COMDATA
CORPORATE PAYMENTS

COMDATA MASTERCARD™ MULTI-CARD USER GUIDE

Disclaimer

Table of Contents

Revision Table

Date	Version	Author	Notes
08/22/2017	Ver 1.3	Steven Harris	Initial document distributed
06/11/2019	Ver 1.4	Steven Harris	Changed "MasterCard" to "Mastercard"
08/26/2021	Ver 1.5	Steven Harris	Updated several components and changed the document title to Mastercard Multi-Card User Guide

Overview

Comdata offers the ability to add a Purchasing and Travel & Entertainment (T&E) program to your business all under one roof with the Comdata Mastercard™ Multi-Card. With this program, you have the choice of using the card solely for Purchasing, T&E, fuel, or all of the above. By adding all these services to one card, you can manage your transactions, invoices, and data from one location.

Comdata can help you set up usage limits, such as the total spendable amount, location, and times (off hours blocking) when the card can be used. In addition, using a Comdata Mastercard Multi-Card means you can automatically reconcile transactions, reduce fraud, gain in-depth insight into your business spending, and even earn monthly rebates on every dollar spent.

Some other benefits include:

- **Unparalleled Global Acceptance.** The Mastercard Multi-Card is backed by Mastercard, providing you security and universal acceptance at nearly 40 million merchants around the world.

- **Earn Money Back on Spending.** Every dollar spent using your Comdata Mastercard Multi-Card earns monthly rebates for your business.

- **Alerts and Notifications.** As part of using a Multi-Card, Comdata offers Alerts and Notifications (A&N), an enhanced fraud detection and management program that helps you and your cardholders quickly and efficiently capture and reduce exposure to credit card fraud.

- **Control and Easy Reconciliation.** Comdata will work with you to set up card controls that limit employees not only from making purchases at certain times and locations, but also from purchasing certain products and amounts of products. By making purchases with a Comdata Mastercard Multi-Card, you can automatically reconcile transactions, reduce fraud, and gain better insight into your business spending.

- **Mastercard Easy Savings.** An automatic rebate program that enables participating merchants to provide rebates eligible to Mastercard small business cardholders registered in the program.

- **Cash Wallet.** An optional feature that allows you to load one-time funds to a cardholder's balance. Cash Wallet is especially useful with travel and purchasing programs to pay per diems or reimburse expenses for cardholders.

- **Cardholder Identification Data.** Cardholders can securely call Comdata to inquire about their cards by using their date of birth or Social Security Number to verify their identity.

- **Virtual Card for Travel.** Simplify the booking process by using electronic virtual card numbers to pay for travel related expenses, such as rental cars, airline tickets, and hotel rooms.

Mastercard Multi-Card Best Practices

Although it is a good business practice in any credit card program to mitigate as much fraud as possible, understand that no matter how well designed your program is, fraud may still occur. However, you can take steps to make your Comdata Mastercard Multi-Card program as fraud resistant as possible. See below for a list of best practices that will aid you in your fight against fraud.

1. **Take advantage of Alerts and Notifications (A&N).**
   Protecting your Mastercard cardholders from fraud and identity theft is a top priority at Comdata. That's why we offer the Comdata A&N program to help you improve security around your Comdata cards and minimize risk. With Comdata A&N, your cardholders receive text messages when Comdata's internal risk analysis system identifies a suspicious transaction. Then, your cardholder can reply to the message confirming if the transaction was fraud. If fraudulent, the card goes into a locked-down state and each additional transaction is declined. However, the cardholder will receive a text message with each declined transaction allowing them to override the declined authorization. If they override, they can swipe their card again and continue the transaction, only if the transaction is for the same amount and from the same merchant. If the cardholder receives a declined transaction they don't recognize, there's no need to respond as the transaction was not authorized.

   Extensive documentation on A&N is available in Comdata's ICD Resource Center.

2. **Design policies and procedures that are detailed, updated regularly, and reflect the roles and responsibilities of your program.**
   Firm policies and procedures are the foundation of a fraud-resistant Multi-Card program. Make sure these policies and procedures are detailed and spell out the accountabilities and responsibilities of cardholders and those monitoring card usage. If the full details of the program (monitoring, specified usage, etc.) are not clearly defined, fraud is more likely to occur.

3. **Appoint a Program Administrator with responsibility and authority over your program.**
   A Program Administrator can ensure cardholders are trained, monitor card usage, and assure that all aspects of the program are kept up to date and reflect all available technology and management controls. Program Administrators are also responsible for distributing cards, training (and retraining) cardholders and transaction reconcilers, and monitoring for unintentional personal use or obvious misuse. Furthermore, Program Administrators are responsible for approving officials who provide daily oversight for the program, assuring contract terms are fulfilled by both the organization and the card providers, and regularly reviewing provider services for Mastercard Multi-Cards.

4. **Implement a detailed written policy requiring the signature of the cardholder and their supervisor to reinforce responsibility and improve accountability.**
   The cardholder's supervisor is accountable for how the card is used.

Therefore, having the supervisor sign a written policy for card use by the cardholder reminds them that they are accountable for and must monitor each cardholder purchase. Each level of monitoring instituted in your card program is another method of minimizing misuse and abuse of your cards.

5. **Designate and communicate roles and responsibilities for transaction reconcilers and approving officials.**
   A prevalent error that occurs in many credit card programs is companies allowing cardholders to have subordinates responsible for reconciling and approving their own transactions. Reconcilers (a person who gathers supporting documentation and posts transactions to a financial system) and approvers (a person responsible for approving cardholder transactions) should not be under the cardholder's supervision.

   These roles must be held by individual people who can make judgements on appropriate card use without the cardholder's direction. Document specific responsibilities for each person involved in the card use and monitor processes so that all transactions receive an appropriate level of scrutiny, and ensure approval and responsibility are properly segregated.

6. **Establish card limits to reduce excessive or inappropriate use.**
   Some companies usually start off with low transaction limits but eventually realize they can reduce purchasing costs and increase incentive revenues by increasing their limits to the highest level possible. Unfortunately, this causes companies to raise limits to unnecessarily high levels. A good rule to follow is to provide card limits that slightly exceed the highest actual purchase in the preceding year by a cardholder. Define limits by the employee or employee class use, not by establishing blanket limits for all cards. Blanket limits provide cardholders considerably more purchasing power than they will need or use, which increases the risk of abuse and misuse.

7. **Conduct mandatory face-to-face training to new cardholders and face-to-face or online refresher training every two years for existing cardholders.**
   Require face-to-face training for new cardholders before issuing them a card and annual or biannual training for all existing cardholders. In-person training ensures emphasis is applied during the initial training and allows new cardholders to ask questions. Most cardholders will use their cards appropriately if they receive proper instruction from the beginning. Reserve computer or web-based training for only subsequent trainings.

8. **Require original receipts for *every* purchase.**
   Every photocopy accepted in support of a credit card program is an increased risk of fraud or abuse. In today's world of technology, obtaining and tracking receipts is difficult, but should still be of utmost importance. If a receipt is absent, require the cardholder to provide every document available to support the transaction.

For web purchases, require cardholders to provide a screen shot of the order confirmation screen and email (if received). Any receiving documentation or packing slips included with delivered purchases should also be included. Do not approve or reconcile a purchase without detailed supporting documentation that delineates the entire amount charged, as well as the specific business purpose of the purchase.

9. **Require electronic transfer of cumulative data from the card-services provider for data mining and analysis based on known risk factors.**
   The creation of comprehensive software to analyze databases for transaction anomalies has increased the need of access to electronic data and improved monitoring of all types of transactions.

   Using software to identify anomalies such as split transactions (multiple transactions designed to circumvent card limits), over-limit purchases, unusual transaction patterns, use of non-standard vendors for standard purchases, and even-dollar transactions at or just below threshold levels will allow more efficient and effective monitoring, prevention, and detection of potential misuse. Defining these anomalies is key to electronic data analysis of card activity. Assuring that the card service provider has the ability to produce Level 1, 2, and 3 transaction information is critical to this analysis process. This information breaks each transaction down by MCC (Merchant Category Code), type of service, vendor identification, and vendor corporate status to assure operational, financial, and tax related information is available to the organization for analysis and use.

10. **Provide a hotline process to report suspected abuse.**
    In most fraud incidents, at least one person knew or suspected the fraud, but didn't know how to report their suspicion. The lack of a defined process to report suspected fraud can be a contributing factor. Provide a confidential process for individuals to report suspected fraud and card abuse, and publicize the process through training and ongoing communication from the Program Administrator.

11. **Establish meaningful and enforced policies governing consequences for misuse.**
    Consequences for misuse must be real, known, and enforced. Treat all card misuse as a violation, and consider the proven use of a card for personal purchases as theft. Prosecute the individual and publicize the prosecution. Not punishing or publicizing the criminal act opens the door for more fraud. Enforcing and promoting consequences can significantly reduce the likelihood of fraud.

12. **Establish recurring audits to evaluate compliance with program policies and requirements.**
    Although routine monitoring processes are best handled by each operating unit's management, regular surprise audits of card usage, combined with data mining and analysis of usage anomalies and transaction information, provide in-depth oversight that can significantly prevent fraud. You can uncover fraud during a routine audit of the unit's card documentation that disclosed irregularities in the explanations for nonstandard transactions and documentation. Without the audit, the fraud may have continued indefinitely. If your program generates sufficient revenue in incentives, this audit activity can be part of your staff, funded by the incentive funds.

Dispute Fraudulent Transactions

In an effort to streamline Mastercard disputes, Comdata has developed a new Online Dispute Smart Form within iConnectData (ICD).

The Online Dispute Smart Form is dynamic in the sense that it generates a unique form with required information based on your selected reason for dispute. These specific forms can help you and Comdata understand the necessary information needed to file your dispute. You can also download a PDF of the dispute after it is submitted for your records.

This document is intended to walk you through filing a dispute through ICD using each of the unique forms.

Note: If you are the company administrator, you may submit dispute forms through the secure ICD website on the cardholder's behalf without obtaining a signature. Doing so confirms that you have a relationship with the cardholder and that the transaction is being disputed by the authorized user. Submitting the dispute via a secure site satisfies the Mastercard signature requirements.

Please note it is important that you notify us about any transaction disputes within **60 days** of the suspicious charge.

The following verbiage regarding this rule is located on each form: "We certify that this information was obtained via a secure website, and is being disputed by the authorized user."

Filing a Dispute

If a cardholder suspects fraudulent activity on their card, instruct them to follow these steps:

1. Call the Comdata Contact Center at 1-800-282-7496, which is open 24/7/365.

2. Let the Comdata agent know they suspect fraudulent charges on their card.

   a) The Comdata agent will block the card and ask the cardholder to contact their Program Administrator (you), who can order the new card.

   Note: Once Comdata is notified of the suspected fraud, then the customer is no longer liable for new fraudulent charges. If you are registered with the Alerts and Notifications program, then the Agent will offer to place the cardholder's card in a "hobble home" status, so they are not without access to a card if they are travelling.

3. The Comdata Agent will then ask the cardholder to contact you to file a dispute and order a new card.

   a) Be aware when a new card is issued so you can update your expense management system with the new card number associated with the employee.

(continued on next page)

b) Filing a dispute online typically takes a few minutes and saves a cardholder from having to fill out any documentation and fax it to Comdata. This also ensures customers have a Dispute ID that verifies that the fraudulent dispute was filed.

c) Filing a dispute also inserts an additional control around the validity of the dispute and ensures it is valid, as invalid disputes can quickly become your responsibility.

Once the dispute is processed in ICD, Comdata will initiate the chargeback process with the merchant involved in the dispute. At this point, you can do the following:

- Enroll the cardholder in Alerts and Notifications.

- Identify repeat-offenders whom might be using the card inappropriately.

Using the Online Dispute Smart Form

The following steps demonstrate how to file a dispute using the Online Dispute Smart Form in ICD.

1. On the ICD home page, select **Manage > Transactions > Real Time Transaction History**.

2. On the transaction history page, enter the required information to run a report. Note that only Posted transactions can be disputed. Click **Submit** when finished.

3. Select the checkbox next to the transaction(s) you want to dispute. Then, click **Initiate Dispute**.

   Note: You cannot dispute the same transaction more than once. If your dispute reason is "I did not authorize or participate in this/these transaction(s)" you can dispute multiple transactions for only one card.

4. Select **I did not authorize or participate in this/these transaction(s)** and then click **Dispute**.

5. The Online Dispute form opens with your contact information populated at the top of the page. Complete each field as necessary. Required fields are denoted by a red asterisk.

This specific dispute form provides three options:

- **My card was lost/stolen at the time of the disputed transaction.** Select this option to fill out additional information as to the circumstances surrounding the fraudulent card use, (date card went missing, start date of unauthorized transactions, if police were notified, etc.). This information helps Comdata better understand the situation, so appropriate action can be taken.

- **My card was in my possession at the time of the disputed transactions.** Select this option if the card was in your possession at that time of the unauthorized transaction. This option can also be used if the card number was used fraudulently while the card was in your possession.

- **The card was misused by the employee assigned to the card.** Select this option if an employee or authorized user caused the fraudulent transaction(s). Then, specify if the employee or authorized user was terminated and the date of termination.

6. After you enter all required information, click **Submit** at the bottom of the page.

Reason for Dispute: I did not authorize or participate in this/these transaction(s)

Please select one of the below available options:

Option #1 ☐ My card was lost/stolen at the time of the disputed transaction(s)

Option #2 ☐ My card was in my possession at the time of the dispute transaction(s)

Option #3 ☐ The card was misused by the employee assigned to this card.

We certify that this information was obtained via a secure website, and is being disputed by the authorized user.

Any documentation required to support your claim must be received within 10 days:

Comdata, Inc.
5301 Maryland Way   Email Legible Copy to:
Brentwood, TN 37027   or   support@comdata.com
Attn: Research Dept.

[Submit] [Cancel]

7. A PDF with the dispute details will display; save the PDF for your records. A confirmation email will also be sent to your ICD email address.

Transaction Online Dispute Processing Form

COMDATA
Payment Innovation

Dispute ID: 88888888X
Date: 05/16/2020

Account Code: AB123
Contact Name: JANE DOE
Company: BUSINESS INC 549
Address: Any Street
City/ST/Zip: Quincy / MA / 0000

Customer ID: BOT12
E-mail: JANE.DOE@COMPANY.COM
Phone Number: 617-000-0000
Fax Number: 617-000-0000

Card Number
XXXXXXXXXXXX8888

Customer ID
BOT12

Disputed Transaction Listing

Transaction Date	Posted Date	Transaction Number CB#	Posted Amount	Recon Amount	Approval Code	MCC	POS	ARD Merchant Name
05/07/2020 12:13:25	05/08/2020 06:38:57	327859 CB0508327859	800.00	800.00	918343	8641	81	55429508127894198299532 MISCELLANEOUS FOOD

Note: Take note of the following in the generated PDF:

- If multiple disputes are filed on one card, a total recon and posted amount will display at the bottom of the PDF.

- The Dispute ID displays in the top right corner of the PDF. Take note of this and use the Dispute ID to identify and track the dispute.

- If there are multiple pages on the PDF, the Dispute ID will display on each page.

Search for a Filed Dispute

ICD's Real-time Transaction History allows you to locate and review submitted transaction disputes.

1. On the Transaction History page, enter the required information to run a report. To search for disputed transactions, follow these tips:

   a) To search for a specific dispute, select **Dispute ID** from the **Search By** radio buttons, then enter the corresponding dispute ID in the **Search Value** field.

   b) To search for multiple dispute transactions across a date range, select **Disputed** from **Transaction Status**. Then, select your date range.

      Note: Disputed transactions will also display on the transaction history report if **All** or **Posted** is selected from **Transaction Status**.

Transaction History

Account Code:	AB123 - TEST
Customer ID:	JANEAC - BOT12 — Hold the Ctrl Key for multiple selections.
Search By:	○ Employee/Vehicle Number ○ Card Number ○ Card Token ○ Last Name ○ First Name ○ Driver Id ● Dispute Id
Search Value:	12345678X
Transaction Status:	Authorized / Posted / Declined / Credit / Disputed — Hold the Ctrl Key for multiple selections.
Sort By:	● Transaction Date ○ Posted Date *Choose sort order.
Date Type:	● Transaction Date ○ Posted Date
Start Date:	01 / 25 / 2020
End Date:	06 / 25 / 2020

* Date ranges are limited to 180 days.
* Earliest start date is 04/25/2019.

[Submit] [Reset] [Download]

2. Click **Submit** to display the transaction history report in your browser. Click **Download** to save the transaction history report in Excel format.

Download View

	E	F	G	H	I	J	K	Y	AA	AI
1	Transaction Date	Transaction Time	Posted Date	Posted Time	Transaction Status	Card Number	Cardholder Name	Accept Location	Posted Amount	Dispute ID
2	02/20/2020	04:58:46	02/20/2020	05:25:19	Disputed	556735XXXXXX2548	AC342 AIRCRAFT JET	Shell Oil 57445630007 Bismarck ND	350.00	38486069I
3	03/09/2020	01:40:28	03/11/2020	08:43:41	Disputed	556735XXXXXX6016	225LP VEHICLE	Miscellaneous Food Sto Los Amigos MEX	9.74	69871729I
4	03/09/2020	01:40:28	03/11/2020	08:43:41	Disputed	556735XXXXXX6016	225LP VEHICLE	Miscellaneous Food Sto Los Amigos MEX	9.74	17881634I
5	03/09/2020	01:40:28	03/11/2020	08:43:41	Disputed	556735XXXXXX6016	225LP VEHICLE	Miscellaneous Food Sto Los Amigos MEX	9.74	56742522X
6	03/09/2020	01:52:00	03/11/2020	08:43:41	Disputed	556735XXXXXX6016	225LP VEHICLE	Miscellaneous Food Sto Los Amigos MEX	9.74	81256609I
7	03/09/2020	02:00:00	03/11/2020	08:43:41	Disputed	556766XXXXXX9359	TEST SUPER	Stationery Office Supp Chicago IL	198.75	67295354I
8	03/09/2020	02:33:53	03/11/2020	08:43:41	Disputed	556735XXXXXX3013	3013 VEHICLE	Pauls Amoco St Charles IL	100.00	311039PE
9	03/09/2020	05:47:38	03/11/2020	08:43:41	Disputed	556735XXXXXX6024	BENJI OLSON	TELIs Through Use Mf M New York NY	8.64	2654289X
10	03/09/2020	05:49:24	03/11/2020	08:43:41	Disputed	556735XXXXXX6016	225LP VEHICLE	Miscellaneous Food Sto Los Amigos MEX	9.74	69871729I
11	03/09/2020	05:49:24	03/11/2020	08:43:41	Disputed	556735XXXXXX6016	225LP VEHICLE	Miscellaneous Food Sto Los Amigos MEX	9.74	17881634I

3. A dispute ID link displays in the left column for transactions disputed electronically. Also, the **Transaction Status** column will display **Disputed**. Click the disputed ID link to open a copy of the confirmation PDF.

4. If you have not already, save this document for your records.

Dispute Confirmation Email

You will receive a confirmation email for each dispute you submit. See below for an example. Confirmation emails contain a link to the PDF form and details on your dispute, such as the number of days to process and reconciliation information.

A MC Online Dispute has been entered for:

Card Token: 222T22A2G2
Card Number: XXXXXXXXXXXX8888

Please use the link provided to view the dispute detail.

https://qaws.iconnectdata.com/forms/PDFServlet?type=disputeMC&seqId=89913355FE&userType=2

    - If all required information is received timely, you should expect a provisional credit on your account, within 30 days.

    - There is a CB reference number assigned to each transaction in your dispute. (see dispute form in link above) You may use that CB ref# number, and/or "CB" plus the last 10 digits of the card number, for "dispute credit" reconciliation.

    - If additional documentation is required to support your dispute, please write the MC Dispute Id number listed on the form, (also listed in the subject line of this email), on your documentation for proper matching.

Important: Incomplete information may cause a delay in processing your dispute.

Please note: This message does not have a valid reply address. Please do not attempt to reply.

To check the status of your dispute, please contact: support@comdata.com

---

Fraud Dispute Frequently Asked Questions

1. **How long do I have to enter the dispute for a fraudulent transaction?**
   You have 60 days from the bill/invoice date of the transaction to enter a fraud dispute.

2. **Why can't Comdata enter my cardholder's dispute?**
   Mastercard regulations require cardholders to certify they did not participate in a fraud transaction. To ease the process for cardholders, you can act on their behalf and certify that the cardholder did not participate via the Online Dispute Smart Form in ICD.

3. **What information can I use to track my dispute?**
   Once you enter a dispute in ICD, you will receive a Dispute ID which can be used to identify the dispute until it is resolved.

4. **What communication will I receive after the dispute is filed?**
   If the merchant represents the transaction, you may receive a progressive letter completed by Comdata's dispute department that reaffirms the dispute. If you want to continue with the dispute, the letter must be signed and returned to Comdata within *eight days* indicating your preference to continue the dispute.

5. **What if I suspect a cardholder misuses their card and are claiming fraud to cover their tracks?**
   Comdata's process allows you to always stay aware of transactions under dispute. This allows full insight into any potential cardholder misuse in order to reduce potential liability and loss.

6. **Should I replace the card which has potential fraudulent activity?**
   If a cardholder states they have fraudulent charges, block the card and replace it to prevent any further transaction activity. Your account manager can also assist with the replacement process.

7. **What steps should I take after I replace a card?**
   Replacing a card has several downstream dependencies. The new card must be entered into the cardholder's expense management tool. In addition, if a card is replaced it must be enrolled into the Alerts & Notifications system to maximize Comdata's fraud prevention tools. You, the Program Administrator, are best positioned to make these changes and control your program.

8. **Can I call the Contact Center to help me with fraudulent disputes?**
   The Contact Center has the ability to block the card in order to prevent any further fraud charges. However, the dispute entry and card replacement should be done via ICD.

Cardholder Identification Data (CID)

When cardholders call Comdata for assistance with their card, they are required to verify their identity. To do so, they can provide one of the following to the Comdata agent:

- Last 4-digits of Social Security Number

- Date of Birth (month, date, year)

Please note that Comdata agents can help cardholders with only the following information and issues:

- Transaction History

- Card Declines

- General program questions

- Available spend amount

- Reporting a lost or stolen card

- Cash Wallet support

For any information or issues outside of those listed above, the cardholder will need to contact you, their Program Administrator. As a Program Administrator, you can send this information to Comdata so we can have it on file for reference. Ask your Comdata representative for a PS14 file, which will allow you to send us your cardholder's information.

Using iConnectData (ICD)

ICD is Comdata's secure, self-service web portal for performing account management tasks, such as ordering cards, checking credit availability, running reports, and much more. The features in ICD are designed to provide self-service account management, which can reduce the need to contact a Customer Service agent.

See below for a list of pertinent tasks on using your account. For more information on the many features available in ICD, see the ICD Resource Center.

- Logging into ICD
- Checking Available Credit
- Performing Codeword Maintenance
- Copying and Deleting Users
- Ordering Virtual Cards for Travel
- Running Reports
- Accessing and Using the Resource Center

Logging into ICD

Once you receive the Welcome Email, you can sign in to ICD at https://w6.iconnectdata.com/Login/init and access all of your available features.

1. Enter your assigned user ID, then select **Continue**.

> Step 1: Please enter your User ID
>
> 👤 | User ID
>
> Continue

2. Enter your assigned password, then select **Continue**.

   Note: It is required that you change your password as soon as you log in, following these guidelines:

   - Must be at least 8 characters

   - Must include 1 number

   - Must include 1 uppercase and 1 lowercase letter

> Step 2: Enter password for KJOHNSON
>
> 🔒 | Password
>
> Continue

3. Select an ImageKey and enter an associated ImageKey caption. The image and caption you specify will display for verification each time you log in. Select **Continue** when finished.

   Note: If the ImageKey and ImageKey caption displayed are incorrect on your next login, call Comdata Customer Service immediately.

> Step 3: Please select an image.
>
> Please select an ImageKey. This image will be associated with your account and will be shown each time you log into iConnectData, confirming that you are at the legitimate website.
>
> Please enter an ImageKey caption that you will recognize next time you log in. This caption will be shown with your ImageKey each time you log into iConnectData, confirming you have reached the legitimate web site. If the caption shown when you login does not match what you entered here, do not enter your password. Please call our customer service, as you may be at a fraudulent site.
>
> 🖼 | ImageKey Caption
>
> Continue
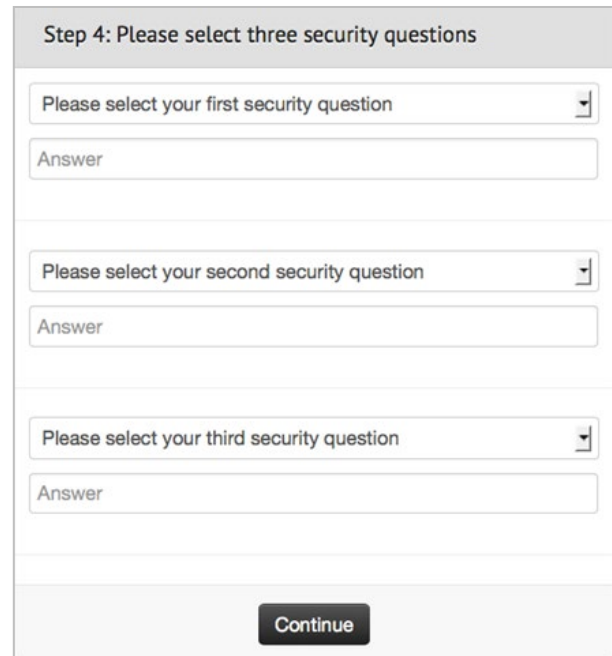
4. Select and answer three security questions. You will be presented with one of these questions any time you log in to ICD from a location not recognized by the system (i.e., logging in from a different computer or browser than your standard). Select **Continue** when finished.

You will be automatically logged in to the ICD homepage.

Note: You can reset your Security Questions and Image Key by selecting the user ID drop-down in the far-right corner of the ICD home page.

Step 4: Please select three security questions

Please select your first security question

Answer

Please select your second security question

Answer

Please select your third security question
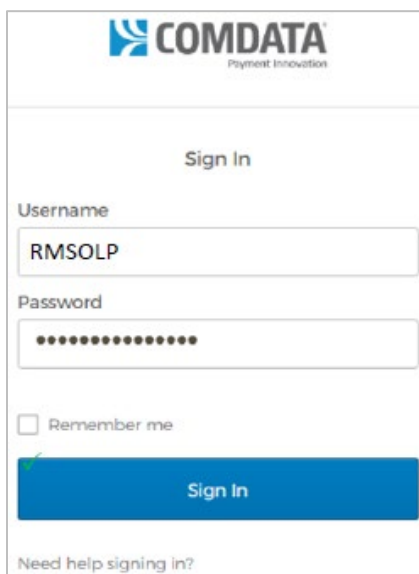
Answer

Continue

5. The message pictured below displays. You should be directed to a new page within 15 seconds. If not, click the "here" link to proceed.

COMDATA / iConnectData
Payment Innovation

You are being redirected to our enhanced security login portal. If your browser does not automatically redirect you, please click here
Please bookmark the new login portal for future ease of navigation.
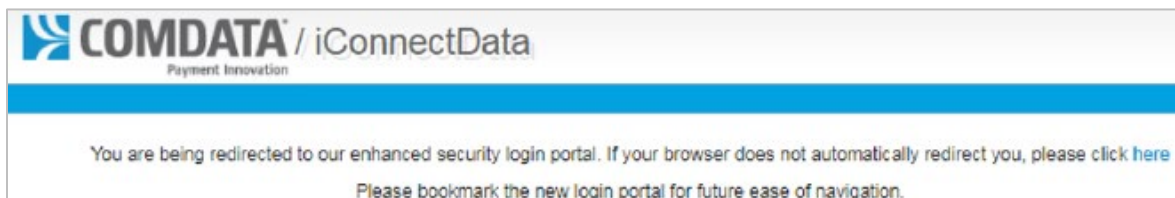
6. Enter your ICD username and password. Then, click **Sign In**.

COMDATA
Payment Innovation

Sign In

Username

RMSOLP

Password

●●●●●●●●●●●●●●●●
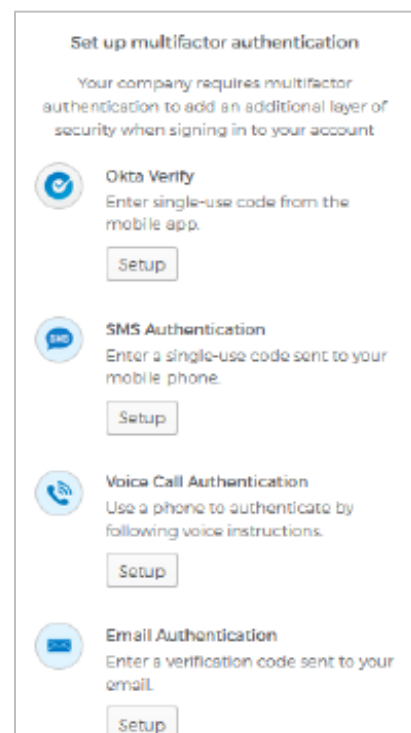
☐ Remember me

Sign In

Need help signing in?

7. In the Set up multifactor authentication dialog box, select your preferred method and click **Setup**. Then, proceed to one of the sections of this document mentioned below for steps on completing your selected authentication method:

- Okta Verify pg. 23
- SMS Authentication pg. 25
- Voice Call Authentication pg. 27
- Email Authentication pg. 28

Okta Verify

1. If you selected **Okta Verify**, a Setup Okta Verify window displays. Select your phone type (android or iPhone).

2. You are prompted to download the Okta Verify app. Download the app from your mobile device's app store, then return to this window and click **Next**. Then, click **Open**.
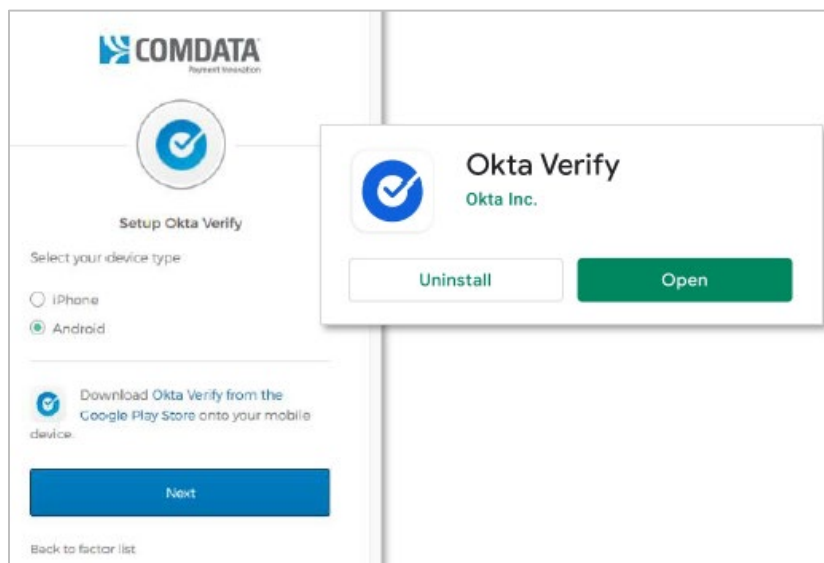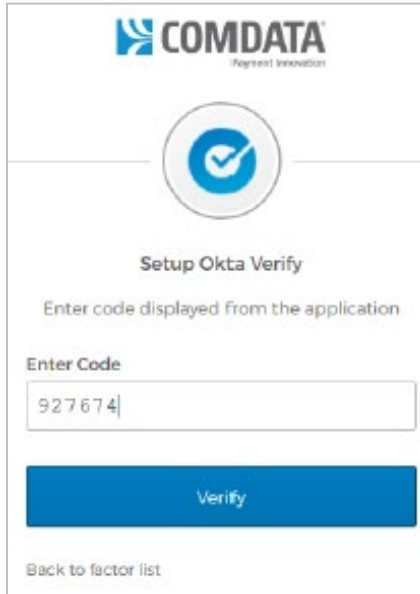
3. Launch the Okta Verify application on your mobile device and tap **Add Account**.

4. Select **Other**, which is used for two-factor authentication code for third party services.

5. Tap **Scan a QR Code**.

6. Use your mobile device to scan the QR code in that now displays in the Setup Okta Verify window. Your mobile device should display a 6-digit authentication code. Click **Next**.
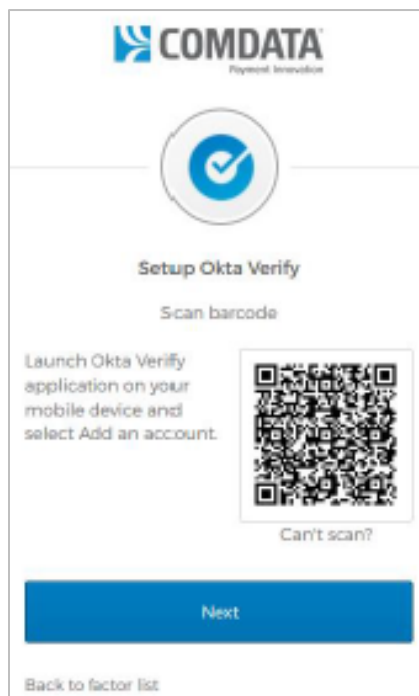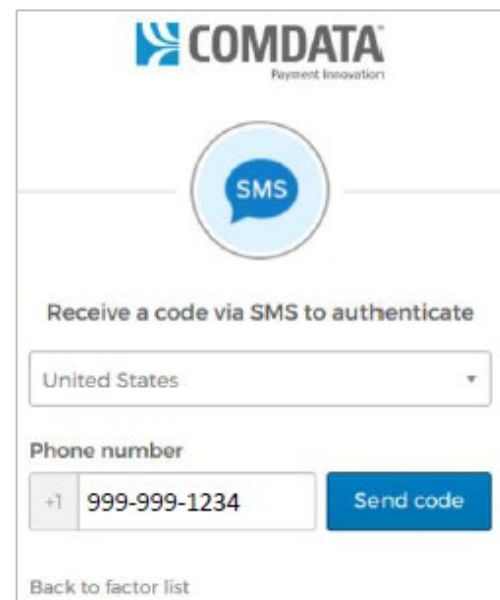
7. Enter the 6-digit code and click **Verify**. Going forward, when asked for the 6-digit code, open the Okta Verify app to retrieve the code.

SMS Authentication

1. If you selected SMS Authentication, an SMS dialog box displays. Select your country of residence and enter the mobile phone number that will receive authentication messages. Then, click **Send Code**.
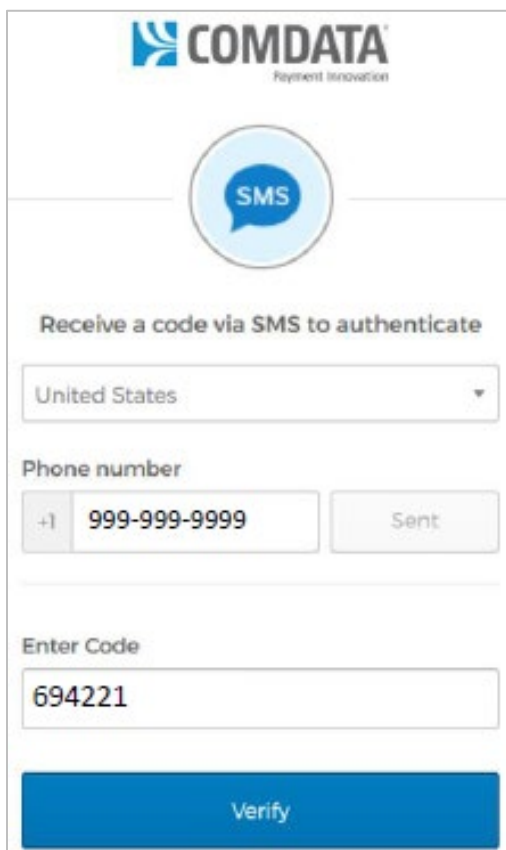
2. The mobile phone number you entered will receive the following message. A different code displays each time.
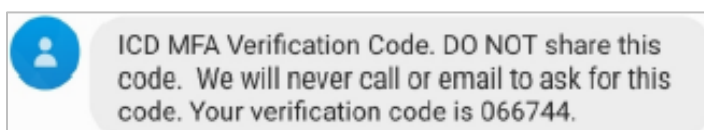
3. Enter the 6-digit code and click **Verify**. If you do not enter the code within 30 seconds, a **Re-send code** button displays in case the first code was not received.

    Note: *Do not* share this code with anyone. Comdata will never call or email you asking for the code.

4. Once verification completes, the system logs you into ICD.

Voice Authentication

1. If you selected Voice Authentication, a Voice dialog window displays. Select your country of residence and enter your mobile phone number. Then, click **Call**.

   Note: An extension can be entered for a land line.
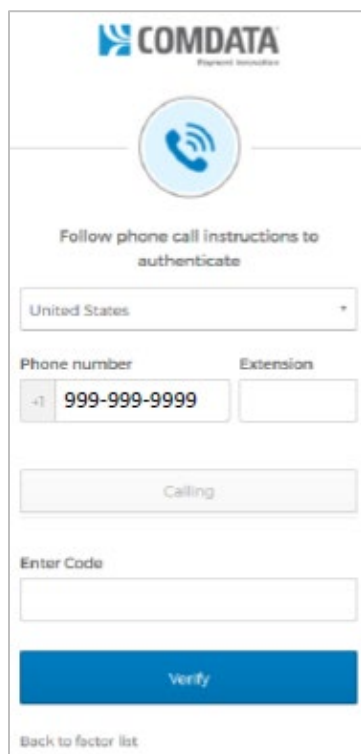
2. You'll receive a phone call at the number entered with the following message: "*Hello. Thank you for using our phone verification service. Your code is ######.*" ######=a randomized 6-digits code. The phone message will repeat the code again and then end with, "Goodbye." Take note of the code.

3. Return to the Voice dialog window and enter the code. Then, click **Verify**.

   Note: *Do not* share this code with anyone. Comdata will never call or email you asking for the code.

   (see image on next page)

4. Once verification completes, the system logs you into ICD.
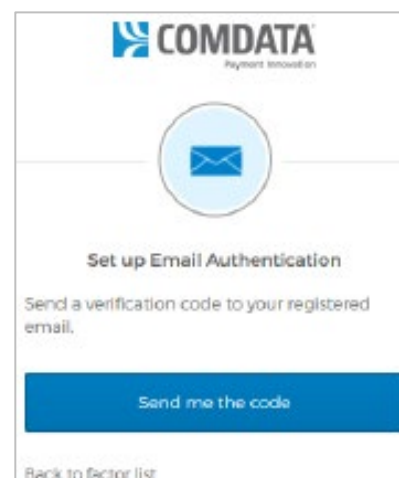
Email Authentication

1. If you selected Email Authentication, a Set up Email Authentication window opens. Click **Send me the code**.

2. You will receive an email with the authentication code at the email address you registered with your ICD account.

   Note: *Do not* share this code with anyone. Comdata will never call or email you asking for the code.

3. Return to the Set up Email Authentication window and enter the 6-digit code from the email. Then, click **Verify**.
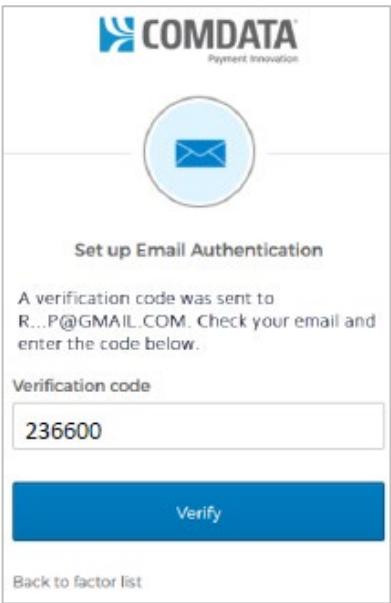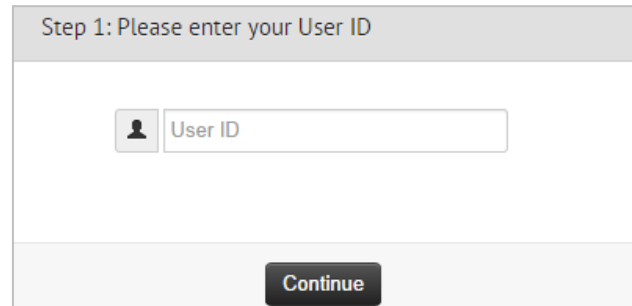
4. Once verification completes, the system logs you into ICD.
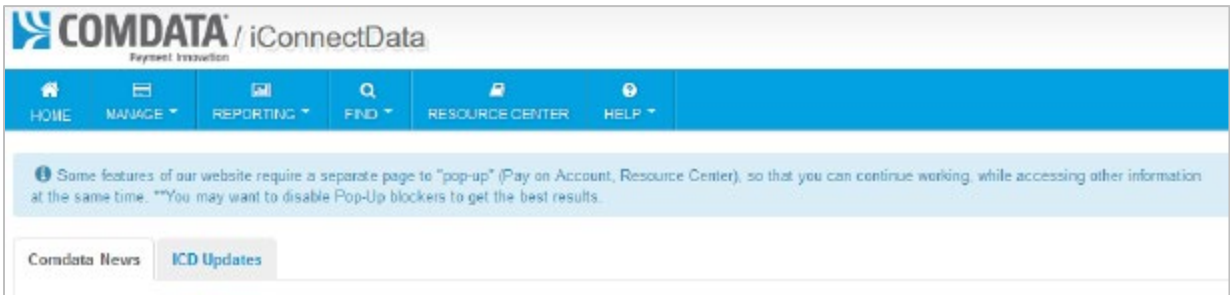
Logging in After Multi-Factor Authentication Setup

The next time you log in after setting up multi-factor authentication, the system uses your selected authentication method.

1. Access the ICD Login page and enter your used ID. Then, click **Continue**.
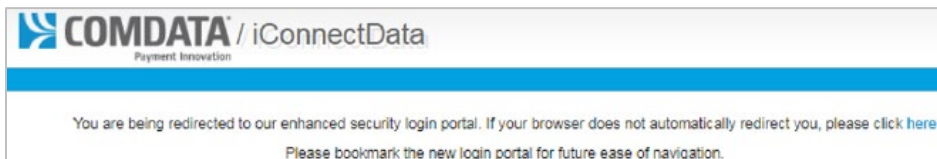
2. A redirect page displays the message below.

   Note: Please note the following:

   - If the system does not redirect you after 15 seconds, use the "click here" button to access the new log in page.

   - Once you are registered for ICD MFA, change your ICD bookmark to the following URL: https://w6.iconnectdata.com/icd-auth. If you log into ICD with your current device (IP address), you will not be required to enter a new 6-digit code for 12+ hours.

   - If you attempt to log into ICD with a difference device (for example, mobile), you must follow the same MFA process when you registered.

3. Enter your ICD username and password. Then, click **Sign In**.

   Note: Select **Remember me** to prompt the system to retain your username for future logins.

4. The dialog box for your selected authentication method displays. Follow the steps mentioned in section on your authentication method (see).

5. Once you receive the single-use code, enter the code in the dialog box. Then, click **Verify Code**.

   Note: A checkbox displays with the message, "Do not challenge me on this device for the next 15 minutes". Select this checkbox to prevent the system from using the authentication log in method on your current device for the next 15 minutes.

6. Once verification completes, the system logs you into ICD.
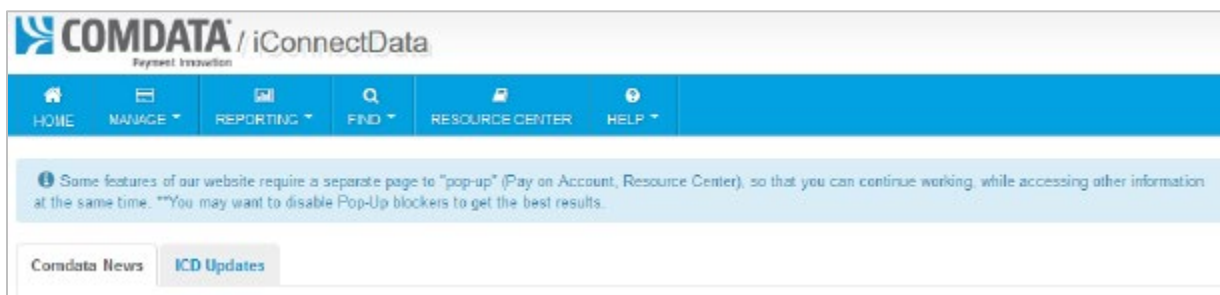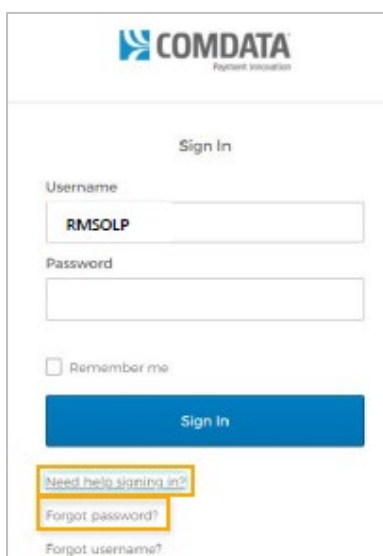
Retrieving your Login Information

If you forget your ICD user ID or password, you can easily retrieve them by selecting one of the following options on the ICD Login page: **Forgot User ID?** or **Forgot Password?**.

Retrieving your Password
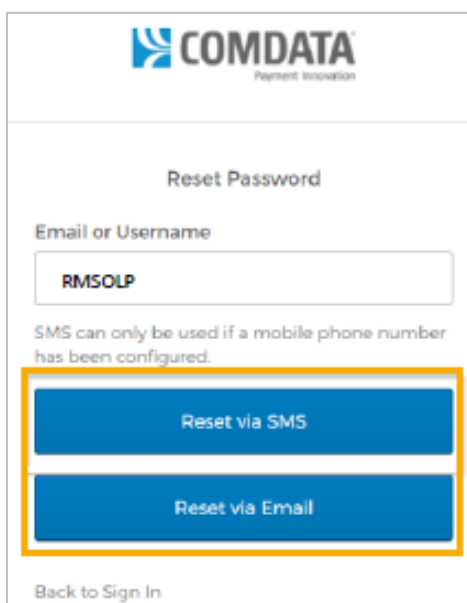
Follow these steps if you forget your ICD password:

1. Click **Forgot Password?** from the ICD Login page.

2. The Reset Password dialog box opens. Click either **Reset via SMS** or **Reset via Email**. **Reset SMS** can be used only if a mobile phone number is associated with your ICD user profile.
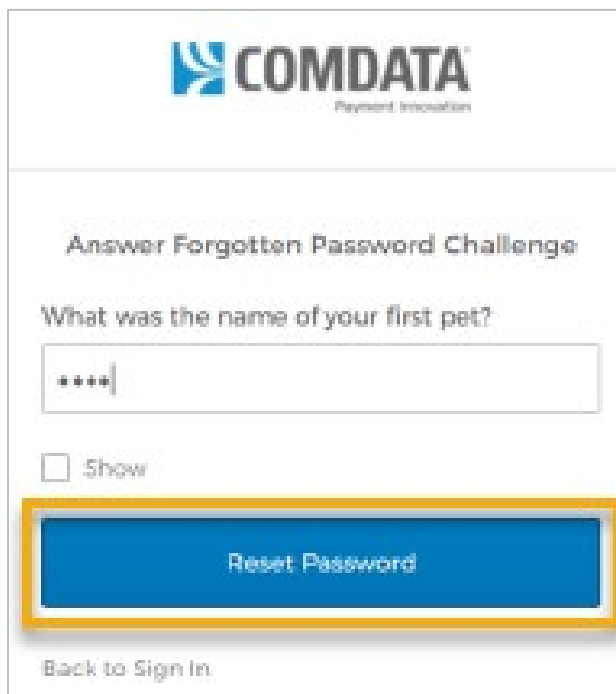
3. If you clicked **Reset via SMS**, a verification code is sent to your selected option. Enter the code in the **Enter Code** field, and click **Verify**.

   Note: If you clicked **Reset via Email**, skip to step 8 on page 35.

4. If verified, you must answer one of your security questions. Enter your answer, and click **Reset Password**.

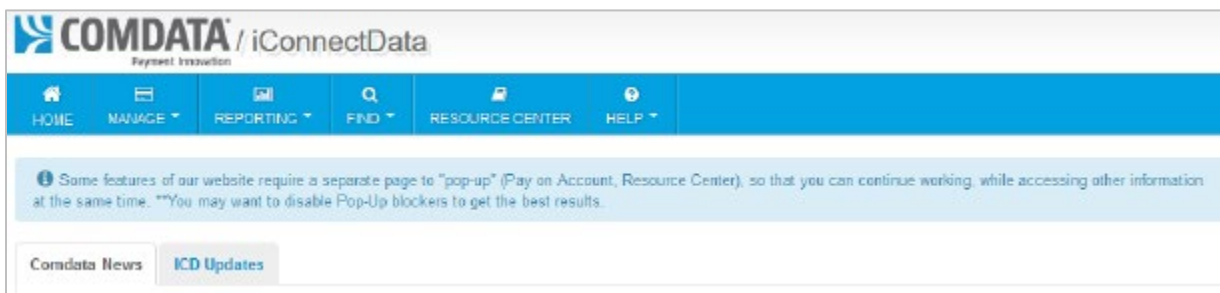5. In the Reset your Password dialogue box, enter your new password in the **New Password** and **Repeat Password** field. Then, click **Reset Password**.

6. A new verification code is sent via SMS. Enter the code and click **Verify**.

7. You are now logged into iConnectData.
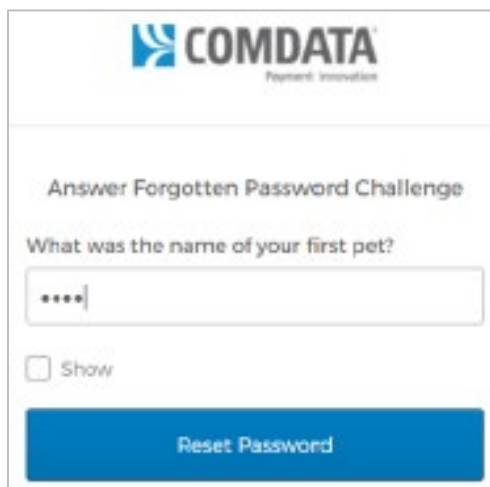

8. If you used the **Reset by Email** option, a confirmation window displays. The email associated to your ICD user profile should receive a message from Comdata.
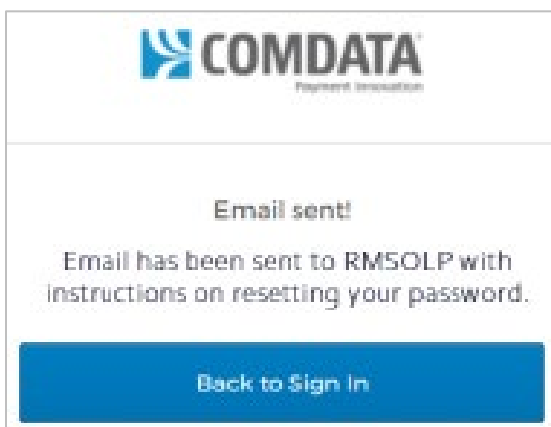
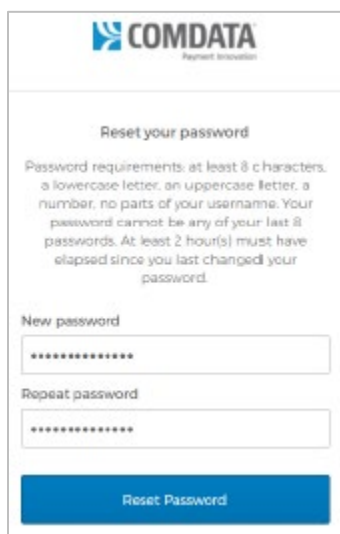9. Open the message and click **Reset Password**.

10. Answer your security question. Then, click **Reset Password**.
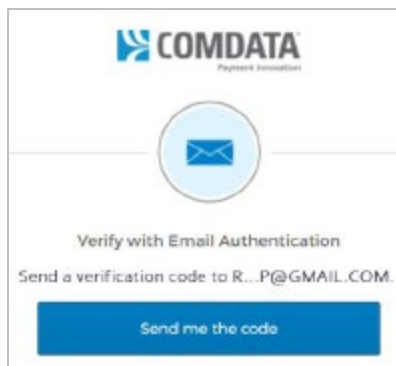

11. In the Reset your Password dialogue box, enter your new password in the **New Password** and **Repeat Password** field. Then, click **Reset Password**.

12. A Verify with Email Authentication window opens. Click **Send me the code**.

13. Check your email for a message from Comdata which contains a verification code. Enter the code in the **Verification code** field in the Email Authentication window. Then, click **Verify**.

14. You are now logged into iConnectData.
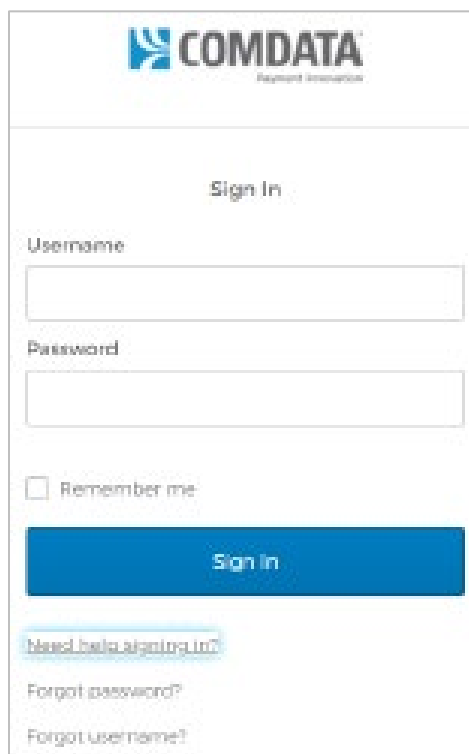
Retrieving your User ID

Follow these steps if you forget your ICD user ID:
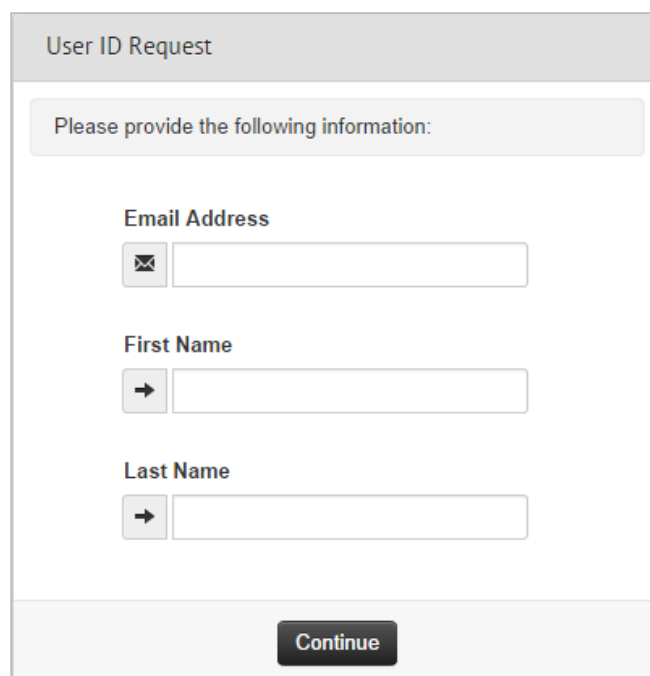
1. On the Sign In dialog box, click **Need help signing in? > Forgot Username**.

2. Enter your email address, first and last name in the fields provided. Then, click **Continue**.

   You should immediately receive an email message titled **Forgot User ID?**, which contains your user ID.

Checking Available Credit

The Available Credit Information function enables you to see your total credit limit for your account(s) and the remaining credit available for use. The available credit reflects only amounts that have been posted to your account.

Note: This information is for review only; do not remit payment based on the account balance shown. You will receive an invoice for payments due.

1. On the ICD home page, click the **Credit Summary** tab.
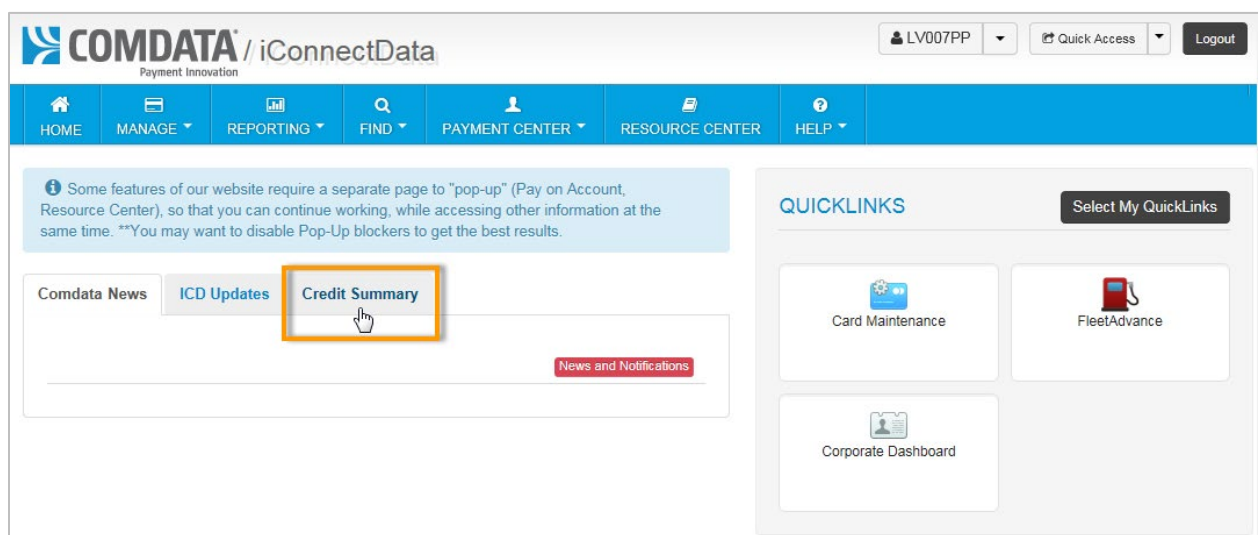
2. Enter your account code and click **Retrieve balances**. The page will refresh to display your current credit information. Hover your cursor over each question mark for more information on each field displayed.

Performing Codeword Maintenance

A codeword is a second tier of security beyond your user name and password. Codewords are assigned to only company representatives with authority to make changes in your account beyond normal maintenance, such as ordering cards.

At the time of account setup, provide your Comdata Implementations Specialist with a list of users and their access levels for codeword assignment. Ongoing codeword additions and changes should be made by an authorized representative, such as your program administrator, using the Codeword Maintenance feature. Note that you can apply multiple codewords to a single customer ID.

1. On the ICD home page, in the upper right corner above QuickLinks, select **User ID drop-down > CodeWord Maintenance**.
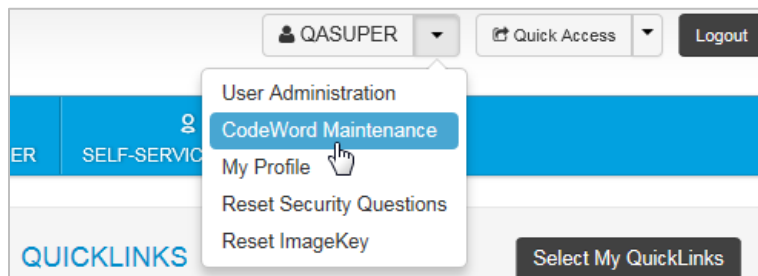
2. The Codeword Maintenance page displays; select a different account code or customer ID, if necessary.

3. Enter the codeword for the user whose access you want to edit, then click **Display**.

4. The page refreshes and displays information matching the codeword.

A. A list of viewing options you can perform for the selected codeword. Options include:

- **Display:** Enter a new codeword and click Display to view its information.

- **User List:** Displays a list of all codewords assigned to the selected customer ID. The list displays each user's full name, codeword status, and office/home telephone number.

- **User Access:** Displays all accesses and limits granted to the codeword; edit accesses and limits as necessary.

- **Previous and Next:** Use these buttons to view the previous or next codeword assigned the customer ID.

B. The next section displays details on the user assigned to the codeword. Click **Add** if the codeword information has not been applied, **Delete** to remove the codeword assignment to the customer ID, **Copy** to copy the details to another customer ID, or **Update** to save any changes you made on this page.

C. The bottom section allows you to set limits on the codeword for the assigned customer ID. Options include:

- **Codeword Maintenance:** Select **Yes** to grant the ability to add or delete other users and to grant access/set limits for other users.

- **Express Cash per XTN Limit:** Enter the individual Express Cash transaction limit for the selected user.

- **Express Cash Daily Load Limit:** Enter the Express Cash daily load limit for the selected user.

- **Express Cash Amt Load Today:** Displays the Express Cash load amount for the current day.

- **XTN Limit:** Enter the Express Check transaction limit.

- **Daily Limit:** Enter the Express Check daily limit.

- **Daily Used:** Displays the amount used of the daily limit.

- **Last Used:** Displays the date Express Check was last used.

- **Issuance, Maintenance, Inquiry, Invoice, and Administration:** For each item, select **Yes** to grant the selected user the ability to perform these actions. Select **No** to remove the ability.

- **Special Instructions:** Enter any notes or instructions on the codeword.

    Note: If the incorrect codeword is applied to a customer ID, users assigned to the codeword will be restricted from several features in ICD, such as editing cards in Card Maintenance and using the Credit Summary dashboard. Use Codeword Maintenance to determine which customer ID has the wrong codeword applied. You will need to contact Comdata to retrieve and apply the correct codeword.

Copying and Deleting User Profiles

As an ICD Administrator, you have the ability to copy and delete user profiles from your account structure. Copying allows you to create a new user profile based on the details from an existing profile.

1. On the ICD home page, in the upper right corner above QuickLinks, select **User ID drop-down > User Administration**.
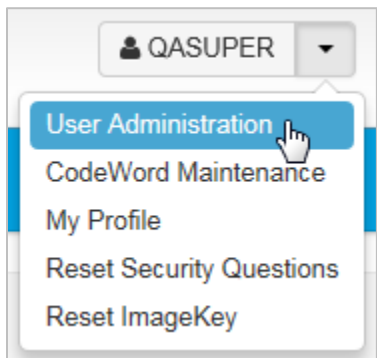
2. The Copy User page opens.

To copy a user, complete the following:

- Enter a user ID in the **From** (existing user) and **To** (new user) fields.

- Enter the new user's first and last name, and email address.

- Select the **Call In** check box to allow the new user to call Comdata to make account changes. The check box will prompt you to enter a codeword for the new user.

- Click **Create User** when finished. You should receive a success message upon completion.

*Note the following when using the **Call-In** check box:*

- Always select the **Call-In** check box when copying a user to avoid codeword issues.

- If the **From** user does not have a codeword setup or all their codewords are incorrect on their customer IDs, the following warning message will display if **Call-In** is selected: "User (to user) has been created, however (to user) will not get call-in access as (from user) does not have call-in access."

- If the **From** user only has codeword access on one or some of their customer IDs, and **Call-In** is selected, the **To** user will have codeword access to only the same customer IDs as the From user. A standard success message will display as this is not considered partial success.

3. When finished, click **Create User**.

A message displays confirming the user profile was created. You will receive an error message if the user ID already exists or if you did not complete the required fields.

4. To delete a user profile, select **Delete User** from the left-hand menu.
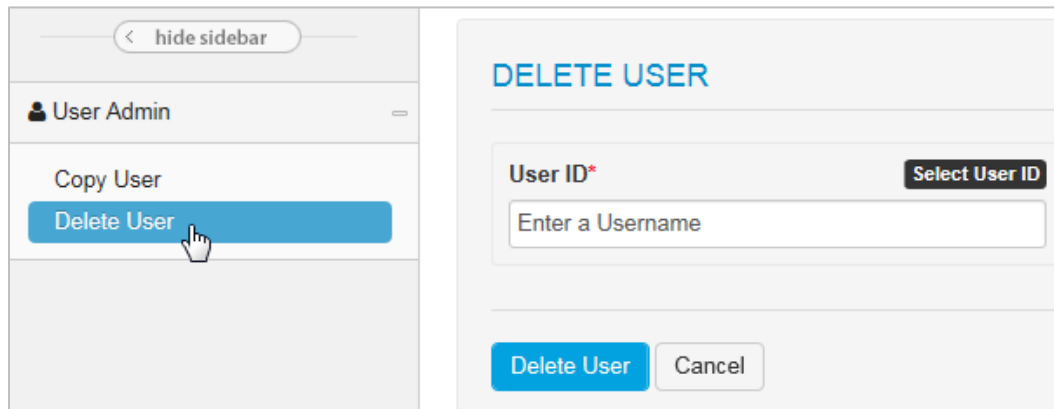
5. Enter the user ID, then click **Delete User**.
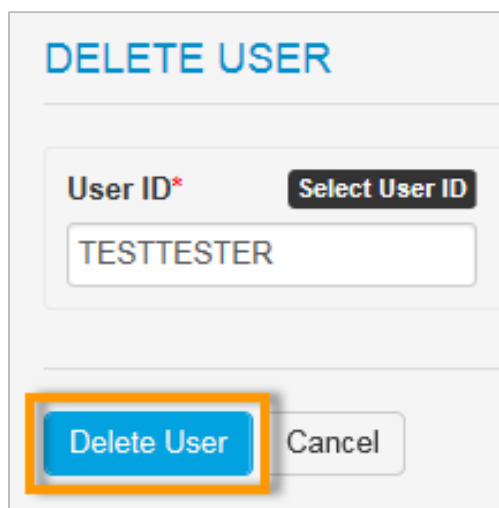
6. You will be prompted to confirm your action. Click **OK** in the pop-up window.
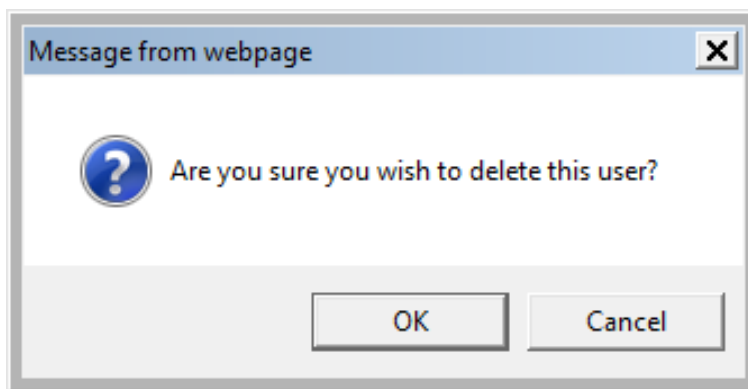
7. A message displays confirming deletion of the user profile.

Ordering Virtual Cards for Travel

As a Comdata Mastercard Multi-Card user, you have the ability to issue virtual cards — one-time use, electronic, card numbers — for travel related expenses. With Virtual Card for Travel (VCT), you can quickly pay for purchases in the travel industry, such as hotel rooms, airline tickets, and car rentals. Use this feature to simplify and quicken your booking and travel process.

For access to VCT, contact your Comdata representative.

Key benefits include:

- Streamline reconciliation when booking travel as only one card number is tied to one transaction

- Send exact payment amounts instead of estimates or guesses

- Resend fax authorizations if one is lost or not processed

- Increase security and reduce exposure to fraud or misuse

- Improve compliance by applying controls on the card that are in line with your company's travel policy

- Allow the travel agency to request additional card numbers

- Fully integrate with leading business travel resources and networks, such as: global distribution systems, Sabre, Amadeus, Travelport, TMC networks, American Express Global Business Travel, BDC, CWT, HRG

This section will instruct you how to:

- Set up a Virtual Card for Travel Order
- Issue a Virtual Card for Travel

Set up a Virtual Card for Travel Order

To issue a virtual card for travel expenses, you will need access to ICD. Once you receive access and are logged in, you will need to modify the information fields necessary to issue a virtual card. This enables you to customize the virtual cards to adhere to your company's requirements, such as limits by merchant groups, invoice details, and discretionary data.

1. To access the Virtual Card Setup page from the ICD menu bar, select **Manage > Virtual Card Setup Option**.
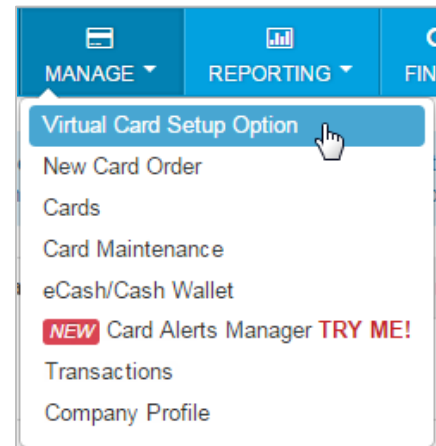
2. Select an account code and customer ID for issuing virtual cards. Then, click **Continue**.

   Note: If you have a large amount of customer IDs, you may be prompted to type in your account code and customer ID. Typing in the search field functions as a keyword search, so you can enter as few as three characters to pull matching results.

3. The Virtual Card Setup page opens, displaying three sections of information fields that you can make optional or required when issuing virtual cards: **Invoice Detail**, **Merchant Categories**, **Fleet/Maintenance Fields**.

   Complete the fields as necessary and select **Save All Fields** at the bottom of the page, or select **Reset** to clear all changes. *See the next page for field descriptions.*

   Note: If you make changes on this page after a virtual card has been issued, they will be applied to existing cards when they are retrieved for editing. For example, if you change the option **Invoice Due Date** to required, users will be required to add the invoice due date to any existing card opened for editing.

Invoice Detail Fields

These fields are specific to the vendor's invoice. Select a check box in the **Display** column to display the field on the Virtual Card Order page or select a check box in the **Required** checkbox to make it mandatory. You can also edit the field name (label) in the **Change Label to** column as needed. Note that you will receive an error message if you duplicate field names.

Note: If your account is set up for virtual card for travel (VCT), some field labels in the **Change Label to** column will default to a specific name. Each defaulted field is noted in the table below.

INVOICE DETAIL FIELDS	Display	Required	Change Label to:
First Name			First Name
Last Name			Last Name
Vendor Invoice Number	✔	☐	Vendor Invoice Number
Vendor Number	✔	☐	Vendor Number
Vendor Name	✔	☐	Vendor Name
Virtual Card Invoice Number	✔	☐	Virtual Card Invoice Number
Payment Number	✔	☐	Payment Number
Invoice Due Date	✔	☐	Invoice Due Date
Location Code	✔	☐	Location Code
Invoice Date	✔	☐	Invoice Date
Assign GL Codes	✔	☐	Assign GL Codes
GL Validation		☐	GL Validation
Invoice Comments	✔	☐	Invoice Comments
Payment Date	✔	☐	Payment Date

Field	Description
First Name	First name of payee. This field is required and cannot be hidden. Defaults to **Traveler First Name**.
Last Name	Last name of payee. This field is required and cannot be hidden. Defaults to **Traveler Last Name**.

Field	Description
Vendor Invoice Number	This field can be used for any discretionary data you want to make optional or required with a card. Defaults to **Confirmation Number**.
Vendor Number	The number assigned to the vendor in the accounting system for the selected customer ID. This field can be used for any discretionary data you want to make optional or required with a card.
Vendor Name	Used to enter the full name of the vendor being paid. Also can be used for discretionary data you want to make optional or required with a card. Defaults to **Hotel Name** for VCT orders.
Virtual Card Invoice Number	Invoice number for which the virtual card is issued.
Payment Number	Vendor-assigned number for the invoice being paid
Invoice Due Date	Date payment is due to the vendor. Defaults to **Check In Date** for VCT orders.
Location Code	5-digit alphanumeric code associated with the vendor's location
Invoice Date	Similar to Invoice Due Date, this field can be used for any discretionary data you want to make optional or required with a card.
Assign GL Codes	Includes a table for assigning up to four GL codes with each virtual card.
Invoice Comments	Select this option if you want the user issuing the virtual card to add comments related to the invoice. Defaults to **Comments** for VCT orders.
Payment Date	Similar to Invoice Due Date, this field can be used for any discretionary data you want to make optional or required with a card. Defaults to **Check Out Date** for VCT orders.

Merchant Categories

This section allows you to determine which MCC groups are available for the virtual card. Your selections here will display on the Virtual Card Order page. When the issuer of the virtual card accesses the Virtual Card Order page, they can apply or disallow your selected MCC groups as needed. Select **Open for any Mastercard Location** to make all MCC groups available for selection.

Merchant Categories

	Display
Open for any MasterCard Location	☑
Business Services Group	☑
Financial Group	☑
Fuel Group	☑
Legal, Insurance Group	☑
Maintenance Only Group	☑
Medical Group	☑
Miscellaneous Group	☑
T & E Group, Airlines	☑
T & E Group, Hotels / Motels	☑
T & E Group, Misc. Transportation	☑
T & E Group, Rental Car	☑
T & E Group, Restaurants	☑

Fleet/Maintenance Fields

If you plan to issue virtual cards to pay vendors for fleet related expenses, select the appropriate fields below. You can set each field as optional or required and edit the field name (label) in the **Change Label to** column as needed.

Fleet/Maintenance Fields

	Display	Required	Change Label to:
PO Number	☑	☑	PO Number
Vehicle Number	☑	☑	Vehicle Number
Repair Order Number	☑	☑	Repair Order Number
Warranty Report	☑	☑	Warranty Report
Warranty Period	☑	☑	Warranty Period
Misc. Costs	☑	☑	Misc. Costs
Total Labor Costs	☑	☑	Total Labor Costs
Total Parts Cost	☑	☑	Total Parts Cost
Total Tax Cost	☑	☑	Total Tax Cost

Description	Comments
PO Number	Purchase order number for the virtual card transaction
Vehicle Number	Vehicle ID of the vehicle receiving service
Repair Order Number	Vendor-assigned number if the virtual card is being issued for repairs
Warranty Report	Used to indicate whether the product or service being purchased includes a warranty. If so, the user will need to enter the warranty type in this field.
Warranty Period	Used to enter the duration the warranty is valid.
Misc. Cost	Used to specify miscellaneous costs for the virtual card; this option is generally used along with the Total Labor Costs, Total Tax Cost, and Total Parts Cost fields.
Total Labor Costs	Used to specify labor costs for the virtual card; this option is generally used along with the Total Parts Cost, Total Tax Cost, and Misc. Costs fields.
Total Parts Cost	Used to specify total parts cost for the virtual card; this option is generally used along with the Total Labor Costs, Total Tax Cost, and Misc. Costs fields.
Total Tax Cost	Used to specify a total tax cost for the virtual card; this option is generally used along with the Total Labor Costs, Total Parts Cost, and Misc. Costs fields.

Issue a Virtual Card for Travel
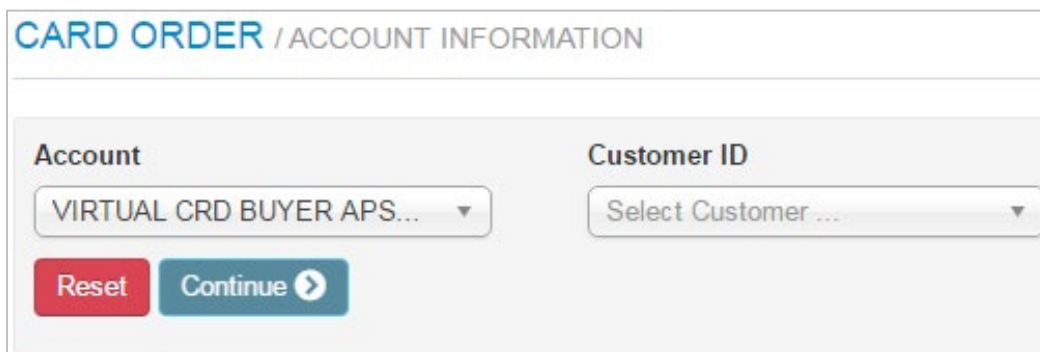
The one-off virtual card feature in iConnectData (ICD) allows users to order virtual cards for purchases in the travel industry, such as hotel rooms, airline tickets, and car rentals. Use this feature to simplify and quicken your booking and travel process.

Note: Virtual cards can be issued only on a one-by-one basis through ICD's Virtual Card Order.

1. On the ICD menu bar, select **Manage > New Card Order**.
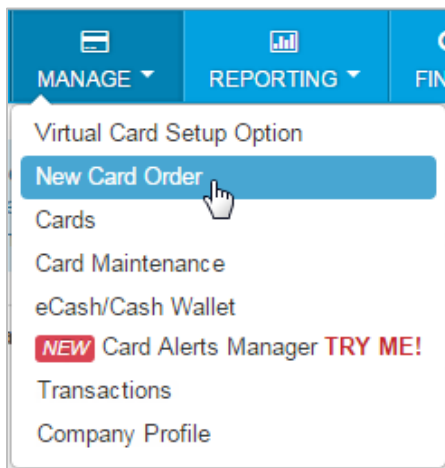
2. Select an account code and customer ID set up to use virtual cards for travel purchases.

3. The Virtual Card Order page opens. Complete each field as necessary; the fields displayed below are default for VCT orders. Your program administrator may change some field names depending on the order's purpose. For example, **Airline Name** might replace the **Hotel Name** field for an airline purchase.

(see image on next page)

Note the following fields:

- **Amount for this Card:** Displays the value from the **Net Amount** field, the total amount for the virtual card. The net amount must be greater than $0.00.

- **Expiration Date:** Select the date the virtual card will expire.

- **Number of Transactions:** Enter the number of transactions allowed on the card (must be greater than 1). For hotel transactions, must equal number of days stay.

- **Amount must be Exact:** Select if the virtual card will be authorized for a single transaction and you know the exact amount. Deselect if the virtual card will be authorized for more than one transaction and you do not know the exact amount, otherwise it will not exceed the amount assigned.

- **Send Email/Send Fax:** Send the remittance advice to the receiving merchant as either a fax or email. Both options can be selected at once, however, hotel transactions require a fax.

- **Comments:** Enter any comments the receiving merchant needs to see. For example, "A room with a view of the harbor".

- **Gross, Discount, Net Amount: Gross Amount** refers to the total amount on the card before any discounts are applied, **Discount Amount** refers to any negotiated discounts with the receiving merchant, and **Net Amount** refers to the total amount on the card after any negotiated discounts.

4. Scroll down and click one of the sliders to either open the virtual card for all Mastercard accepting locations or lock it down to specific Mastercard Category Groups (example: hotels, motels, restaurants, etc.). This feature is useful in preventing receiving merchants from using the virtual card for unintended purposes. When finished, click **Submit**.

Resend Fax or Email Remittances

If you need to change or resend a fax or email, you can do so from ICD's New Card Maintenance. This feature is useful if a vendor cannot find a fax and/or email.

1. Log in to ICD and select **Manage > Card Maintenance**.

2. Use the search field to locate a virtual card set up for VCT. You can search by any of the virtual card's attributes (card number, customer ID, account code, etc.). Click on the card in the search results to open its details.

3. The virtual card's details open. Click **Resend Remittance** to resend an email or **Resend Fax** to resend a fax remittance. The merchant that received the virtual card will receive the resent remittance advice.

   Note: Click **Edit** to change the email address or fax number. If you change one of these values, you must resend the remittance advice.

Example Email Remittance Advice

CREDIT CARD AUTHORIZATION FORM

AP BUYER COMPANY NAME PS20Q
123 AP BUYER ADDR Q SUITE PS20Q
APBUYERCITY, TN 37999
(615) 370-7000
QACOMDATAAPBUYER1@COMDATA.COM

Hotel Information

Hotel Info: Fairfield Inn New Bedford MA   **Confirmation #:** 997766

P: **Check-Out:** 08/30/2016
F:

Guest Name(s):

Check-In: 08/25/2016

Comments: A room with the view of the harbor
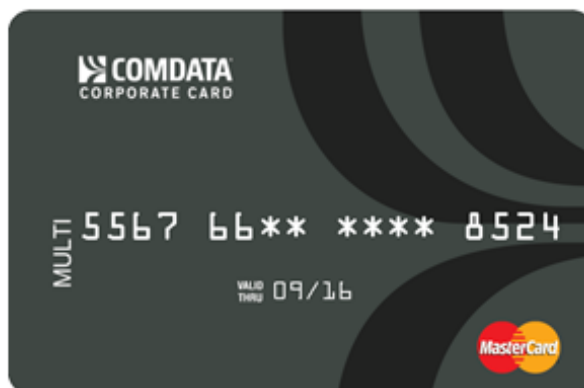
You are required to debit the card above according to the following restrictions, including all applicable taxes;

Room Cost: 1200.00

Payment Restrictions:

REGRESSION TEST GROUP 1

Example Fax Remittance Advice (required for hotel transactions)

Page 1

Fax

To:		From:	advisory, payment
Fax:	6153707211	Fax:	
Company:		Voice:	

Date: August 07, 2016

Subject: Virtual Card Travel Booking from Ap Buyer Company Name Ps20q

Comments:

Page 2

COMDATA
Payment Innovation

CREDIT CARD AUTHORIZATION FORM

AP BUYER COMPANY NAME PS20Q

123 AP BUYER ADDR Q SUITE PS20Q

APBUYERCITY, TN 37999

(615) 370-7000

QACOMDATAAPBUYER1@COMDATA.COM

Hotel Information

Hotel Info:	Fairfield Inn New Bedford	Confirmation #:	856777
		Check-Out:	08/23/2016
Ph:		Travel Agency	
Fax: (615) 370-7211			
Guest Name(s):	JIMI HENDRIX	Booking Agent:	
Check-In:	08/19/2016	Comments:	Get a room wiht the view of the harbor

COMDATA
CORPORATE CARD

MULTI 5567 6600 0000 0000

VALID THRU 09/16

JIMI HENDRIX

MasterCard

OT.04 32698 ICA7963 12/15   If found, send to P.O. Box 1849 Brentwood, TN 37924

506

Authorized Signature Not Valid Unless Signed
Do NOT write your PIN anywhere on this card.
Cardholder Services   855-823-8859
Servicios de Cuentahabiente 855-823-8859

COMDATA   Use of this card constitutes acceptance of the terms and conditions of the cardholder agreement as amended from time to time.
THIS CARD IS ISSUED BY REGIONS BANK PURSUANT TO LICENSE BY MASTERCARD INTERNATIONAL

MasterCard

You are required to debit the card above according to the following restrictions, including all applicable taxes;

Room Cost: 1200.00

Payment Restrictions:

REGRESSION TEST GROUP 1

Displaying Real-Time Transaction History

Real Time Transaction History allows you to view authorized, posted, and declined transactions on your account for all transactions. In addition, you can also view specific information in regards to a decline and get simple solutions to fix the cause of the decline in many cases.

1. Access the Real Time Transaction History page (**Manage > Transactions**).
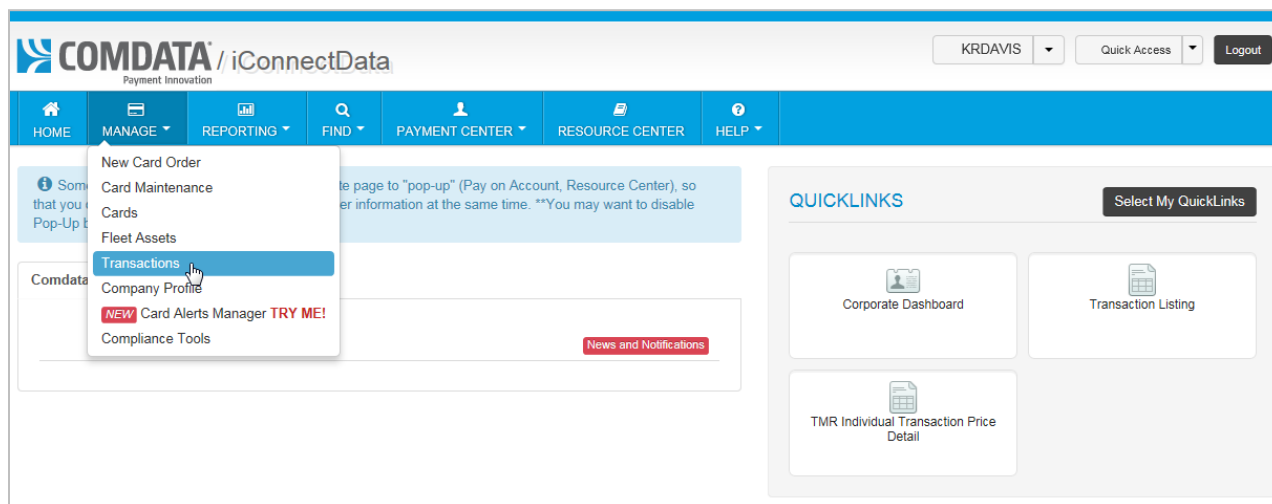
2. Select **Real Time Transaction History**.
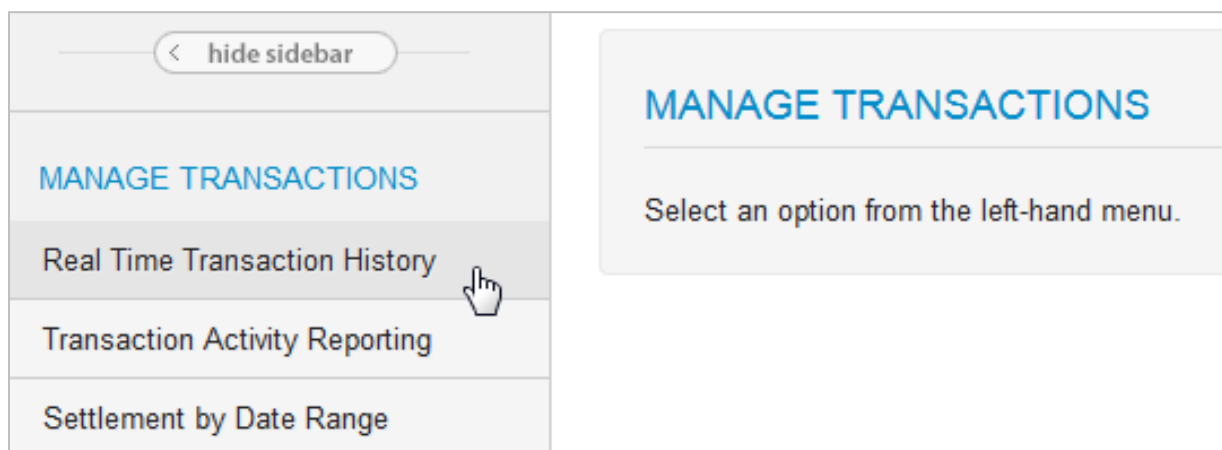
3. Complete each field on the Transaction History page, then click **Submit**.

   Note: Click **Download** to save an Excel spreadsheet of your search results.

   - **Account Code:** Enter your 5-digit Comdata-assigned account code.

   - **Customer ID:** Select one or more customer IDs, or use **Select All** to include every customer ID under the selected Account Code.

   - **Search By:** Narrow your search results by one of the provided values. For example, select **Card Number** to display only transactions that fall under a card of your choosing. Or select **Dispute ID** to display all transactions associated to a specific dispute ID.

   - **Search Value:** Enter the value related to the **Search By** value. For example, if you selected **Card Number**, enter the full 16-digit card number here.

   - **Transaction Status:** Used to display only transactions with a specific status.

   - Hold **Ctrl** on your keyboard

   - to make multiple selections. Options include: **Authorized**, **Posted**,

   - **Declined**, **Credit**, **Disputed**.

   - **Sort By:** Sort transactions in the report by their transaction date or posted date.

   - **Date Type:** Select **Transaction Date** to display all transactions or **Posted Date** to display only transactions that have posted.

   - **Start Date/End Date:** Select the date range of transactions (limited to 45 days within the previous 180 days).

4. The Transaction History report displays based on the values you entered in the query.

Note: Additional fields will display if you download an Excel spreadsheet of the Transaction History.

Field Name	Description/Comments
Dispute ID	If the transaction was disputed, the Dispute ID displays in the far-left column. Click the Dispute ID link to open the Dispute Resolution Form for the transaction.
Customer ID	5-digit customer ID or IDs you selected to display. The customer ID used for virtual cards should be unique; i.e., it should be for only virtual cards.
Transaction Date/Time	Date and time (central standard time, 24-hour military format; no AM or PM) the transaction took place. If the transaction has posted, these fields match the Posted Date/Time fields.
Authorized Amount	The amount in US dollars and cents authorized for the transaction. If the authorized amount is a credit, the value will appear preceded by a minus sign (for example, - $26.31).
Posted Date/Time	Date and time (central standard time, 24-hour military format; no AM or PM) the transaction posted. If the transaction has not posted, this field will be blank.
Posted Amount	The amount in US dollars and cents posted in the transaction. If the authorized amount has not yet posted or was declined, this field will display 0.00.
Merchant Name	Full name of the merchant company receiving the virtual card.
Transaction Status	Real-time status of the transaction, including: **Posted**, **Authorized**, **Declined**, **Credit**, and **Disputed**. Click one of these links to view additional transaction details.
Cardholder Name	The name associated with the card or another identifier such as "Virtual Card".
Card Number	16-digit card number used in the transaction. Click a link in the **Card Number** column to view the card balance information. Note that some card numbers are masked for security, depending on your account's setup.
Card Token	Full 16-digit number used in place of the card number for security purposes.
MCC	4-digit Merchant Category Code (MCC) that denotes the specific business type.
Original Transaction Amount	Original transaction amount if a credit was processed.
Currency Code	3-digit country code for the original currency used in the transaction.

Field Name	Description/Comments
Additional Fields Displayed in Excel Spreadsheet	
Account Code	5-digit Comdata-assigned account code.
Corporate Code	5-digit Comdata-assigned Corporate Code. This field displays "N/A" (not applicable) unless the account falls under a Corporate Account Code.
Card Expiration Date	4-digit card expiration date (MMYY format, example: 0817 = August 2017).
Decline Code	Reason code for a transaction decline.
Decline Message	Message describing the decline code.
Decline Corrective Action	Corrective action needed in response to the decline code and message.
Prompted ID	6-digit (or less) identification code that can authorize a transaction or show what is entered at the Point of Sale (similar to a PIN).
MCC Group	A grouping of merchants by types, such as fuel group, maintenance, legal, etc.
MCC Number	4-digit Merchant Category Code (MCC) denoting the specific business type used in the transaction.
MCC Description	Description of the MCC (Gas Services, Miscellaneous Food Stores, United Airlines, etc.).
Merchant Address	Full address of accepting merchant.
Merchant City	City of accepting merchant.
Merchant State	State of accepting merchant.
Merchant Zip	Full zip code of accepting merchant.
Accept Location	Merchant information that is in the vendor's Point-of-Sale device.
Pre-Authorization Amount	The amount in US dollars and cents authorized before the transaction. If the authorized amount is a credit, the value will appear preceded by a minus sign (for example, - $26.31).
Approval Code	Authorization number given for the transaction.
Reversal Flag	**Y** (Yes) or **N** (No). This shows whether the authorization for the transaction was released or not.
Transaction Fee Amount	Amount of any fees associated to the transaction.

5. On the Transaction History page, click a link under the **Transaction Status** column to view additional details.

- **Posted** detail includes authorized and posted information on the transaction. Use this information for reconciliation purposes and to view behind-the-scenes data related to the authorized and posted amount. The same page displays if **Disputed** is clicked.

- **Authorized** detail includes information around the authorization of a transaction. Use this information to view authorization data such as the method used and total authorized amount.

- **Declined** detail includes information around a rejected transaction. Use this information to understand why a transaction was declined and the corrective action needed to authorize it.

Decline Detail

Account Code:	MC180	Accept Location:	88888 Chicago IL
Customer ID:	MCREG	Merchant Category Code Group:	30001
Corporate Account Code:	N/A	Merchant Category Code Number:	5499
Cardholder Name:	TESTFILE	Merchant Category Code Description:	FOOD STORES
Cardholder Card Number:	556735XXXXXX8888	Authorization Method:	E
Card Expiration Date:	8888	POS Entry Mode:	001
Authorized Amount:	99999.00	POS Entry Mode Description:	KEYED TRANSACTION
Local Date (CST):	01/23/2017	Decline Code:	1100
Local Time (CST):	14:34:09	Decline Message Description:	ENHANCED RISK MONITORING DECLINE
Prompted ID:		Corrective Action:	
Employee Name:		Accept ID:	683103202800000
Reversal Flag:	N	Authorization Transaction Fee:	0.00

- **Credit** detail includes information on a posted amount credited back to the card, such as in the event of a returned item. Use this information for reconciliation and reporting purposes.

Posted Detail

Account Code:	MC180	Merchant Address:	1234 MAIN STREET
Customer ID:	MCREG	Merchant City:	VANCOUVER
Corporate Account Code:	N/A	Merchant State/Zip:	BC L5P 1B2
Cardholder Name:	SPARE DRIVER II	Merchant Category Code Group:	30005
Cardholder Card Number:	556735XXXXXX6032	Merchant Category Code Number:	3000
Card Expiration Date:	0000	Merchant Category Code Description:	UNITED AIRLINES
Original Currency Amount:	15.00	Posted Amount:	-11.54
US Currency Amount:	11.54	Posted Date:	04/27/2017
Transaction Date:	04/27/2017	Posted Time:	14:14:10
Merchant Name:	UNITED AIRLINES UNITED	Posted Control Number:	248622
Reversal Flag:	R	Posted Message Number:	0

Back

See below for a list of all possible fields on the Transaction Status screens.

Field Name	Description/Comments	Comments
Account Code	5-digit account code.	This is the primary account code assigned when the account is opened. It displays as a number and a name.
Accept ID	Terminal ID for vendor's POS device.	
Accept Location	Location code for the merchants as it appears in the vendor's POS device.	
Approval Code	Authorization number given for this transaction.	
Authorization Method	E - Electronic, O - Manual	Method by which the transaction was authorized.
Authorization Transaction Fee	Amount of any fees associated with the transaction.	

Field Name	Description/Comments	Comments
Authorized Amount	The amount in U.S. dollars and cents authorized for the transaction.	If the authorized amount is a credit, the value will appear preceded by a minus sign (for example, - $26.31).
Customer ID	5-digit customer ID or IDs you selected to display.	The customer ID used for virtual cards should be unique; i.e., it should be for virtual cards only.
Cardholder Name	The name associated with the card or another identifier such as "Virtual Card".	
Cardholder Card Number	16-digit card number used in the transaction. Note that some card numbers are masked for security, depending on your account's setup.	
Card Expiration Date	4-digit card expiration date (MMYY format, for example: 0817 - August 2017).	
Corporate Account Code	5-digit Comdata-assigned Corporate Account Code.	This field displays "N/A" (not applicable) unless the account falls under a Corporate Account Code.
Corrective Action	Message describing action to take in response to a decline.	Decline Detail only
Decline Code	Reason transaction is declined.	Decline Detail only
Decline Message Description	Message describing the reason for decline code.	Decline Detail only
Employee Name	Employee first name followed by middle initial (optional) and last name.	
Local Date (CST)	Date of transaction	
Local Time (CST)	Time of transaction	Central standard time, 24-hour military format; no AM or PM (00:00:00).
Merchant Address	Full accepting merchant's address.	
Merchant Category Code Description	A description of the business entity related to the MCC.	
Merchant Category Code Group	A grouping of merchants by types such as fuel group, maintenance group, T & E, business services, financial group, legal, medical group, etc.	
Merchant Category Code Number	The 4-digit Merchant Category Code (MCC) denoting the specific business type.	
Merchant City	Full accepting merchant's city's name.	
Merchant Name	Full accepting merchant's name.	

Field Name	Description/Comments	Comments
Merchant State/Zip	Merchant's state and zip code.	Two-letter abbreviation for state and full zip code.
Original Currency Amount	The transaction amount as shown in the original currency that it was processed in.	Example: $5.00 CAD
POS Entry Mode	A code identifying how the transaction was processed.	See codes and descriptions below.
POS Entry Mode Description	Description of method used to enter transaction at POS.	**00** = Entry mode unknown **01** = Manual entry **02** = Auto-entry via magnetic stripe-track data is not required **03** = Auto-entry via bar code reader **81** = Entry via electronic commerce, including chip **90** = Auto-entry via magnetic stripe-the full track data has been read from the data encoded on the card and transmitted within the authorization **999 =** Comdata Manual Authorization
Posted Amount	The amount in US dollars and cents posted in the transaction.	If the authorized amount has not yet posted, this field displays $0.00
Posted Control Number	The control number Comdata applies to the posted transaction used for tracking purposes.	
Posted Date	Date transaction posted	
Posted Message Number	A numeric code that represents the posted amount.	Internal message code from posted transaction: **00000** = success Any other value is an error.
Posted Time	Time the transaction posted	Central standard time, 24-hour military format; no AM or PM (00:00:00).
Prompted ID	Up to six digits identification that can authorize a transaction or show what is entered at the POS (similar to a PIN).	
Reversal Flag	**Y** (Yes) or **N** (No)	This shows whether the authorization for the transaction was released or not.
Transaction Country Code	Name of the country where the transaction occurred. Example: UNITED STATES, CANADA, MEXICO, etc.	
US Currency Amount	US equivalent of the Original Currency Amount.	

Note: If a transaction has posted, you can also use this page for disputes. Click on the check box beside the transaction in question, then click Initiate **Dispute** at the top of the page. Select your dispute reason and click the **Dispute** button. A form specific to your dispute reason will display.

Also, click a link in the **Card Number** column on the Transaction History page to view additional details on the card used in the transaction.

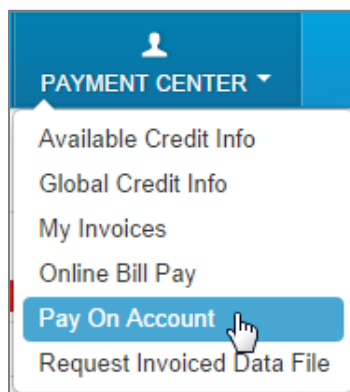The information on the Card Balance Information page is in real-time.

Pay an Invoice

If your account is setup for Electronic Bill Pay (EBP), then your users will have access to the Pay On Account feature in iConnectData (ICD). Pay On Account allows you to remit payments on your Comdata account when you have invoices available and ready to be paid.

Please note that if your account has a payment method other than EBP, then you will not have access to this module.

1. To access, select Pay On Account from the ICD home page (**Payment Center > Pay On Account**).

   Note: You cannot initiate payment on an invoice the date the invoice is generated.

2. You are directed to the Pay My Accounts page.

Setting Up Payment Methods

As a first-time user, you will need to set up and store your checking and/or savings account information for use in making payments. Once you have a payment method set up, you can edit or delete it, if necessary.

Setting up a Bank Account

1. On the Pay My Accounts main page, select **Payment Methods** from the left-hand menu.

2. On the Payment Methods page, select **Add a new bank account** from the drop-down and then click **Go**.

3. On the Add New Bank Account page, complete each field with your bank account information. Click **Add** when finished. Please note:

- If you enter an account nickname, ensure that it can be easily identified if you use several bank accounts.

- You must select the check box at the bottom of the page to agree to the authorization agreement terms and conditions. It is recommended that you first select the link to read the authorization agreement.

4. A confirmation message will display with your bank account information. Ensure everything is correct. If not, return to the Payment Methods page and make edits.

Editing an Existing Bank Account

You can edit a payment method from the main Payment Methods page. You can make corrections, update information, or even delete an account.

1. Select the account you want to edit from the **Payment method** column. Note that if a nickname was entered during setup, that nickname will display as the account's name. If no nickname was entered, the masked bank account and routing number will display, as shown below.

2. Make changes to any of the fields and click **Update** when finished. Note that selecting **Delete** permanently removes the account, but you can add it back at any time.

Making Payments

Once your payment method is setup, you can begin remitting payments to Comdata.

1. On the Pay My Accounts page, select the check box for each account you want to pay and then click **Continue**.

2. The next page displays the amount due for each account you selected. Note that:

    *   You cannot initiate payment on the invoice the date the invoice is generated.

    *   The **Payment Amount** method column contains the total amount due that you will pay when you select **Continue**. You can change this to any other amount, but it cannot be lower than $1.00 or higher than the total amount due.

    *   Payments must be entered with a decimal.

    *   The **Payment Date** will always be the current date and cannot be changed.

    *   If you don't want to pay on an account in the list, uncheck the box next to the account

    *   The **Cancel** button will direct you to the Payment Activity page

    *   The total amount due displayed between the hours of 10:00 pm - 8:00 am CDT may not reflect your activity during these hours. It is recommended that you initiate your payments during the normal processing hours of 8:00 am - 10:00 pm CDT.

    *   If you are set up to pay only one Comdata account, this is the first page you will see when selecting **Pay My Accounts**. Step 2 will be replaced with Step 1.

    *   You are limited to only one payment per day on each of your accounts.

(see image on next page)

3. Select a saved bank account from the **Payment Method** drop-down and then select **Continue**. If you do not have any bank accounts saved, you must select **Enter a new bank account** before you can proceed. See Setting Up Payment Methods for more information.

4. Review your payment information to verify everything is accurate. To make edits, click **Change** to return to the previous page. Select **Delete** to remove a payment. Select **Cancel** to go to the Payment Activity page.

In the example image below, a payment was already made earlier in the day for this account. Since only one payment is allowed per account each day, a warning message is displayed, stating that their payment (Payment 2 only) will not process. However, the payment will be stored for future use. If everything is correct, click **Make Payment**.

Note: Delete is not an option if you have only one account listed on this page.

5. The Payment Request Submitted page displays after confirming your payment. Select **print this page** at the top of the page to print a copy for your records.

(see image on next page)

Payment Request Submitted

Thank you - the payments below have been submitted. Please print this page or make note of the Reference IDs.

Payment 1

Reference ID:	1385200003
Payment Status:	**Payment Submitted**
Date and Time: (mm/dd/yyyy)	**09/30/2011 10:41:30 (CDT)**
Account Code:	EB705
Payment Amount:	$2,244.89
Payment Date: (mm/dd/yyyy)	09/30/2011
Customer Name:	**Bob Smith Trucking Bob Smith**
Payment Method:	**BOB** **Payment method added successfully**

Payment 2

Reference ID:	1385201003
Payment Status:	**Payment Submitted**
Date and Time: (mm/dd/yyyy)	**09/30/2011 10:41:32 (CDT)**
Account Code:	EB711
Payment Amount:	$556.00
Payment Date: (mm/dd/yyyy)	09/30/2011
Customer Name:	**Bob Smith Trucking Bob Smith**
Payment Method:	**BOB** **Payment method added successfully**

Back to Payment Activity

Reviewing Payment Activity

The Payment Activity page displays transactions for all of your associated active accounts. You can review the status of transactions and drill into more detail.

1. Select **Payment Activity** from the left-hand menu.

2. In the Display drop-down, you can select:

- **Payments for all active accounts.** Displays all payments for all of your active accounts. This option is defaulted.

- **My payments.** Displays only initiated payments

- **Account Name (example: EB711).** Displays only the payments associated to an individual account.

To drill down into more details on an individual payment, select the link in the Reference Id column.

3. The Payment Details page opens, displaying all information associated with the selected payment.

   Note: Image below is a split image of the full screen.

Running Reports

ICD contains several preformatted, canned reports that allow you to review specific details on your account. Use these reports to monitor and manage many aspects of your account, such as transaction spending per cardholder and disputed transactions. Follow the steps below to access and run reports.

1. On the ICD home page, click **Reporting > reportQ**.
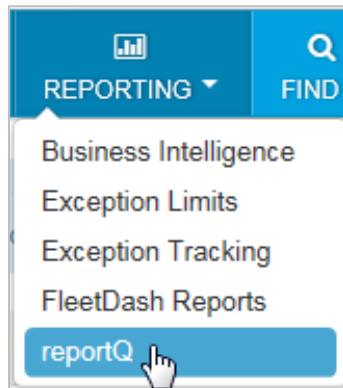
2. This action directs you to the Quick Reports page, a library of reports available to you. Quick Reports is split into two sections:

   - The left side contains all quick reports available to you. Click one to open the report parameters.

   - The right side allows you to view the status of reports and download them when finished.

3. When you open a report on the left side of the page, a list of parameters specific to the report display. Use these options to customize the report and run it for your purposes.

Once you click **Submit PDF** or **Submit Excel**, the system returns you to the main report page and the status of the report will display in the right side of the page.

The following reports are available to you as a Mastercard Multi-Card user by default:

- **Card Listing Report.** View current record information for all cards associated with your account, including the name on the card, card/vehicle/employee ID number, spending profile and description, and last activity date. Available in PDF and Excel.

- **Cardholder Activity Fleet.** View transaction details by cardholder, including card information, merchant information, spend per transaction, price, and quantity of the purchased products. Available in PDF and Excel.

- **Cardholder Activity Report General.** View transaction detail by card, including card information, merchant information, spend per transaction, price, and quantity of purchased products. Use this report to monitor your cardholders' spend. Available in PDF and Excel.

- **Cardholder Group Summary.** High-level view of spend by card, including card information and spend by merchant category code (MCC). Available in PDF and Excel.

- **Cardholder ID Report.** View cardholder ID information, including associated customer ID, and first and last name of cardholder. Available in PDF and Excel.

- **Cardholder Usage Report General.** View transaction detail by cardholder, including customer information, merchant information, spend per transaction, price, and quantity of purchased products. Use this report to monitor your cardholders' card usage. Available in PDF and Excel.

- **Corporate Dashboard.** Provides interactive account summary of spend and allows you to view year over year, types of products, and geographical information. Requires Adobe Flash Player.

- **Corporate Payments Account Spend Report.** View a high-level overview of your program performance month-by-month. Provides graphic summaries of key program metrics including your month-by-month spending, spend per transaction, top vendors, and rebate information. Available as a PDF only.

- **eCash Transaction Activity - All Activity.** Ability to select Load, all Withdrawals, ATM, POS Debit, Direct Deposit, Comcheck Convenience Check, Fuel, or Telecommunications.

- **eCash Transaction Activity - Company Only.** Detailed Express Cash data, such as transaction type, senders name, and ancillary data.

- **Exception Listing Report.** View a list of transactions that trigger exception flags that have been set up on your account, including transaction details. Available inn PDF and Excel.

- **F Save Report.** View transaction details by customer ID, including merchant and SmartBuy information, price per gallon (PPG) paid, potential SmartBuy discount amount, and difference between paid potential discounts. Use this report to view potential savings available to your fleet at SmartBuy locations. Available in PDF only.

- **Fuel & Maintenance MCC Report.** View spends by merchant, including merchant and merchant group details, and account, customer, and card information. Available in PDF and Excel.

- **ID Report.** View transaction-level detail by prompted ID and name. Includes transaction detail, prompted ID number that was entered at the time of purchase, and the point-of-sale name associated with the prompted ID. Available in PDF and Excel.

- **Mastercard Dispute Report.** A record of all credits applied to customer accounts related to customer-initiated disputes.

- **Mastercard Rebates Report.** Report of rebates paid to customers. Data is updated every 12th business day of the month.

- **Merchant Location Activity Report.** High-level view into spend and transaction volume by individual merchant location, including merchant information, average price per unit (PPU), gallons, and spend per merchant. Available in PDF and Excel.

- **MCC Summary Report.** View total spend and merchant details by merchant category code (MCC). Use this report to compare total spend across MCCs. Available in PDF and Excel.

- **MPG Report.** View mileage details per transaction by vehicle or unit number, including beginning and ending odometer readings, miles driven, miles per gallon (MPG), cost per mile (CPM), and transaction information. Available in PDF and Excel.

- **Product Summary.** High-level view into spend and transaction volume by product purchased, including quantity purchased, spend per product, and hierarchy data. This report also includes the discount and rebate net cost. Use this report to monitor patterns in spend per product. Available in PDF and Excel.

- **T&E Cardholder Activity Summary.** View travel and entertainment transaction details by cardholder, including total spend and transaction volume, and spend and transaction volume by airline, hotel, rental car, and other. Available in PDF and Excel.

- **T&E Cardholder Airline Activity.** View air reservation transaction details by cardholder, including card information, merchant information, carrier or service class code, departure and arrival location, and flight number. Available in PDF and Excel.

- **T&E Cardholder Car Rental.** View car rental transaction details by cardholder, including card information, merchant information, rental and return information, and additional rental details (when provided by merchant). Available in PDF and Excel.

- **T&E Cardholder Hotel Activity.** View hotel transaction details by cardholder including card information, merchant information, arrival and departure date (total nights purchased), and room rates (when available). Available in PDF and Excel.

- **Transaction Listing.** View transaction detail captured at the time of purchase, grouped by card number, including card information, merchant information, spend per transaction, price, and quantity of the purchased products. Use this report to reconcile accounts or find missing transactions. Available in PDF and Excel.

- **Transaction Listing Enhanced.** View transaction detail captured at time of purchase, grouped by card number, including card information, merchant information, spend per transaction, price, and quantity of purchased product. Report is summarized in different tabs to provide quick summary of transactions such as spend by Cust ID, Gallons by State, Top Merchants, etc. Available in Excel only.

- **Vehicle Listing.** View vehicle numbers associated with your card numbers, including account and customer IDs, card information, and Misc1/Misc2 data (if available). Available in PDF and Excel.

- **Vehicle Report.** View transaction details by vehicle number, including card information, merchant information, spend per transaction, and description, price, and quantity of purchased product. Available in PDF and Excel.

Using the Resource Center

The ICD Resource Center is the central location for accessing support and training materials on many of Comdata's products. The home page offers the ability to search for content via a search bar or navigate through the product pages. For example, if you want to learn about Alerts and Notifications, type "Alerts and Notifications" in the search bar and press **Enter** on your keyboard. The search results will display every document and/or video related to your search criteria.
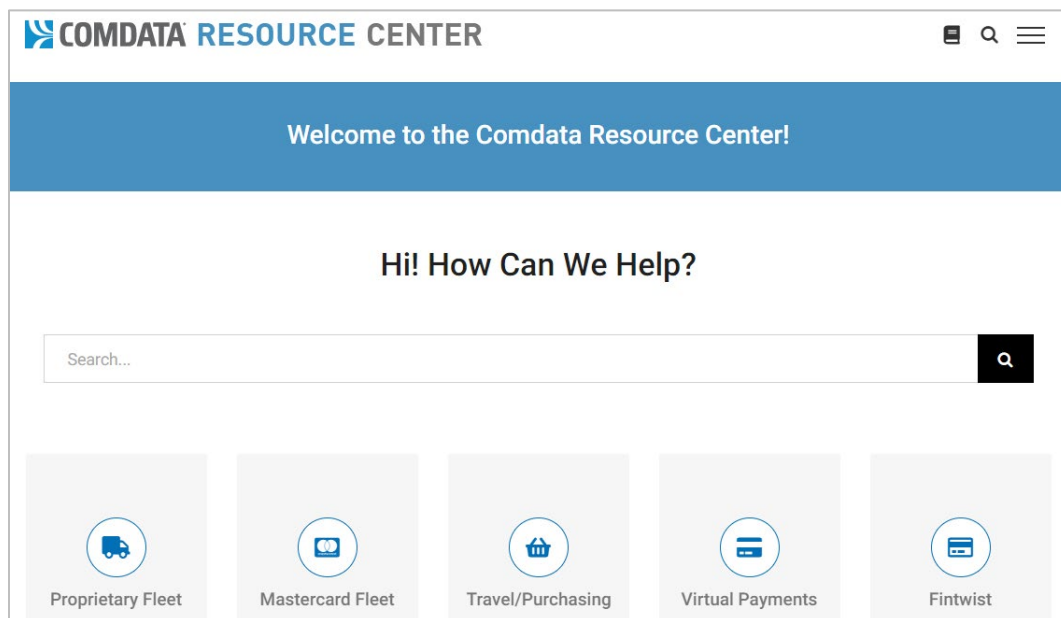
Or open one of the product pages. For example, Mastercard Fleet and Travel/Purchasing contain resources on Alerts and Notifications and many other products.
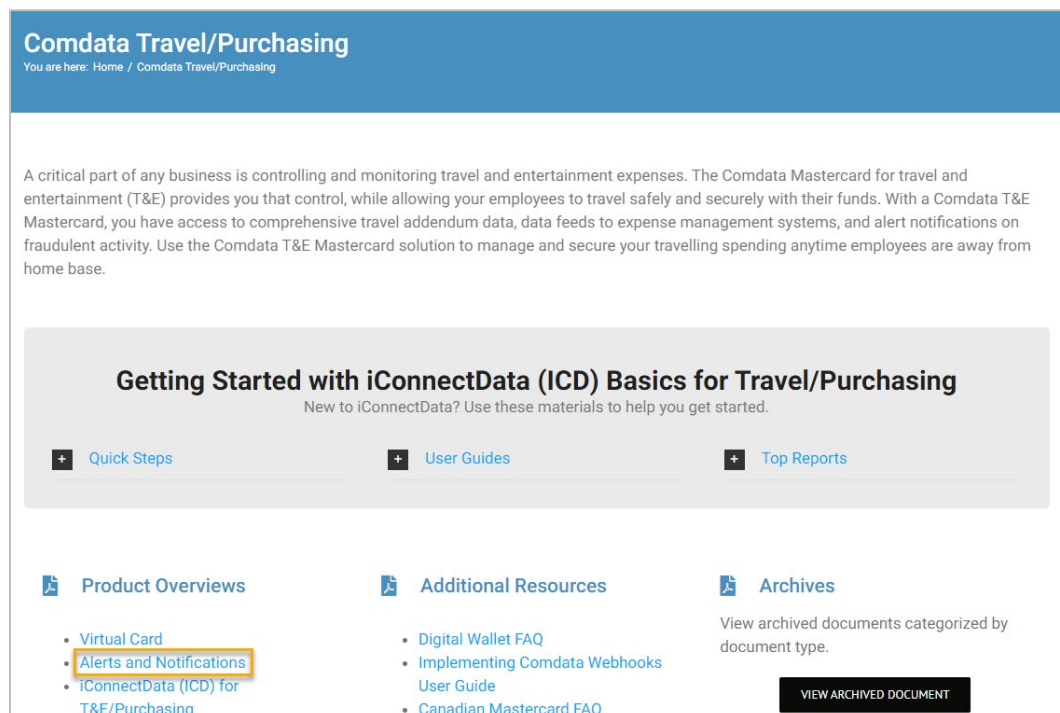
Appendix

Sample Cardholder Email Communication

Below is a sample of the email communication you can send cardholders when they first sign up for a Comdata Mastercard Multi-Card. Contact your Comdata account representative for an Alerts and Notifications brochure to include in the communication.

_____

We are excited to announce the rollout of a new program at <INSERT COMPANY NAME> - a corporate Mastercard® credit card program supported by Comdata. This tool signifies our ongoing commitment to take complexity out of the business and put information and controls in the hands of our business managers. The new credit cards are intended to be used for <Insert Card Usage Parameters>.

There are many positive attributes of this program. Most notably, it:

- **Provides sharing in the credit card interchange fees with Comdata** – every dollar we spend turns into rebate dollars to <INSERT COMPANY NAME>

- **Shifts expense liability to the company and off of your personal credit cards** – you no longer need to wait for reimbursement

- **Makes it easier to pay for minor, but necessary items you need to run your department** – no more one-time vendor set ups

- **Creates transparency (and accountability) around expense details** – real time, on demand information to keep up with financial transactions

- **Provides fraud protection and services to limit impact of misuse** – flexibility for our business managers; protection for our company

As part of the rollout process, we are making Purchasing policies more consistent across the business, as well as documenting best practices that are already being followed.

The Corporate Card team has worked hard to 1) design an intuitive solution that will accommodate our various processes and platforms, and 2) anticipate and plan for the downstream effect that will occur by instituting this program. The latter is always more difficult.

As a follow up, you will be receiving a message from the Corporate Card team setting expectations around the program and how to order cards for your department. The cards should be available for your use by <INSERT DATES>.

Prior to receiving your card in the mail, you will receive an email allowing you to enroll in Comdata's Alerts & Notifications text message program. Additional information about the text alerts can be found in the attached brochure. You may enroll in the text alerts prior to receiving your card. Simply take action on the email you receive with instructions.

Thank you in advance for your participation and making this program a success.

Cardholder Agreement

Below is a sample of the cardholder agreement. Remember, this agreement should be signed by the cardholder and their supervisor.

_____

I, _____ hereby acknowledge receipt of a _____ Mastercard, issued by Regions Bank (the "Card") and provided to me by my _____ ("Company"). As a corporate cardholder, I agree to comply with the terms of this agreement, including the guidelines outlined in the _____.

I understand that the Card will not be used for personal, family or household purposes or for any purpose that is not for the benefit of the Company. Further, Card may be used only for valid and lawful purposes.

I understand that I will not request or receive cash back from suppliers as a result of exchanges, rebates, and refunds or for any other reason.

I understand that I am the only person authorized to use the Card assigned to me. I will not authorize the use of this Card by other company employees who may want to use it to make approved purchases.

I understand that the Company can terminate my right to use the Card at any time, for any reason.

I have reviewed the _____. I understand the procedures and requirements for using the Card and for providing the required documentation for each transaction made on the Card.

I understand that any violation of the terms of this agreement may result in disciplinary or civil and criminal legal action, up to and including termination of employment. I understand that I will owe the Company an amount equal to the total of any discrepancies, of the total amount of any personal gain, and/or of any fees related to the collection of such money. I understand that the Company may elect to collect this money even if I am no longer employed by them.

_____   _____
Cardholder Name (print)   Manager or P-Card Dept

_____   _____
Cardholder Signature   Date