

Citi® Virtual Card Accounts

Frequently Asked Questions

This document provides answers to frequently asked questions about using Citi® Virtual Card Accounts (VCA). These FAQs are meant to supplement information our clients may have previously received from Citi® Commercial Cards.

1. What is a Citi® Virtual Card Account (VCA)?

Citi Virtual Card Account, or VCA, allows Citi Commercial Cards clients to securely and efficiently pay merchants using plastic-less single-use or multi-use cards. Our award-winning solution replaces existing payment methods, such as cumbersome paper checks and even standard card solutions, to help streamline the payment process while offering greater control and flexibility.

2. What are the benefits of accepting Virtual Card Number payments?

By using Virtual Card Number payments, clients are able to benefit from the cost and process efficiencies associated with standard card payments, while being able to receive a greater level of control, flexibility and data associated with any given transaction.

- **Control:** Each transaction can be set: (a) as multi-use or single-use, (b) for a designated period of time (i.e., specific start and end date), (c) with an overall spend limit per Virtual Card Number issued, (d) with the ability to set the spend limit to an exact amount or allow for a percent buffer above the limit (i.e., useful for hotel and/or car rentals), (e) with the ability to select spend categories allowed, down to actual vendors, and; (f) with work-flow approvals based on user group, spend type or spend amount.
- **Flexibility:** Set up the Virtual Card Account tool in one of three ways: (a) provide employees with a Citi issued web-portal which they log into in order to request a Virtual Card Number anytime they need, (b) integrate the Virtual Card Account tool directly into your own system for a custom interface and direct feed into your internal system programs, or; (c) a file-based approach to pay suppliers via Virtual Card Numbers using existing Accounts Payable processes.
- **Enhanced Data Elements:** Each Virtual Card Number requested can be appended with additional data elements at time of Virtual Card Number request. Common pieces of data sent are cost center, department number, PO number, reason for purchase, and requestor name. For T&E purchases, additional data elements often requested are: traveler name, spend category, meeting ID/number, number of event attendees, date of travel/event, and employee ID.

3. What if my merchants do not accept Credit Cards or Virtual Cards for payment?

Citi Supplier Enablement Services plays a key role in helping Citi Commercial Cards clients maximize the benefits of their Virtual Card Account (VCA) programs by supporting all merchant on-boarding activities, including developing customized merchant outreach campaigns to communicate the roll out of Virtual Card Number payments, addressing merchant questions about the program, and providing general education on the benefits of card acceptance. If you have a list of non-accepting merchants which do not accept commercial card payments, Citi will review the list with our Citi Supplier Enablement Services team to onboard the merchants as appropriate.

Additionally, organizations often offer merchants incentives – such as accelerated payment terms or “preferred merchant” status – to encourage acceptance of Virtual Card Numbers and other commercial card solutions. Alternatively, you may mandate later payment terms for merchants who choose not to accept Virtual Card Number payments.

4. How is a Virtual Card Number different than other Citi Commercial Card payments that I make?

Virtual Card Numbers are processed via your merchants’ existing Point of Sales (POS) devices in the same way as other Card-Not-Present credit card transactions. By leveraging Citi’s VCA program, you can issue a unique Virtual Card per payment, each valid solely for duration of time you specify. This process effectively eliminates the need for merchants to store your credit card information, creating increased security and reducing the possibility of fraud.

5. How will I provide a Virtual Card Number payment?

The Virtual Card Number is shared with the merchant in the same way a normal Card-Not-Present account number is shared with merchants currently. If desired, Citi can also securely send an e-mail with the Virtual Card Number payment details, inclusive of an ‘image’ of the front and back of the card, needed to process the payment to the e-mail address provided for that merchant at point of purchase. The merchant will receive a separate e-mail for each Virtual Card Number payment. Sample e-mails are provided at the end of the document.

Alternatively, Citi offers a fax functionality in which the card image and authorization information can be received via fax. Faxes are stored for seven days and are accessible to your Citi team via an online portal during that 7-day window. This feature is commonly leveraged for purchases made with hotels where the hotel requires a front and back image of a card to be faxed to the hotel site before it will process the purchase request.

6. What e-mail address or fax number should I enter for the merchant when sending the Virtual Card Number payment details?

Although we would love to say use the stored e-mail address or fax number from your GDS booking system, we find that these are often outdated. Therefore, we recommend – unless this is a merchant who has already provided a centralized e-mail account to your Accounts Receivable department or a broad distribution list accessible across multiple employees – you leverage the e-mail address supplied when making the booking/reservation with the merchant. For instance, if you are booking a hotel stay at the Marriott in San Francisco at Fisherman’s Wharf, then ask for the e-mail address or fax number for that specific establishment to ensure the e-mail or fax is not inadvertently sent to another Marriott location, thereby causing an error with the booking.

7. What information is contained within Virtual Card Number e-mails and faxes?

- **Virtual Card Number and related details:** The 16-digit Virtual Card Number, a validity date, the unique CVC2 (e.g., 3-digit security code typically located on the back of a physical card), and the corporate billing address of your buyer.
- **Payment parameters:** Including the billing amount to be processed for payment, and whether the Virtual Card Number can be used only once or for multi authorizations up to the billing amount. The Virtual Card Number will be successfully authorized for payment only if the client-specific parameters are met.
- **Enhanced Data Elements:** You can choose to store and present in the e-mail any of the custom data fields completed at time of booking which will aid with the reconciliation process. Select the data elements based on your unique needs. It is best to confirm with your vendors what information they require when determining how to set up the e-mail/fax. Note: only one e-mail/fax format is made available per client, therefore, whatever fields/format provided for one merchant will be provided for all merchants.
- **Card Image:** Although this is an optional feature, and not often required to process the Virtual Card Number for most merchants, we do find that most hotels and rental car agencies do require the image to be included on a fax or e-mail for processing.
- **Special Instructions:** Contact information and/or additional processing details can be provided within the customizable section of the standard e-mail/fax format.

8. What does the merchant do with the information received in the Virtual Card Number e-mail/fax?

The merchant will process the payment as instructed in the e-mail by entering the 16-digit card number and additional data elements, as required, through their credit card processing equipment. The credit card transaction must meet the payment parameters in the e-mail (amount, date of expiration, etc.) in order to receive a successful authorization.

9. How does the merchant know which invoices this payment is for?

When requesting the Virtual Card Number for making the payment to the merchant, you can provide the remittance details in the e-mail that specifies the invoices in scope for payment or other payment information. You may choose to bundle multiple invoices into one payment; in those cases, the e-mail typically will list all invoices associated with the payment. Or you may choose to send remittance details separately from the virtual card e-mail.

10. How long will it take my merchants to receive payment?

As with most credit card transactions, merchants will typically receive their funds within 24 to 48 hours once they process the Virtual Card Number.

11. What if the merchant does not process the payment before the end of the validity period?

The Virtual Card Number payment cannot be completed after the validity period. In this scenario, you may modify the Virtual Card Number payment parameters or, instead, opt to supply a new Virtual Card Number to the merchant.

12. Who would the merchant contact about the details in the Virtual Card Number e-mail or fax?

Should there be any questions or concerns about the e-mail or fax, your merchant will need a contact person to assist with answering any questions. We recommend the contact person be the person who is managing the booking if the purchase is for T&E or Meetings & Events (M&E), or the person who is submitting the expense if the purchase is for B2B activity.

Please do not inform merchants to reply directly to the Virtual Card Number e-mails, as they are sent from an automated mailbox to which you do not have access. Responding directly to the e-mail (i.e., by hitting "reply") will delay any requested action.

13. What should I do if I sent a Virtual Card Number, but the merchant has not received it?

If relying on fax or e-mail for communicating the Virtual Card Number, ask the merchant to check their spam folder for the e-mail or near the fax machine for the fax document. If the e-mail or fax still does not appear to have been received, verify you have the correct e-mail address or fax number. A fax can be resent within seven days of the Virtual Card Number issuance. E-mails cannot, unless you have opted to have a copy of the e-mail sent to an internal e-mail address; then you can re-forward the e-mail to the merchant. If needed, you can send a new Virtual Card Number to the merchant for payment.

14. What do I do if the Virtual Card Number is declined when the merchant seeks authorization?

Normal card payment protocol would ensue. The merchant will need to verify the transaction amount, 16-digit Virtual Card Number, validity period and 3-digit CVC code (as required) associated with the specific Virtual Card Number have been accurately entered. In some instances, despite the information being accurately provided, errors may occur resulting in your merchant requiring a new Virtual Card Number to be issued in place of the one which was declined. Should this be necessary, simply cancel the current Virtual Card Number and issue a new one.

15. Can I modify or cancel a Virtual Card Number which was issued to a merchant?

Yes, you can make changes to the Virtual Card Number payment details once an account is issued. Your merchant, however, will not receive updates via e-mail or fax. You will need to update your merchant directly if a change warrants their awareness for processing.

16. How are Virtual Card Numbers secured?

First, Virtual Card Numbers are masked 16-digit numbers; these are not the real-card numbers. Therefore, should anyone gain access to a Virtual Card Number, it would have to be processed per the parameters determined at issuance or the purchase would be declined; it would not be possible to use that number for additional purchases. Additionally, because it is a masked number, the real card number is never provided and therefore remains secure from misuse.

Second, e-mails sent with the Virtual Card Number are sent via the Citi VCA solution, transmitted securely over the internet using an encrypted transmission feature called the Transport Layer Security (TLS) protocol. TLS adheres to both PCI standards and MasterCard or Visa network rules for encrypted transmission of card information. No special software is required to receive Virtual Card Number e-mails.

Merchants will receive the Virtual Card Number e-mails in one of two secure ways, based on whether or not the merchant's e-mail server supports TLS:

- If the merchant e-mail server supports TLS, the e-mail will be sent securely to the merchant's e-mail server, and then routed to the appropriate e-mail inbox. The merchant will be able to open the e-mail normally and immediately see the Virtual Card Number payment information.
- If the merchant's e-mail server does not support TLS, the merchant will receive an e-mail with a link to a secure MasterCard or Visa portal where the merchant will need to log in to retrieve the needed payment details. The merchant will need to complete a one-time registration process after receiving the first Virtual Card Number e-mail.

17. Are Virtual Card Number Payments subject to PCI Data Security Standards (DSS)?

Yes, Virtual Card Number payments, like other commercial credit card solutions, are subject to PCI DSS requirements. That said, Citi Virtual Card Numbers can offer additional safeguards against potential misuse beyond those typically available with traditional credit cards thanks to authorization controls that clients can apply to each Virtual Card Number at the time of creation. Single-use Virtual Card Numbers, for example, are valid solely for one authorization, after which the Virtual Card Number becomes inactive or disabled and cannot be reused for any additional activities, even if somehow the Virtual Card Number is disclosed unintentionally to a third party. Many Citi VCA clients apply this single-use control to the Virtual Card Numbers sent to merchants for payment.

Further information on PCI-DSS can be found at www.pcisecuritystandards.org. Please contact your merchant acquiring bank with questions about whether your card processing systems are in compliance with PCI-DSS guidelines.

Sample payment e-mail (MasterCard):



17. Are Virtual Card Number Payments subject to PCI Data Security Standards (DSS)?
(continued)

Sample payment e-mail (Visa):

This is an automated email Payment Notification generated by Visa for ACME INC.

<p>Buyer Information Contact Name: ACME INC. Email: tester@acmeinc.com Address: 514 Market Street</p>	<p>Supplier Information Contact Name: ABC Supplies</p>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------

The following payment has been authorized by ACME INC. to be paid using the Visa credit card account established with your company.

The last four digits of the card account number are shown below. The remaining card account digits can be obtained by accessing the URL within 1 day(s), by entering the last four digits of the card account and providing the validation information requested at the Website. Once the information has been validated, the remaining card account digits will be provided.

URL:
https://vpa.commercialservices.visaonline.com/CommercialLogin/SupplierNotificationWeb/notification.do?id=116217&value=FD7A38D7-AC6A-F17A-7403-2196916EE23E&locale=en_US

Note: Please do not click on the link for the URL. Instead, copy the URL text and paste it into your browsers address field. Some browser security settings may prevent you from accessing the URL directly if you click on it.

Card Account: XXXX-XXXX-XXXX-8670
Number of Transactions: 3

Gross Amount: 300.0 USD

The authorization for this card account number is for the gross amount shown and will expire in 10 day(s)

Invoice No	Invoice Date	Amount
INV1	01/06/2015	100.00