoice. Often these transfers replace the use of depository transfer checks or expensive wire transfers.	B2B
Point of Purchase Conversion	POP	Single entry debits used at the point of purchase (or bill payment kiosk). The check becomes the source document for capturing the MICR (customer's bank account information) data, and for creating the debit entry (thus converting the check into an ACH debit).	B2C
Prearranged Payment and Deposit	PPD	Entries may be debit or credit entries for single or recurring authorizations, used to collect or to pay funds to consumer accounts. A typical bill payment application would involve a written authorization for recurring debits. Examples include: payment for insurance premiums, utility bills, mortgage payments, subscriptions, membership dues, loan payments, monthly pledges, rents, leases, and tuition payments... Although the purchase may be transacted via telephone, authorization and banking information were provided via a separate written authorization	B2C
Telephone Initiated Entries	TEL	Single Entry or Recurring Entry debits authorized by consumers over the telephone for paying a bill, or for the purchase of goods and services. Examples include: charitable donations mail order purchases, collection of late bill payments or credit card payments.	B2C
Internet Initiated Payments	WEB	Single Entry or Recurring debits authorized by customers over the internet for the purchase of goods, or services, or to pay bills. Examples include: purchase of consumer items such as CD's, books, clothes, electronic equipment, software, bill payment at merchants website.	B2C

* Source: *NACHA 2001 Operating Guidelines*

Components of a Personal Check

John & Nancy Smith ❶
111 Your Street ❷
Anytown, USA Zip

Check No. 1234 ❸

Date _____
1-8
210

Pay to the
Order Of _____ \$ _____
Dollars

First National Bank ❹
Anytown, USA Zip

For _____ Authorized Signature

❺ ❻

⑆ 0 3 1 0 9 8 7 6 5 4 ⑈ ⑆ 2 3 4

KEY:

1. Customer name or names
2. Customer address
3. Check number – usually appears both in upper corner and in the MICR imprinting along the bottom of the check
4. Customer account number
5. Routing/Transit Number
6. Bank Name and address

Components of a Business Check – Parsing the MICR Line Data

SAMPLE CHECK

NETZERO MEMBER
123 NOWHERE LANE, APT 1
SOMEWHERE, NY 00001

Date _____

Pay to the order of _____ \$ _____
Dollars

Memo _____

⑆ 1 2 3 4 5 6 7 8 9 ⑈ ⑆ 0 9 8 7 6 5 4 3 2 1 0 ⑈ 0101

Routing number appears first and is always 9 digits
⑆ 1 2 3 4 5 6 7 8 9 ⑈

Account Number may vary in length and may include dashes
⑆ 0 9 8 7 6 5 4 3 2 1 0 ⑈

Do not include check number. It may appear before or after your account number
0101

Business Checks Ineligible for Conversion

NACHA – 2006 Rules Changes

Introduction

Checks will be ineligible...

if they contain an auxiliary On-Us field in the MICR line **14** and are written for an amount greater than \$25,000



Auxiliary On-Us Field

Routing Number

Account Number

The auxiliary On-Us field is the 6 to 10 position field found to the left of the routing number on the check MICR line.

There is an auxiliary On-Us field only on business size (7½ to 9 inch) checks.

Due to the presence of an auxiliary On-Us field, this sample check will not be eligible for check conversion to ACH.

The Amendment

The amendment does not affect RCK.

The RDFI will need to send/make available a check serial number for each entry to the business Receiver via periodic statements.

The new Return Reason Code R39 (Improper Source Document) signifies that the RDFI can return the item in a normal time frame; no WSUPP is required.

Methods for Receivers to Opt-Out

Change check stock to checks that contain an auxiliary On-Us field

Contact the Originator directly to opt-out of ARC or refuse to sign an authorization for POP at point-of-sale

Continued on next page

Business Checks Ineligible for Conversion, Continued

Impact on Originators

- Must establish procedures to identify checks with auxiliary On-Us fields
 - Must establish procedures to identify checks over \$25,000
 - Zeropass processors
 - Create substitute check
 - Pull item for review
 - Expect some returns from debit blocks
 - Currently originators must allow opt-out
 - Applies to all subsequent checks
 - Database of R29s
-

Appendix B

Overview

This Appendix contains the following:

- Positive Reason Codes
 - Authorization Declines
-

Positive Reason Codes

Code	Error Description	Comments
100	Approved	Successfully Approved
101	Validated	Account passed Chase Paymentech negative file and data edit check
102	Verified	Account passed external negative file
103	Pre-noted	Passed pre-note (see note below)

A value of 100, 101, or 102 will be returned in the Host response to the original prenotification request if successful. Prenotification occurs at the time of deposit and the final approval (code 103) will show in the merchant's eCheck reporting, not in the online Host response.

Authorization Declines

Code	Error Description	Comments
519	On Negative File	Account number appears on negative file
750	Invalid Routing Transit Number	Routing Transit number is invalid, fails check digit
751	Routing Transit Number Unknown	Routing transit number not on list of current acceptable numbers
754	Account Closed	Bank account has been closed
755	No Account/Unable to Locate	Does not match any account for the customer at the bank
756	Accountholder Deceased	Customer or accountholder has died
757	Beneficiary Deceased	Beneficiary on account has died
758	Account Frozen	Transaction posting to account prohibited
759	Customer Opt-Out	Customer has refused to allow transaction
760	ACH Non-participant	Banking institution does not accept ACH transactions
763	Invalid Account Number	Account number is incorrect
764	Authorization Revoked by Customer	Customer has notified their bank not to accept these transactions
765	Customer Advises Not Authorized	Customer has not authorized bank to accept these transactions
767	Invalid Account Number Format	Formatting of account number is incorrect
769	Account Non-Convertible	The account presented by the customer cannot be processed as an ECP transaction
834	Invalid MOP for Transaction Division	ECP was not correctly set up on the Salem system

Best Practice FAQs

Rules and Regulations – Unauthorized Returns

Question	Answer
As a merchant, what do I need to know regarding the NACHA requirements for unauthorized returns in excess of 1%?	<p><u>Network Enforcement Rule:</u> On March 22, 2008, NACHA implemented reporting requirements which require merchants to provide, when requested by NACHA, certain information for unauthorized entries in excess of one percent. The Network Enforcement Rule requires merchants to reduce the returns rate to a rate below one percent within sixty days after receipt of the National Associations written request for information and maintain that return rate below one percent for an additional, 180 days. This amendment applies to all SEC codes.</p> <p>NACHA states that if a merchant exceeds a 1% threshold for ECP unauthorized returns in a 60 day window, the merchant is then subject to a "detail process" that NACHA has outlined they must follow to then prove that the return rate will be reduced in the future via steps and timelines outlined by NACHA.</p>
Unauthorized Returns - Definition	<p>R05, Unauthorized Debit to Consumer Account Using Corporate Standard Entry Class Code</p> <p>R07, Authorization Revoked by Customer (adjustment entries)</p> <p>R10, Customer Advises Not Authorized, Notice Not Provided, Improper Source Document, or Amount of Entry Accurately Obtained from Source Document (adjustment entries)</p> <p>R29, Corporate Customer Advises Not Authorized</p> <p>R51, Item is Ineligible, Notice Not Provided, Signature Not Genuine, Item Altered, or Amount of Entry Not Accurately Obtained from Item (adjustment entries)</p>
How is the 1% threshold for unauthorized returns calculated?	Simply put, NACHA divides 60 days worth of transaction requests by 60 days worth of total returns.

Continued on next page

Rules and Regulations – Unauthorized Returns, Continued

Question	Answer
Am I subject to a fine by NACHA if I exceed the 1% allowance for unauthorized returns?	<p>Only if the merchant has violated the time frames set forth by NACHA to explain their plan or put the necessary measures in place to maintain a < 1% return rate per the NACHA schedule are they then fined by NACHA. Any merchant, who has exceeded the 1% allowance, has 10 days to show NACHA the process they are using for authorizing and authenticating their consumers and produce a detail plan specific to how they will improve their process. In reality, the fines are not tied directly to any volume of unauthorized returns a merchant may experience, but rather to their inability to meet the NACHA follow up process to put an effective plan in place in a time frame determined by NACHA that can sustain a <1% return rate over time.</p> <p>Below is the detail merchant time table per NACHA <i>Operating Rules</i>:</p> <ul style="list-style-type: none">• 10 day clock begins with the notification from NACHA to the ODFI• Within 60 days after receiving notice from NACHA the merchant will be required to reduce the unauthorized entries below the one percent rate <p>The merchant must maintain that return rate below one percent for an additional 180 days.</p>
What are the fines specifically for unauthorized returns?	<p>Below is an example of the NACHA fine policy in the event that a merchant has exceeded the 1% return rate and is unable to comply with supplying NACHA with the appropriate information requested above in a timely manner:</p> <ul style="list-style-type: none">• Class 1 – First Recurrence - a maximum of \$1,000• Second Recurrence – a maximum of \$2,500• Third Recurrence – a maximum of \$5,000• Class 2 – a maximum of \$100,000 per month• Class 3 – a maximum of \$500,000 per month <p>In Class 3 rule violation situations where fines have been unsuccessful in resolving the issues causing the violation, Suspension from the ACH network may occur.</p>

Continued on next page

Rules and Regulations – Unauthorized Returns, Continued

Question	Answer
<p>What reporting requirements am I subject to by NACHA if I exceed the 1% return rate?</p>	<p>Both the ODFI and merchant are required to respond back to NACHA with specific reporting requirements within a 10 day window:</p> <p>The following are the ODFI's reporting requirements:</p> <ul style="list-style-type: none"> • Originator's volume for the time period specified by NACHA • The actual return rate for unauthorized entries, in total and by SEC Code, for the Originator that process through the ACH network • A statement either (1) refuting NACHA's claim that the Originator exceeded the return threshold or (2) explaining the reason causing the excessive returns <p>Merchant Reporting Requirements:</p> <ul style="list-style-type: none"> • A detailed plan and time line for reducing the Originator's return rate for entries returned as unauthorized • The address, telephone number, contact person, principal owner and officer of the Originator • A description of the nature of the business of the Originator • The length of the ACH relationship between the ODFI and the Originator • The complete legal name, any doing-business-as name and taxpayer identification number of the Originator
<p>What are some best practices to help me avoid being fined for unauthorized returns?</p>	<ul style="list-style-type: none"> • Monitor the unauthorized return rate weekly • Contact the consumer to understand why the authorization was not recognized • Pay attention to a consumer's notice to stop automatic debits – create a process to update systems • Develop a plan to reduce the rates if the returns are due to fraud <ol style="list-style-type: none"> 1. Enhanced authentication – confirms accuracy of consumer name, address and phone number 2. Engage third party to confirm above plus Date of Birth and/or Social Security # 3. Know your ECP customers

Continued on next page

Rules and Regulations – Unauthorized Returns, Continued

Question	Answer
What steps can I take to help me manage the amount of unauthorized returns?	<ol style="list-style-type: none">1. Ensure Proper Authorization is obtained from each client2. Enhance document retention practices to provide proof of proper authorization3. Consider “call back process” to confirm authorization4. Ensure Proper use of SEC when originating transactions. i.e. CCD should only be used for Corporate Accounts5. Review check conversion rules to ensure only approved source documents are converted to ACH6. Ensure timely Opt out process in place to ensure clients are removed from “ACH” “billing” etc.7. Perform data validation of routing numbers (required for TEL and WEB entries) and account numbers by utilizing verification resources i.e. Fed ABA list and check verification/guarantee services.8. Initiate pre-notification or trial deposits to ensure valid account at Receiving Depository Financial Institution.9. For Internet Initiated Entries:<ol style="list-style-type: none">a. Improve customer authentication practices by asking for several forms of identifying information and check that information against databases, ask challenge questions based upon credit bureau or other information.b. Send the consumer a specific piece of information, either online or offline such as a \$.01 entry into their bank account before initial ACH entry then ask consumers to verify that information as a second step in the authentication process.c. Enhance fraudulent transaction detection systems by tracking payment history, behavior, purchase type, delivery information, etc.10. Use originator name identifying information (as per company name field new rules) that clearly shows receiver who is debiting account11. Visit the following websites: for updated rule changes and other helpful information12. www.electronicpayments.org13. www.nacha.org

Continued on next page

Rules and Regulations – Unauthorized Returns, Continued

Question	Answer
I am seeing a high volume of “requests to provide proof of an original authorization from issuing banks. Why?	<p>It could be for several reasons, however, the 3 most common are:</p> <ol style="list-style-type: none">1. The merchant description that is printing out on the consumer’s bank statement does not clearly identify the merchant and/or the goods or services purchased. Therefore, the consumer is oftentimes confused why their account was debited and will request authorization proof. An example of a generic descriptor that some merchants have used, causing consumer’s confusion is “Services” or “Consumer.” It is strongly encouraged that all merchants make sure the “descriptor” (10 digit field) they choose is easily identified by their consumers and can be related to the company/merchant name or goods/services purchased.2. The consumer did not really want the goods/services and felt pressured in some way to agree initially to the transaction. Again, it is strongly encouraged that any merchant who is using an ECP MOP, should know their consumers.3. Your consumer authentication practices may need to be re-examined and possibly enhanced to protect you against malicious activity.
How long does a consumer have to request a return or unauthorized payment?	<p>In accordance with NACHA, the 60-day right of return offers an automated process to return unauthorized debits through the ACH network.</p> <p>In addition, REG E states that a consumer has 90 days from the date of their bank statement to request an unauthorized return.</p> <p>However, it should be noted that the NACHA ruling is in addition to, not in lieu of, the liabilities established under the ACH Network warranty. The NACHA language does not limit itself to the period of time in which an RDFI can recover funds through the systemic process.</p> <p>Hence, the liability is really not limited to the 60 day return time but limited only by the statute of limitations for breach of contract claims under the applicable state law which can be up to 7 years in some states.</p>

ECP Processing and Implementation

Question	Answer
According to NACHA, what does “similarly authenticate” mean?	<p>The term “signed” or “similarly authenticated” means that the agreement was physically signed by the Receiver or that an electronic signature such as a pin or password has been used to authenticate the Receiver and authorize the transaction. The authentication method chosen must evidence both the signer's identity and his assent to the terms of the record. When using TEL or WEB, the consumers' identity cannot be verified face to face, therefore additional methods must be used in order to authenticate both parties in the transaction:</p> <p>Example: WEB Entries:</p> <ul style="list-style-type: none">• Shared password or pin that only the consumer and merchant have access to:• Multiple step password process by which consumer must validate password via clicking on a separate email sent by the merchant to the consumers designated email address after to activate the password.• Send the consumer a specific piece of information, either online or offline such as a \$.01 entry into their bank account before initial ACH entry then ask consumers to verify that information as a second step in the authentication process• Multiple questions/answers of personal questions:<ul style="list-style-type: none">– Mother's maiden name– Favorite pet– Father's middle name– State born in– Current street name– Oldest child's name <p>Example: TEL Entries:</p> <ul style="list-style-type: none">• Consumer must explicitly authorize the debit entry orally via the telephone confirming they agree to the transaction. A silent response is not valid.• Company is obligated either to tape record the oral authorization, or, to provide, in advance of the Settlement date, written notice to the consumer that confirms the oral authorization, to include”:<ul style="list-style-type: none">– Date of authorization and date and amount of debit– Consumer's name and telephone number for consumer inquiries– Statement that the authorization will be used to originate a debit to the consumers account.

Continued on next page

ECP Processing and Implementation, Continued

Question	Answer
<p>Is Authorization the same as an Authentication?</p>	<p>No, "Authorization" is the permission a consumer gives either in writing or orally, that allows a transaction to be processed. "Authentication," goes to the origin or source of the order and confirms identity. You must have BOTH in order for authorization to be valid!</p> <p>An example of an "Authentication Statement" is:</p> <ul style="list-style-type: none"> • I am Ann Smith • I am Ann Smith, holder of bank account number XXXX-XXXX-XXXX <p>An example of an "Authorization Statement" is:</p> <ul style="list-style-type: none"> • I authorize this debit • This electronic check transaction is authorized
<p>Am I charged both a "Validate" and "Deposit" fee?</p>	<p>No, if a transaction is rejected/returned at the "validation" stage, then you are charged an eCheck Reject Fee. If, however, the validation is approved and the transaction moves on to the deposit stage, then you are only charged a "deposit" fee. In other words, you are charged either a reject fee or deposit fee, not both.</p>
<p>When should I use the "verification" process?</p>	<p>The verification stage is an optional process for every merchant. We recommend that in addition to the "validation" stage of every ECP transaction, merchants request the verification process for those consumers they are doing business with for the first time in order to ensure you are doing everything possible to reduce the risk of a returned transaction.</p>
<p>Does a pre-note transaction verify that there are sufficient funds in a consumers account for me?</p>	<p>Basically, there is no transaction that can verify account balance for a merchant via the ECP process prior to a deposit transaction. A pre-note transaction does not verify sufficient funds. A pre-note does, however, verify the following:</p> <ul style="list-style-type: none"> • status of an account – open/closed • accuracy of a consumer's account number • account type <p>Once a pre note transaction is submitted, the merchant MUST wait 6 business days before sending in the actual transaction according to NACHA rules. This waiting time will be reduced to 2 business days in 2014 with a new rule amendment.</p>
<p>How long does it take for an ECP transaction to go through the entire validation/deposit process and the information is available for me to view on line?</p>	<p>Assuming that there are no returns or re-deposits required, a merchant should see their transaction detail on their on line reports within 5 business days of the initial transaction. In those cases where a re-deposit may be needed or a return has been initiated, this detail information can still be found on their online reports within the 5 business days but a final deposit may not be complete depending on the action required by the merchant.</p>

Continued on next page

ECP Processing and Implementation, Continued

Question	Answer
Does the on line Report Center give me the same information of any paper documents I may be receiving from Chase Paymentech?	Yes, all information that is currently provided on the ECP returns documents can be found on the ECP Returns Received Report (PDE-0018 or PDE-0022). If you do not have this report in your “reporting packet”, please contact you Account Executive or Merchant Services.
Can I charge my consumer’s a service fee for any checks or transactions that are returned due to insufficient funds in the account?	Any service fee that a consumer is charged must be authorized by that consumer in order for the transaction to be processed electronically according to the NACHA and ACH rules. The merchant is required to provide the appropriate verbal or written notice to the consumer prior to the transaction and must send the service charge transaction separate from the sale transaction.

ECP Authorization Methods

Question	Answer
When do I use the CCD (Corporate Credit and Debit) SEC code?	<p>Any transaction that is intended to either debit or credit another business entity must be coded CCD regardless of how the transaction is authorized.</p> <p><i>This application can be either a credit or debit where funds are transferred between corporate entities.</i></p> <p>CCD Authorizations:</p> <ol style="list-style-type: none">1. Can support stand alone funds transfer, or a limited amount of payment related data with the funds transfer.2. Merchant must have what is considered a legal binding contract with the corporation which authorizes the merchant to debit their ACH account prior to any transaction being submitted3. Contract can be verbal or written <p>Merchants are not obligated to provide to an RDFI a proof of authorization if requested for CCD transactions.</p>

Glossary

ACH (Automated Clearing House)	The process by which member financial institutions perform the clearing of electronic debits and credits
ACH Transaction	An electronic debit or credit to or from a merchant's bank account as authorized by the Merchant Agreement; or an electronic debit or credit to a customer's bank account as authorized by an agreement between the merchant and the customer. A debit transaction represents a sale of goods or services to the customer.
Auxiliary On-Us field	A 6-10 character field located to the left of the routing number on the MICR line of a business-size check; presence of this field makes the check ineligible for conversion
Canadian Payments Association (CPA)	The Canadian organization that establishes and controls the rules and regulations under which financial institutions may process Direct Electronic Funds Transfers www.cdnpay.ca
CPA's Rule H1 for Pre-Authorized Debits	A continuing but revocable written authority given by the customer to the merchant that authorizes the merchant to issue preauthorized debits against the customer's account at the customer's bank and specifies whether such preauthorized debits are made for personal/household or business purposes
Deposit	The aggregate of sale and refund transactions submitted to Chase Paymentech for processing
Deposit Matching	The process of matching transaction information (account number, RDFI number, consumer name, account type) submitted by a merchant to Chase Paymentech to Chase Paymentech's NOC database to check if information must be corrected to post properly to the customer's account
DFI (Depository Financial Institution)	An acronym used to describe a depository financial institution
Dishonor	The process of rejecting untimely return of U.S. ECP transactions
ECP (Electronic Check Processing)	An electronic payment process designed to accommodate the requirements of various consumer and corporate payment applications in the U.S. and Canada
Facsimile Draft	A document created by Chase Paymentech upon the request of a merchant; a document created for a U.S. ECP transaction when the receiving bank is not a member of the Automated Clearing House
Insufficient Funds	When the available and/or cash reserve balance of a customer's account is not sufficient to cover the debit entry

Continued on next page

MICR (Magnetic Ink Character Recognition)	The machine recognition of characters printed with ink containing particles of magnetic material
NACHA	The National Automated Clearing House Association formed in 1974 to assist in developing standards and formats for ACH associations www.nacha.org
Notification Of Change (NOC)	A non-dollar entry sent to Chase Paymentech by the bank. It is created in response to the bank receiving either a prenotification or live dollar entry that contains incorrect information. The NOC contains both the original information and the correct information.
ODFI (Originating Depository Financial Institution)	The financial institution or its agent that originates an ECP transaction. Also referred to as the Originating Bank.
Prenotification	Also referred to as Prenote. A non-dollar transaction sent through the ACH network by the Originator to a Receiver for the purpose of verifying the accuracy of account data. The prenote contains the same information as the subsequent live dollar entry with the exception of dollar amount and transaction code.
RCK	A Returned Check entry class. If a paper check submitted to ACH is returned for NSF/Uncollected Balances, a merchant can use the ACH system (RCK) to redeposit it one time.
RDFI (Receiving Depository Financial Institution)	The financial institution that receives an ECP transaction. Also referred to as the Receiving bank.
Redeposit	The process of representing a transaction returned for insufficient or uncollected funds according to the timeframe parameter established in the merchant file.
Reject	A transaction in the initial deposit file transmission that does not pass Chase Paymentech's front-end edit checks.
Return	A transaction that is "charged back" for a variety of reasons by the customer's bank
Regulation E	The Electronic Funds Transfer Act that states that Preauthorized Electronic Fund transfers (ACH) from a consumer's account must be authorized by a writing signed or similarly authenticated by the consumer, and a copy of the authorization shall be provided to the consumer by the party that obtains the authorization from the consumer. www.federalreserve.gov

Continued on next page

Telemarketing	A plan, program or campaign which is conducted to induce the purchase of goods or services by use of one or more telephones and which involves more than one interstate telephone call. Regulated by the Federal Trade Commission. www.ftc.gov
WSUPP	Written Statement Under Penalty of Perjury. This is the document consumers are required to complete at the bank when disputing a payment as unauthorized. This document initiates a request for debit authorization from the consumer's bank to the merchant.
Validation	The process by which Chase Paymentech determines if the ECP transaction being presented can be processed through the Federal Reserve System or the Canadian Payments Association.
Verification	The process of electronically matching ECP transaction information against a negative file account database for the purpose of identifying accounts with unfavorable histories or that have been closed for cause by the financial institution.
Written Authorization	The authorization provided to the merchant by a consumer to electronically debit his/her account; the agreement between the merchant and the consumer that details the terms of the authorization and provisions for the revocation of the authorization by the consumer.