



U.S. Bank Corporate Payment Systems Program Administrator Guide



Table of Contents

Contact Numbers	3
Program Structure	4
Virtual Payment Managing Account Numbers:	4
Virtual Payment Types	4
Billing and Payment Types	5
Card Management Portal	6
Program Fees	6
Merchant Category Codes (MCCs)	6
Billing and Payment Methods	8
Card Issuance	9
Virtual Payment Program Management	9
Card Activation and PIN Selection	10
Credit Limits	11
Cardholder Declines	12
Common Declined Authorization Codes	14
Card Maintenance	17
Cardholder Access Online Log-in	18
Disputes	19
Central Travel System Account Disputes	21
Dispute Resolution – Credit, Charge Backs or Rebills	21
Fraud Prevention & Best Practices	21
Fraud Alerts	22
What Cardholders Can Do to Prevent Credit Card Fraud	23
What Program Administrators Can Do to Prevent Credit Card Fraud	23
U.S. Bank Secure Mail	23
Receiving a Secure Mail Message	23
Replying to or Composing New Secure Mail Messages	26
U.S. Bank Monthly Credit Card Auto-Purge Process	26
Card Reinstatement Process & Procedures	29
Cardholder Bankruptcy	29
Cardholder Benefits	30
Cardholder Verification	30
Travel Assistance	30
Automatic Worldwide Travel Accident Insurance	31
Filing a Travel Accident Insurance Claim	32
Excess Lost/Damaged Luggage Coverage	32
Excess Lost/Damaged Luggage Coverage Exclusions	32
Filing an Excess Lost/Damaged Luggage Claim	33
Liability Waiver Insurance	33
Insurance Documentation	33
The Importance of Filing Every Potential Claim	33
Financial Extracts, File Delivery and Data Feeds	34
File Transmission	34
Third-Party Expense Management Feeds	34

Contact Numbers

24-Hour Customer Service	800.344.5696
Customer Service International Collect Calls	701.461.2042
Access Online Technical Assistance Program Administrators Cardholders	877.452.8083 877.887.9260
Disputes & Dispute Follow-Up Fax	800.344.5696 701.461.3464
Fraud Investigations	800.523.9078
Collections	800.837.6708
Charged-Off Accounts	800.308.3648
24-Hour Visa Emergency Travel Assistance	800.VISA.911 (800.847.2911) / Collect 303.967.1096
MasterCard Travel Assistance	800.MC.ASSIST (800.622.7747)/ Collect 636.722.7111
U.S. Bank Managed File Services	800.765.9549 Option 1
Virtual Payments Supplier Support	855.268.5386
Access Online Payment Plus	paymentplus@access-online.com

U.S. Bank Program Administrator Support Team

Service Contact	
<Paste servicing information here>	Day to day program administrator support including: • Account maintenance/inquiry • Access Online Reporting • New managing account builds/card issuance • General questions and support
Relationship Contact	
[First and Last Name] [Phone] [Email]	Consultation and support for the following: • Program reviews • Product updates • Mergers/acquisitions • Contracts/rebates
Supplier Enablement Contact	
[First and Last Name] [Phone] [Email]	Manages the following supplier activities: • Supplier enrollment and updates • Initial supplier payment processing • Initial supplier payment processing • Supplier expansion • Enablement strategy and prioritization • Straight through processing (STP) enrollment

Program Structure

The card program is structured into hierarchies, which allows you to organize your program according to departmental need, and to simplify billing and reporting. A list of your hierarchies is provided below:

[3046 xxxx xxxxx]
[7129 xxxx xxxxx]
[4596 xxxx xxxxx]

Access Online Hierarchy

The components in a hierarchy include:

- **Bank:** this identifies the product (corporate card vs purchasing card).
- **Agent:** this identifies the kind of plastic associated with your program.
- **Company:** this identifies the billing and liability association for the individual accounts within the company. It is also known as a managing account.

Virtual Payment Managing Account Numbers: ***[insert last four digits here]***

Virtual Payment Types

Single Use Accounts

A one-time use account number is drawn from an account number pool and assigned to a supplier for a specific payment amount. The system generates an email payment notification to the supplier. The supplier retrieves account information from the email via an embedded link and processes the payments. In order to access the link and obtain the card details, the merchant will need to use a **PASSWORD**. This password is called a **CREDENTIAL TEXT**.

Pre-Authorized Limit Accounts

The supplier is provided with an assigned reusable account number set to a \$0 credit limit. The account number is unique to the supplier and retained in the supplier's A/R system. When a payment is authorized, the credit limit will be adjusted to the exact payment amount and the payment notification is emailed to the supplier. Once the supplier processes the payment, the account is reset to a \$0 credit limit.

Preferred Supplier Program

This is a program (included in the card program agreement) which provides certain suppliers with preferential interchange pricing.

Straight-Thru Processing

This payment type allows an electronic deposit for the exact amount of the Payment Authorization to be made directly into a supplier's depositing bank account. After deposit, the system generates an email payment notification to the supplier, providing payment remittance related details. No action is required by the supplier to process payment, as funds are deposited directly into their merchant account.

Card Program Liability Types

Liability of a card program identifies who is ultimately responsible for the balances due on a cardholder account. The three liability types available are Corporate, Contingent (also referred to as Individual Liability), and Joint & Several Liability. Corporate Card programs can be any of the three liability types mentioned above. All One Card, Purchasing Card and Virtual card payments are Corporate Liability. Your organization can choose to have differing liability types based on its needs.

Corporate Liability

The cardholder's employer is ultimately responsible for balances due on the cardholder account, and all collections efforts will be primarily with the employer. No credit checks are performed on cardholder accounts.

Contingent Liability

The cardholder is ultimately responsible for balances due on the account, and collections efforts will be made to reach the cardholder in case of late payments. The company is responsible for legitimate business charges, should the cardholder be unable to pay. The credit systems will occasionally conduct a soft-inquiry on the cardholder's credit profile, however it would not impact the cardholder's credit score.

Joint & Several Liability

Both the employer and the cardholder are responsible for the balances due on the cardholder account. In cases of late payment, the cardholder would be contacted; however, after 90 days past due, the employer will be contacted regarding the outstanding balances.

Billing and Payment Types

Billing Types identify how statements are generated and Payment types identify how funds are paid to U.S. Bank and applied to the account. The available billing types are corporate billing or individual billing.

Corporate Bill and Corporate Pay

Corporate billed accounts receive one central master statement which includes transaction level detail for each cardholder in that managing account, with cardholders receiving "memo statements" which provide transaction level information for their individual account. Corporate payment indicates that the organization will send one payment to cover all balances due, and the payment will be applied at the managing account level.

Individual Bill and Individual Pay

Individual billed accounts will receive an individual statement per cardholder which will include instructions on how to pay the bill. Individually paid accounts will have all payments applied at the

individual cardholder account.

Cycle Dates

The cycle date is the date when a statement is generated. Activity for the cycle period is calculated with a previous balance to provide a new account balance. Statements are generated and available online the day after cycle and mailed out within three days via the U.S. Postal Service if requested.

Due Dates

The payment due date may vary based on your program; due dates are a specified number of calendar days from the cycle date. Please refer to your card program agreement for specific payment terms.

Expanded Limits

Expanded limits are applicable only to managing accounts with higher spending limits. Generally, this is applicable to managing accounts that have over \$10 million in spend or payments per cycle. Expanded limits account have a slightly different structure to support the larger spend needs.

Card Management Portal

[Access Online login site](#)
access.usbank.com

Organization Short Name is: **[CLIENTOSN]**
You will also need your Username and Password.

<Insert User ID's and Access Level Here>

****U.S. Bank Access® Online Mobile App** - U.S. Bank Access Online Mobile App works with iPhones and Android Smartphones. The app can be downloaded from the App Store or Google Play.

Program Fees

Program Fees (including late fees, foreign exchange fees, and expedited fees) are outlined in your card program agreement. Please consult your Relationship or Account Manager if you have any questions about applicable fees.

Merchant Category Codes (MCCs)

You have the ability to block or allow different merchant category codes for your card program. For the most recent list of MCC Codes and Groupings, please contact Client Services.

The following MCC templates have been applied to your program:

[TO BE COMPLETED BY IPM]

Access Online Training Resources

Instructor-led training courses are available for program administrators. Self-guided trainings are available to both program administrators and cardholders.

Access Online self-guided training classes are available by following this [link](#).

Current Web Based Training Passwords:

<Add WBT password information here>

The training passwords change approximately every 60 days. Updated passwords are available through the training link within your organization's Access Online profile.

Registration for Access Online Instructor-Led classes for program administrators is available [here](#).

Billing and Payment Methods

Managing account and cardholder statements are available in both hard copy and electronic formats in your Access Online.

Statement Suppression

Statements are available electronically, if you have a need for paper statements reach out to the Client Services team to make the change.

Payment Information

While electronic payments are an industry-accepted best practice, U.S. Bank accepts any of the following payment methods:

- ACH
- Wire
- Check
- TelePay (via automated system or by calling a customer service representative)
- AutoPay (Direct Debit to a designated account)

Payment methods can be changed at any time throughout the duration of your program. If your organization would like to make changes to your payment method, please contact Client Services and they can provide the necessary documentation to assist with next steps.

ACH Payment

Client Initiates ACH Payment to U.S. Bank Corporate Payment Systems

ACH Payments will only be accepted in a CTX or CCD format.

ACH Payments may be sent to:

FRD/ABA Routing Number: **091000022**

U.S. Bank / DDA Acct. Number: **16-digit client billing account number**

TR Number (optional): **04200001**

Customer ID is **1510351118**

Wire Transfer Payment

Client initiates Wire Transfer to U. S. Bank Corporate Payment Systems

TO: **U.S. Bank National Association**

ABA/Routing #: **091000022**

DDA/Acct #: **Please use 16-digit account number**

SWIFT Code: **USBANKUS44IMT**

Please include cardholder name in wire instruction comments.

Mail Payments

Please note that if payment will be made by check, the full 16-digit account number must be included on the check so that payment can be applied accordingly.

Overnight Mail Address:

Corporate Payment Systems
830 North 11th St.
Department 790428
St. Louis, MO 63101
866.257.2861

Standard Mail:

Corporate Payment Systems
PO Box 790428
St Louis, MO 63179

Cardholder Payments

Cardholders can pay U.S. Bank directly by:

- **Check:** Payments can be mailed to the payment remittance or overnight payment remittance address listed above.
- **TelePay:** Cardholders can call Customer Service at 800.344.5696 to set up payments by phone.



- **Mobile App or Access Online:** Cardholders can make payments through the Access Online Mobile App or in Access Online by visiting access.usbank.com. *Once in the system, the cardholder would go to Account Information → Statement → Pay Electronically and enter in their payment account details.*

Cardholder Billing Inquiries

U.S. Bank - CPS
PO Box 6343
Fargo, ND 58125-6343

**Please include the referenced account number with all payments or correspondence.*

Mailing Address

U.S. Bank Corporate Payment Systems
200 S. 6th St, EP-MN-L25C
Minneapolis, MN 55402

Card Issuance

Program administrators may submit requests for new card through Access Online. In most cases, the account set-up process can be completed in a few minutes and the account number is generated immediately.

If the new card needs to be expedited, please create the card in Access Online and select the appropriate shipping method. The card will be created overnight, and shipped out the next business day.

Program Administrators can complete all cardholder account maintenance through Access Online; including account closures, address changes and cardholder credit limit adjustments.

Virtual Payment Program Management

Card numbers can be created through an automated process, or they can be created in the online form of Access Online. The automated process feeds U.S. Bank information directly from your organization's accounting software, whereas the online form allows for manual payment creation within the portal.

Supplier Enablement

The Enhanced Supplier Management area of Access Online allows the Program Administrator to add supplier names and details to the system. This is a best practice method for updating the virtual card program. Alternatively, Program Administrators can contact the Supplier Support team and provide the following details for set up:

- Client contact name
- Supplier/vendor ID
- Supplier phone number
- Supplier contact at vendor
- Supplier email address
- Confirmation if Precise Pay should be added to the Supplier profile
- Which hierarchy this supplier should be linked to

What is Precise Pay?

Precise Pay functionality drives greater control and auto reconciliation by controlling the precise payment amount that may be authorized on a Single Use Account. This eliminates manual reconciliation processes, audit implications and supplier follow-up regarding payment discrepancies.

NOTE: Not every supplier or transaction will work with Precise Pay due to the following:

- Terminal limitations when processing can occur

- Combined Invoices
- Dollar Drop test transactions (\$1.00 additions for processing)

If there are any issues processing payments that fall into this segment, please contact the Supplier Support team for assistance.

NOTE:

- In some cases, the U.S. Bank Supplier Support team can provide temporary, real-time removal of Precise Pay on the assigned Single Use Account to allow merchants to re-process declined transactions due to Precise Pay limitations.
- Client also has the option of cancelling and reissuing the payment.

Entitlement to send CVV codes

Program Administrators can request the ability to receive CVV/CVC codes by contacting Client Services to have Secure Email added to the User ID. Once this functionality is enabled Program Administrators can receive CVV/CVC codes directly from the card management system to their email address, via U.S. Bank secured mail process. Please refer to page 21 for additional details on Secured Mail.

Card Activation and PIN Selection

Upon receipt of their card or virtual account number cardholders must call U.S. Bank Customer Service at 800.344.5696 and follow the steps below for card activation. Please note that your organization may have chosen something other than the Social Security Number for card activation. In this case, please provide this four-digit code to the cardholders and remind them to use it in place of the last four digits of the Social Security Number.

	• Required Information* : 16-digit Account Number, Mailing Address, ZIP Code, Business Telephone, last 4 Digits of Social Security Number or other four digit code provided by Program Administrator
	• Call 800.344.5696 and complete the following prompts:
1.	
2.	• “Welcome to Corporate Payment Systems. Please enter your 16-digit account number”
3.	• “Please enter the five-digit ZIP of your mailing address.”
4.	• “To activate your account, press 1.”
5.	• “To activate your account, please enter in the last four digits of your social security number.”
6.	• “Please enter your preferred business phone number, beginning with the area code.”
7.	• Listen to Express Consent notification. Accept or decline the terms to activate your card.
9.	• “Your card has been successfully activated. Thank you.”
10.	• “Please select a new 4 digit Personal Identification Number.”
11.	• “For verification, please re-enter the PIN you selected.”
12.	• “Thank you. Your PIN has been updated.”

* If nothing is entered in the SSN/Activation field cardholders will use '0000' when calling to activate their cards

*For SSN requirement this can also be the PIN activation provided by the program administrator during implementation.

*If the cardholder is unable to provide all required information, they will be transferred to a Customer Service Representative for personal assistance.

Credit Limits

Managing Accounts Limits

Managing Account Limits are established when the managing account is created for your organization. Limits can be adjusted by calling or emailing the Client Services team with your request.

Cardholder Limits

Corporate (T&E) cardholder limits can be hard-capped, meaning the cardholder cannot spend more than the credit limit established, or they can be provided with increased limits for travel and entertainment expense codes.

Increased Limits for Travel and Entertainment (T&E)

Upon request, U.S. Bank can provide T&E cardholders with increased travel and entertainment purchasing capability when the cardholder has exceeded their available spending guideline under the following conditions:

- The account is not suspended or closed
- The transaction falls within travel specific Merchant Category Classification (MCC) codes

Increased limits are made available at a hierarchy level and will impact all cardholders in the hierarchy. The following table outlines what the increased limits would be for various credit limit tiers:

Credit Limit	Cycle Velocity
Up to \$5,000	\$25,000
\$5,001 - \$25,000	\$50,000
\$25,001 - \$50,000	\$75,000
\$50,001 - \$100,000	\$100,00
\$100,001 +	Equal to established credit limit

How Credit and Cash Limits Are Calculated

Example

Credit Limit = \$3500

Cash = 20% (\$700)

How to Calculate a Cardholder's Retail Credit Limit

Example

\$3500 (Limit)

- \$700 (Cash)

\$2800 (Limit *minus* what is reserved for Cash)

The balance may consist of both travel and retail purchases. Retail is not a separate limit. ALL charges make up the balance.

If your organization has requested increased travel limits for its corporate cardholders, once the available limit has been met, the cardholder can continue to spend up to \$25,000, but transactions that fall outside travel-related merchant category codes will be declined.

The cardholder still has access to T&E. Assuming the account is open, if they attempt a *retail purchase (like Walmart)*, their charge will decline. If they need to purchase an airline ticket or pay for a hotel or food that charge will still be approved.

Cash Access

Cash Access is separate from the credit limit and is a percentage allocated to cash (e.g.; 5%) and the limit is replenished when a payment to the account is received. If a cardholder processes their expense report monthly, their cash limit will also replenish monthly.

Adjustments to Cash and Credit Limits

Any adjustment requests for cash or cardholder credit limits must come from the Program Administrator and can be processed directly in the card management portal or by contacting Client Services. Cash cannot be maintained through Access Online if the existing cash field (e.g.; cash %) on the account is 0. Any changes to this must be requested through Client Services.

Please contact your relationship or account manager for assistance if cash is not included on the contract as a contractual modification will be required.

Most cash adjustment requests are processed the same day received; however, please allow up to 48 hours for processing. The Account Coordinator will notify the Program Administrator of any issues or concerns with processing the request.

Reduction of Credit Limits

Corporate Card accounts are reviewed regularly by the U.S. Bank Risk Assessment Department. As a result, an account's credit limit may be decreased due to:

- Non-Sufficient Funds checks (NSF)
- Excessive non-business charge activity
- High cash usage
- Sporadic changes in charge activity and/or pay history
- Account delinquency

The U.S. Bank Client Services team will notify Program Administrators if any cardholders will have their credit limits decreased. Program Administrators may request reconsideration of the credit limit reduction and should submit this request along with a business justification to the Client Services team in writing.

Cardholder Declines

If a cardholder's transaction is declined, the decline reason can be viewed in Access Online via the Account Management screen → View Account Profile → Account Authorizations. A quick reference guide is included below, as well as decline reasons. The Access Online Help Desk can assist with clarification on the decline reason.

Understanding Declined Transactions

You can use this quick reference guide as a fast reminder of the basic steps to find out why the merchant declined a transaction at the point of sale.

1. Select **Account Information**

2. Click **Cardholder Account Profile**



3. Specify search criteria
4. Click **Search**

Cardholder Account Profile

Search & Select an Account

[View Diversion Account](#) | [View Managing Account](#)

Cardholder Account Search

Search for an account by Cardholder Account Number, Account Unique ID, Name, or Social Security Number. You can also find a cardholder account by first [Searching for a Managing Account](#).

Account Number (Last 4):

Account Unique ID: [?](#)

OR

Last Name (or Vehicle Name): First Name:

OR

Social Security Number:

OR

Search

5. Click **Account Authorizations**



- Click the declined transaction's authorization time link.

Cardholder Account Profile
Account Authorizations

Card Account Number: *****8774, CHASTIN J DORDING
Card Account ID: 212095029942

Name:
Records 1 - 2 of 2

Auth Date	Auth Time	Response	Auth Number	Type
02/17/2011	04:42 PM ET	Approved	074354	Mail/F
02/17/2011	03:34 PM ET	Declined		Mail/F

- Review the information on the *Decline* tab

Decline Account Merchant Parent Diversion Process

The Request was declined due to 0805 Exceeded account single trans limit
The Request was declined at the INDIVIDUAL
The velocity type for the decline was NOT DECLINED FOR VELOCITY
The following reasons would also have declined the request:
1. 0805 Exceeded account single trans limit

Common Declined Authorization Codes

The table below lists and defines common declined authorization codes. The processing system assigns these codes to transactions that the merchant declines at the point of sale. These codes display in the Access Online account profile function when you view account authorizations for declined transactions. If the transaction was not declined, the screen simply states that the transaction was approved.

In the text of the account authorizations, you may encounter the term *velocity*. The term *velocity* refers to the authorization limits set for cardholders and managing accounts in Access Online. You may also encounter the terms *corporate* and *individual*. In a decline reason, the term *corporate* refers to the managing account authorization limits and the term *individual* refers to the cardholder account authorization limits.

Reason	Code	Description
Account Coded (Credit Rating)	0031	The account used for the attempted transaction has a negative credit rating.
Account Coded M9	0016	The account used for the attempted transaction is a suspended account.
Account Coded V9	0015	The account used for the attempted transaction is a closed account.
ADS I Strategy	0851	The transaction falls within bank fraud parameters.
Arrest	0003	The account used for the transaction is a confirmed fraud account with a credit rating set to fraud.
Caution Account	0001	The account used for this transaction is flagged as a fraud/caution account.

Reason	Code	Description
Card Not Activated	0001	The cardholder has not yet activated the account used for the attempted transaction.
CRV Status	0134	The account used for the attempted transaction is not yet activated.
Card Expired	0007	The account used for the attempted transaction is an expired card.
Charge-off Account	0008	The account used for the attempted transaction is an account that has been charged-off.
Closed Account	0002	The account used for the attempted transaction is a closed account.
Exceeded Account Single Trans Limit	0805	The attempted transaction exceeds the account's single transaction limit.
MCCG Included, No Match	0823	The attempted transaction is with a merchant <i>not</i> in an authorized merchant category code group with a control set to approve only those included merchants.
Exceeded MCCG STDL	0808	The attempted transaction exceeded the single transaction limit for the merchant category code group associated to the account.
Exceeded Account Velocity Amount	0813	The attempted transaction exceeds a velocity limit set for the account.
Exceeded Account MCCG Velocity Amount	0818	The attempted transaction exceeds a velocity limit for the merchant category code group associated to the account.
Exceeded Number of ATM Per Day	0113	The account used for the attempted transaction has exceeded the allowed number of automated teller machine (ATM) transactions for that day. This authorization check applies to corporate cards used for travel.
Exceeds ATM Daily Limit	0112	The account used for the attempted transaction has exceeded the allowed daily dollar value of ATM withdrawals. This authorization check applies to corporate cards used for travel.
Exceeds Down-Time Processing Limit	0117	The processing system was down and the attempted transaction could not be processed.
Invalid Card Verification Value/Check	0125	The card verification value the user gave for the attempted transaction did not match the card verification value on file for the account.
Invalid Card/Account	0103	The card and/or account used for the transaction is not a valid card and/or account.
Invalid PIN	0111	The personal identification number the user entered is not valid. This authorization check applies to corporate cards used for travel purposes.
Invalid Plastic Used	0831	The account used for the attempted transaction does not have a plastic card issued, but the authorization request indicates that a card was swiped.
Lost Card – Pending Transfer	0006	The account used for the attempted transaction is a reported lost or stolen card with a balance that has not yet been transferred to a new card.

MCCG Exclude	0803	The attempted transaction was with a merchant in a merchant category code group with a control set to exclude transactions.
MCCG Included, No Match	0823	The attempted transaction is with a merchant <i>not</i> in an authorized merchant category code group with a control set to approve only those included merchants.
Reason	Code	Description
Not Enough Available Money	0048	The attempted transaction would send the account over the account's available credit limit.
# of Monthly Transactions Exceeded	0092	The attempted transaction would have exceeded the account's allowed number of monthly transactions.
# of Daily Transaction Exceeded	0093	The attempted transaction would have exceeded the account's allowed number of daily transactions.
Obtain Positive ID	0038	The account used for this transaction has a fraud credit rating because of suspicious activity or potential fraud on the account.
MCCG Included, No Match	0823	The attempted transaction is with a merchant <i>not</i> in an authorized merchant category code group with a control set to approve only those included merchants.
Not Enough Available Money	0048	The attempted transaction would send the account over the account's available credit limit.
Nmbr Monthly Transactions Exceeded	0092	The attempted transaction would have exceeded the account's allowed number of monthly transactions.
Nmbr Daily Transaction Exceeded	0093	The attempted transaction would have exceeded the account's allowed number of daily transactions.
Obtain Positive ID	0038	The account used for this transaction has a fraud credit rating because of suspicious activity or potential fraud on the account.
Over Limit	0084	The account used for the attempted transaction is already over its allotted limit.
Pick-Up – Fraud Code F1	0004	The account used for the attempted transaction has an F1 fraud status due to the plastic card being flagged as lost, stolen or never received by the cardholder. This decline reason may also display for an account with a F1 fraud status due to fraudulent activity on the account despite the cardholder possessing the card.
Single Purchase Limit Exceeded	0091	The attempted transaction exceeds the account's single purchase limit.
Transferred Account	0005	The account used for the attempted transaction has been reported as lost or stolen, and the balance transferred to a new account, but the attempted transaction used the old account.
Vendor Excluded	0800	The merchant for the attempted transaction is excluded from the organization's preferred vendor list.
Over Limit	0084	The account used for the attempted transaction is already over its allotted limit.

Pick-Up – Fraud Code F1	0004	The account used for the attempted transaction has an F1 fraud status due to the plastic card being flagged as lost, stolen or never received by the cardholder. This decline reason may also display for an account with a F1 fraud status due to fraudulent activity on the account despite the cardholder possessing the card.
Single Purchase Limit Exceeded	0091	The attempted transaction exceeds the account's single purchase limit.
Transferred Account	0005	The account used for the attempted transaction has been reported as lost or stolen, and the balance transferred to a new account, but the attempted transaction used the old account.
Vendor Excluded	0800	The merchant for the attempted transaction is excluded from the organization's preferred vendor list.

Card Maintenance

Non-Receipt of Card

If a cardholder has not received their U.S. Bank Corporate Card within 15 days of issuance, the cardholder should contact U.S. Bank Customer Service at 800.344.5696.

Upon notification, U.S. Bank Customer Service will take the following steps:

- Verify the billing address.
- Confirm that the card has not been returned to U.S. Bank.
- If the card has not been returned, Customer Service will then determine if the card was lost or stolen.
- Customer Service will close the account.
- The account information is transferred to a new account number.
- Arrangements are made for a replacement card to be sent to the Cardholder.

Lost or Stolen Cards

U.S. Bank Customer Service will use the same process mentioned above. If there are fraudulent charges on the account, Customer Service will assist the cardholder in identifying those charges and provide support to complete the proper dispute or fraud process.

Damaged Cards

If a card becomes damaged, the cardholder should contact Customer Service at 800.344.5696 and request a replacement card.

Card Expiration

U.S. Bank Cards are valid for a 4-year period from the month of issuance and expire on the last day of the expiration month. The expiration date is embossed on the card using a month/year format (e.g.; mm/yy). A renewal card will be sent approximately one month prior to your card's expiration date and must be activated by calling 800.344.5696.

Renewal cards will not be issued on accounts with the following status:

- 22+ months of no activity.
- Account that is three or more billing cycles past due.
- Account which has been suspended or closed.

Please note although the expiration date is set for a 4- year period, accounts with 22 consecutive months of non-use will be considered inactive, closed, and purged from the U.S. Bank system.

If a cardholder is preparing to use their card after a long period of non-use, please check with U.S. Bank at 800.344.5696 to confirm the card is active.

Card Reissuance for Expiring Cards

- Automation is in place to pull cards during the first week of the month prior expiration (e.g.; cards set to expire at the end of February are pulled for reissuance in early January).
- Once the reissue file is created and sent for processing, expiration dates on the accounts will be updated in the system to include the new expiration date. This does not impact the validity of the existing card until the new card is received and activated.
- U.S. Bank will ship all reissued cards no later than the last business day of the month prior to expiration and upon shipment, cardholders will receive cards within 7-10 business days. When the new card is activated, the existing card will automatically deactivate.
- Cards that are 60 days past due or in M9, V9, or T9 fraud referral status will not be automatically reissued. Additionally, cards that have had no activity in 22 months or more will not be automatically renewed, however the cardholder can call customer service and request a new card.

Self-Select PIN

During card activation a cardholder can select a PIN of their choice through the automated phone system.

NOTE: Cash access up to the available cash amount may also be obtained at a bank without a PIN.

Cardholder Access Online Log-in

Cardholders should sign up for an ID to access their statement and transaction information using U.S. Bank Access Online.

Access Online: access.usbank.com

Org Short Name = **See page 5**

Go directly to *Self- Registration*

Through Access Online, cardholders can:

- View General Account Information/ Balances/ Payment Address
- View Current and Historical Statements Online
- Maintain their address/phone number on account (if your organization allows them to maintain their address)
- View & Dispute Transactions
- Run Transactional Reports
- View Foreign Transactions/US dollar amount on posted Items
- Set up text and email fraud alerts

Through the Access Online Mobile App, cardholders can:

- Request and receive virtual accounts on their mobile device for online or phone payments
- Use the convenient ePay service to pay for expenses
- View account status, balance, payment due date, available credit balance and credit limit
- Search, filter and store the 99 most recent transactions
- Take photos of receipts and attach receipts in Transaction Management (if Transaction Management is enabled for your organization)

Please note that cardholders will still require their Organization Short Name, User ID and password to log into the mobile app. For assistance related to the mobile app, please contact our Access Online Help Desk at 877.887.9260.

By Calling U.S. Bank Customer Service at 800.344.5696 cardholders can:

- Change their PIN
- Report Lost/ Stolen /Non-Received/ Damaged/ Expired Cards
- Initiate Payment and Transaction Disputes
- Request Name/ Address Changes

Cardholder Account Changes

For changes not performed in the card management portal, all account changes must be routed to Client Services via email. Requests must be in writing for the following:

- Address Changes
- Limit Adjustments
- Transferring an Account
- Closure & Reinstatement Requests

Disputes

A transaction in Dispute status is a charge questioned for validity, which has posted to a cardholder's account. Disputes are governed by the card association operating regulations which provide instructions for action and timeliness by type of dispute.

To preserve their billing rights, cardholders must notify U.S. Bank Corporate Payment Systems within 60 days from the date of the first statement on which the item was billed. This can be done by calling our 24-hour customer service number (800.344.5696), or by initiating the dispute under Transaction Management in Access Online or in the Access Online Mobile App. It is recommended the cardholder first contact the merchant to attempt to resolve the issue prior to initiating a formal dispute. The cardholder should provide, in writing, full details of merchant contact including date of contact, method of contact (phone, email, etc.), name of merchant representative and the merchant's response to request. Upon entering a charge in dispute, either the Customer Service Representative or the Access Online form will instruct the cardholder on required documentation for the dispute type.

Additional documentation may need to be provided by the cardholder for certain types of disputes, such as an airline credit or hotel cancellation.

Types of Cardholder Billing Disputes

Photo Only Request

A cardholder may also make a Photo Only or Receipt Copy request. A Photo Only request assumes a charge is valid and will not place the item in dispute. A Photo Only request does not automatically guarantee suspension of the charge. If the statement which contains the transaction becomes 60 days past due, the cardholder will be unable to dispute the charge. A request for Photo Only can be initiated by contacting Customer Service or within the Transaction Management section of Access Online.

Payment Disputes

When reconciling a statement and an anticipated payment has not posted to an account:

- Contact the financial institution from which the check was drawn to verify the funds have cleared.
- If the funds have cleared, request a front and back copy of the canceled check and mail or fax to U.S. Bank Customer Service with a letter of explanation.
- Contact U.S. Bank Customer Service at:

Phone: 800.344.5696
Fax: 701.461.3464
Address: U.S. Bank Service Center
PO Box 6343
Fargo, ND 58125-6343



Transactions and payments can be monitored daily through Access Online Transaction Management. (access.usbank.com)

Credit Transactions

Credit Transactions are not put into dispute status while being researched.

Dispute Type	Explanation
Altered Amount	Transaction amount posted is greater or less than the original purchase amount: Cardholder needs to provide copy of sales slip.
Canceled Hotel Reservation	Travel Agency, company, or cardholder canceled guaranteed hotel reservation; To credit the account, date and time of cancellation and cancellation number are required.
Canceled Recurring Transaction	Charges that are billed to an account on a monthly, annual or periodic basis after the service has been canceled (typically subscriptions, membership fees, service agreements); a copy of the cardholder's letter to the merchant is required.
Paid by Other Means	Transaction was paid by check or other credit card; cardholder must provide proof of other payment.
Returned Merchandise	Cardholder waiting for credit from merchant; cardholder must provide proof of return.
Trans Billed to Wrong Account	This is a service to the customer and requires signed transfer authorization form by the cardholder receiving the debit.
Unused/Lost Airline Ticket	Cardholder waiting for credit; cardholder must return original ticket to the travel agency for credit for unused ticket; a Lost Ticket Application must be completed by the travel agency or the airline if the ticket is lost.
Duplicate Posting	Two or more transactions for similar amount and/or same goods posted to the account more than once; cardholder needs to identify which transaction is correct by giving the reference number of valid transaction.
Unrecognized Charges	Cardholder does not recognize transaction; cardholder provides note with signature stating transaction is not recognized. Some merchants such as airlines, hotels, and car rental agencies frequently process additional/delayed charges related to the original purchase transaction; common hotel charges include room service, laundry, and other services related to the hotel stay; airlines may charge prepaid, upgrade, or lost ticket fees; car rental agencies may add fuel, drop-off fees, and/or car phone charges.

Central Travel System Account Disputes

A Central Travel System account number is issued to provide the company's designated travel agency a direct account to post and bill business travel expenses. No plastic is typically issued. The primary transaction type is airline; however, some relationships include processing of lodging and car rental transactions through the Central Travel System Account.

The Travel Agency is responsible for processing transactions billed to the account. Disputes on Central Travel System accounts are generally identified by either the travel agency during reconciliation by the travel agency or the company.

Central Travel System dispute information must be obtained from the travel agency or your company. Please complete the CTS Dispute form completely and submit to:

Via Mail

U.S. Bank Card Services
Attn: Central Travel System Research Dept
MC: Fargo 0200
PO Box 6344
Fargo, ND 58125-6344

Via Fax

Attn: Central Travel System Research Department
701.461.3463

Dispute Resolution – Credit, Charge Backs or Rebills

The following chart illustrates the result of dispute resolution - Credit, Charge Back, or Rebill:

Type of Resolution	Resolution Specifics
Account is Credited	Charge is proven as invalid Amount is credited to the cardholder account and charged back to the merchant bank Cardholder is notified by letter of account credit
Charge is Proven to be Legitimate	Charge is valid Charge is removed from dispute (added back into Payment Due Amount on the next billing; no line item will appear) Cardholder is notified by letter of responsibility to pay the charge
Rebill	Merchant bank returns charge to U.S. Bank; U.S. Bank puts charge back on account (rebill) Example of Rebill: • Merchant also issued credit • Sales Slip was signed and/or imprinted • Cardholder only wanted a copy • No Visa Charge Back Rights

Fraud Prevention & Best Practices

Credit card fraud has increased dramatically in recent years and is becoming more complex as criminals are becoming more sophisticated.

Common Fraud Types

Type of Fraud	Description
Application Fraud	Application completed with false information
Non-Receipt of Issue	Replacement Card stolen out of mail
Account Takeover	Crook assumes identity of accountholder & is falsely using the card
Counterfeit	A duplicate copy of the plastic has been produced
Lost/Stolen	Cardholder lost card or Card was stolen
Remote Order (MOTO)	Account Number was used via mail, telephone or internet without authorization from cardholder. No card present at the time of the transaction
Type of Fraud	Description
Program Administrator Fraud	Card Administrator has used their access to credit card data and company funds to make payments to their account or other accounts
Phishing	Fake/Fraudulent e-mails and websites designed to fool recipients into divulging personal financial by hijacking the trusted brands of well-known banks, online retailers and credit card companies

U.S. Bank employs dedicated teams of fraud analysts who constantly monitor fraud and misuse trends. These analysts create fraud rules for the point of sale or monitor a transaction after it has occurred. Rules at the point of sale may be set to decline or refer based on the fraud risk of the transaction.

The monitoring rules may flag an account for review after the transaction has been approved, declined or referred at the point of sale, and generally includes the following:

- Review account opening and Maintenance Policies.
- Monitor Limit Changes and MCC Restrictions. Analyze new fraud trends.
- Pattern Detection Software will score transactions based on the following criteria and will place a temporary hold on accounts scoring high in these areas:
 - **Geography:** If transaction is made in high-risk area.
 - **Merchant:** Is the merchant in a high risk MCC category?
 - **Dollar Amount:** How high is the dollar amount of the transaction?
 - **Velocity:** The number of transactions being made.
 - **Fraud History:** Is there a history of fraud at this merchant?
 - **Individual History:** Does this cardholder have a history of fraud?

When fraud is suspected and the account is flagged for review, the team will attempt to call the cardholder via the phone numbers listed on the account to confirm the validity of the transaction(s) and a temporary block status may be applied to the account to prohibit further charging activity.

Fraud Alerts

U.S. Bank offers text and email fraud alerts, which cardholders can enable via Access Online. If a cardholder is enrolled for this service, they will receive an email or text if a fraud alert has been placed on the account. The cardholder can respond via text to confirm if the transaction is fraudulent or legitimate. Once contact is made and validity of the transaction is confirmed, the block is removed. If the cardholder has not contacted U.S. Bank before the end of the business day, the account will appear on a report that Client Services receives the following day. Client Services will send an email to the Program Administrator to advise that the account needs to have activity confirmed by the cardholder.

What Cardholders Can Do to Prevent Credit Card Fraud

- Promptly review account statements and transaction activity via Access Online and report any discrepancies to the card issuing bank immediately
- Secure statements and receipts and destroy any that are unnecessary
- Be mindful of your card
- Do not disclose your PIN number or share the card
- Do not provide credit card or personal information over the phone or via e-mail unless you initiated the call or e-mail
- Report suspicious e-mails to our fraud prevention e-mail address: fraud_help@usbank.com or you can contact U.S. Bank Fraud directly at 800.260.8469
- Register for fraud alerts

What Program Administrators Can Do to Prevent Credit Card Fraud

- Be mindful of how you store and destroy card information
- Keep cardholder records up to date ensuring that the contact numbers are valid numbers. In case of any suspected fraud, those are the phone numbers that our team will attempt to use
- Ensure your termination process includes destroying the card and closing the account
- Report suspicious e-mails to our fraud prevention e-mail address: fraud_help@usbank.com OR directly at 800.260.8469
- Notify your Relationship/Account Manager or Account Coordinator of major spending changes (international travel, upcoming purchases outside of your normal spend pattern, etc.)
- Restrict program administrator access so individuals are unable to approve payments or credit balance refunds to their own accounts and periodically review program administrator processes and card spend to ensure the program is being run within company guidelines

U.S. Bank Secure Mail

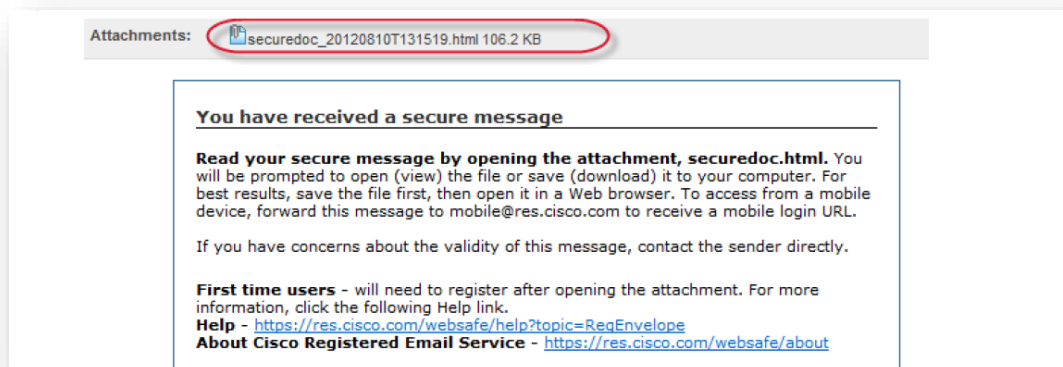
U.S. Bank has implemented a tool called Secure Mail, which provides U.S. Bank customers and vendors a secure way to get confidential information from U.S. Bank via internet email. Any U.S. Bank employee can initiate an email to a vendor or customer with an internet email address. Recipients access a secure website within the bank to retrieve the confidential information.

Receiving a Secure Mail Message

When a U.S. Bank employee sends you an encrypted email message, you will not get the message directly into your mailbox. You will receive a notification that an encrypted email has been sent to you, who it was from, the subject, and a link to follow to retrieve the message.

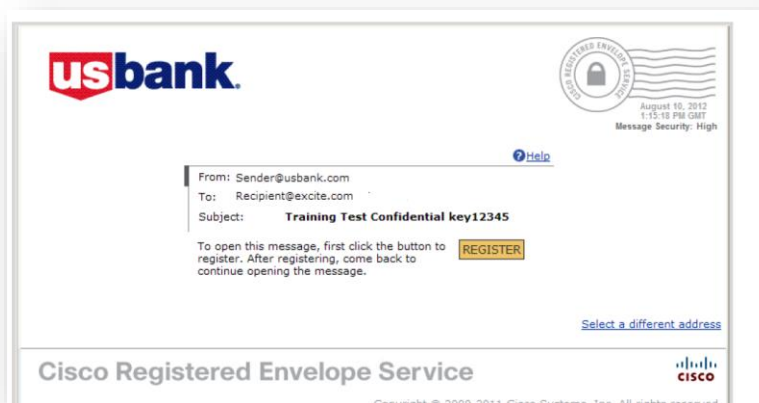
Step 1: Save the Encrypted Message File Attachment to Your Hard Drive

When you receive a Registered Envelope notification message, you need to open the file attachment to view the Registered Envelope. For best results, double-click the **file attachment** (**securedoc_date_time.html** where *date* and *time* represent the time stamp appended at the time the mail was sent) and save it to your hard drive before opening it, as shown below.



Step 2: Open the Attached File in a Web Browser

Open the attached file (**secure_date_time.html** where *date* and *time* represent the time stamp appended at the time the mail was sent) in a web browser, such as Microsoft Internet Explorer or Mozilla Firefox. The registered envelope is displayed.



Step 3: Click the Register Button to Enroll with the Service

Click the **Register** button on the Registered Envelope to enroll with Cisco Registered Envelope Service. The New User Registration page displays.

NOTE: Your company may have configured single-sign-on (SAML) authentication for you to use with the Cisco Registered Envelope Service. In this case, the new user registration is a shortened registration and only requests that you enter the portal Language, First Name and Last Name. Personal security phrases are not required for SAML authentication. Please contact your company's support group to see if SAML is available to you.

Figure 1-3 New User Registration with SAML Authentication

NEW USER REGISTRATION

To ensure future messages from this service are not accidentally filtered out of your email, please add "DoNotReply@cisco.com" to your Address Book or Safe Sender List. * = required field

Enter Personal Information:

Email Address: newuser@cisco.com

Language: English The language setting will be saved for future login and email notifications.

First Name*

Last Name*

Register

Cisco Registered Envelope Service

About Terms of Service Privacy Policy Copyright © 2009-2013 Cisco Systems, Inc. All rights reserved.

New User Registration Form with SAML Authentication

Complete the online registration form and click **REGISTER**.

FINAL STEP: ACCOUNT ACTIVATION

Your Cisco Registered Envelope Service account was successfully created.

Instructions to activate your account have been emailed to Recipient@excite.com

Please check your inbox. If you do not see an account activation email, check your junk email folder.

Step 4: Activate Your Cisco Registered Envelope Service Account

Check your email for an activation message from the service. The headline in your email will look similar to this:

From:	CRES Do Not Reply <DoNotReply@res.cisco.com>
Subject:	Please activate with CRES

If the email is not in your inbox, check the spam or junk email folder in case the activation message was filtered.

Step 5: View the Registered Envelope Again and Enter Your Password

Return to the Registered Envelope. The Register button is replaced with an **Open** button. Enter the password for your Cisco Registered Envelope Service user account and click the **Open** button. Use this frequently asked questions document below to assist you with troubleshooting if problems persist. Support may be reached at 866.412.6113.

[Frequently Asked Questions](https://res.cisco.com/websafe/help?topic=FAQ)
res.cisco.com/websafe/help?topic=FAQ

Replying to or Composing New Secure Mail Messages

You will only be able to send messages to registered users of Secure Mail. Click the **Reply** button to reply back to the sender of the message. To compose a new message, click the **New Message** button in the left-hand navigator. After sending your message, your Secure Mail sent view is displayed.

U.S. Bank Monthly Credit Card Auto-Purge Process

U.S. Bank will purge inactive credit card accounts for security purposes.

U.S. Bank purges accounts monthly on the **2nd Sunday** of the month. Accounts are flagged to purge with a DEL status when they meet the following criteria, they will be deleted/purged from the system the following month on the 2nd Sunday if the delete status has not been removed.

Open Accounts	Closed Accounts
\$0 Balance	\$0 Balance
No Credit Rating	Closed Credit Rating of P9, V9, T9, Q9
Account has expired	Inactive for at least 12 months
Inactive for at least 22 months	Closed Credit Ratings of S1, R9, F1 or FA need to be inactive for 22 months

U.S. Bank can provide Program Administrators with a Pre-Purge Report, which identifies accounts that were flagged to be purged. Program Administrators that wish to receive this report should notify their Account Coordinator to schedule. The report is available monthly on a requested basis and will be delivered via Access Online Data Exchange.

Program Administrators that wish to keep an account on the system must notify their Account Coordinator in writing. The request must contain the following information:

Cardholder Name	Truncated Acct #	Address Verified?	Order new Card?	Card Delivery Information?
Joe Cardholder	XXXXXX4000000000	New Address: 123 Any St Anytown, US 12345	Yes, Regular Mail	Send Card Regular mail to Systems Address
Sue Cardholder	XXXXXX4000000000	Current	Yes	Send card to me, regular mail.

Frequently Asked Questions

- **If I close an account that hasn't been used in 15 months, when will that account purge?**
The account will be flagged to be purged on the 2nd Sunday of the following month.
- **What if I forgot to respond to my Account Coordinator to keep accounts from purging?**
If it is before the 2nd Sunday of the month, we will do our best to keep the account from purging. Any requests received after the 3rd Sunday cannot be processed.
- **Is there a way to get an account back after it's been purged?**
Once an account is purged, the account information cannot be retrieved. A new application is required.
- **Now that accounts have a four-year expiration date, will this cause an inactive account to stay on the system longer?**
Yes, if the Program Administrator has not closed an inactive account, it could be on the system longer.
- **Will an account purge if it has been inactive for 22 months and is then used by the cardholder within the 22nd month of inactivity?**
 - If an account is attempted to be used after the account is flagged for purge, the transaction will be declined.
 - If a transaction is approved within 3 days of the 2nd Sunday and the transaction has not posted by the 2nd Sunday, the account will be flagged to purge and when the transaction attempts to post, it will have to be manually applied once the account has the delete status removed.
- **What type of activity on an account would keep the account active?**
Activities are monetary transactions posting to the system. An authorization at the merchant is not considered activity until that transaction posts to the system.

Credit Rating Codes

Credit Rating Codes appear on reports and identify cardholder account status.

Code	Reason	Account Results
F1	Lost/Stolen	Declines All Authorizations Declines Reissue Places Pick-Up Status on Card
FA	Fraud	Declines All Authorizations Declines Reissue Places Pick-Up Status on Card
M9	Suspension	Assigned when an account reaches 60 days past due Declines all Authorizations Declines Reissue Status automatically removed when past due balance has been paid

S1	Cancellation	Assigned when an account reaches 90 days past due Declines all authorizations Declines Reissue Full payment <u>will not</u> automatically result in reinstatement Company must request in writing
T7	Investigation	Account under investigation/waiting for verification from program administrator
T8	Closed- OFAC	Account permanently closed due to confirmed hit on OFAC list
T9	Termination	Declines All Authorizations Declines Reissue Places Pick-Up status on card
V9	Voluntary Surrender	Declines All Authorizations Declines Reissue
R9	Revocation	Assigned when an account reaches 120 days past due Declines all authorizations Declines Reissue Places Pick-Up status on card
Q9	Closure	Declines all authorizations Declines Reissue
P9	Closure	Declines all authorizations Declines Reissue Places Pick-Up status on card

Delinquent Account Collection Flow Chart

Delinquency Status	U.S. Bank Action
1st Statement Generated	No action required by U.S. Bank.
2nd Statement Generated 30 days past due 45 days past due	Late fee assessed as outlined in contract. The first past-due notice will be generated and sent to cardholder and collections calls begin.
3rd Statement Generated 60 days past due 61 days past due	The past-due balance is assessed a late fee, if applicable and another notice is sent to the cardholder. The account is suspended (coded M9) from further charge authorization until the past-due amount has

been paid; account suspension will automatically be removed when payment in is received for the 60 day balance.

4th Statement Generated

90 days past due

The past-due balance is assessed a late fee and another past due notice is generated.

91 days past due

Card privileges are revoked (Coded S1); the account is closed; payment in full will not automatically re-open the account; Company Program Administrator may also be contacted at this time for Collection assistance.

5th Statement Generated

120 days past due

The past-due balance is assessed a late fee and the 120-day past due notice is generated.

121 days past due

The account is permanently closed (Coded R9); payment in full will not automatically re-open the account; collection calls and letters will continue; an attorney's letter may be sent to the cardholder.

6th Statement Generated

150 days past due

The past-due balance is assessed a late fee and the 150-day past due notice is generated.

7th Statement Generated

180 days past due

The past-due balance is assessed a late fee and the 180-day past due notice is generated.

The account will be charged off at the end of the calendar month.

Card Reinstatement Process & Procedures

Cardholders whose accounts have been closed because of delinquency may be eligible to have their accounts reopened, though this will be reviewed on a case-by-case basis.

Program Administrators can contact Client Services with reinstatement requests.

If an account is charged off as a bad debt, the balance must be paid in full and a new application is required. This includes any money previously paid by the Liability Waiver Insurance. Charged Off accounts can never be reinstated. If an account had not been previously reinstated and charges off, a new account can be opened as the cardholder's one-time reinstatement. The new account will have Travel Only limits and will not have cash.

In order to process a reinstatement, accounts must have a \$0 balance.

If you have any questions about an account reinstatement, contact your Client Services Team.

Cardholder Bankruptcy

If a cardholder has a contingent liability card and they have filed for bankruptcy, U.S. Bank will notify the Program Administrator and the cardholder will also receive a notification letter in the mail that the account will be closed.

The outstanding balance should be paid off in 60 days or less, otherwise the balance will charge off. Once the account is closed, Program Administrators may reapply for a new contingent liability card for the individual, using the normal card opening processes in the system.

Cardholder Benefits

U.S. Bank is committed to providing exceptional services and benefits to its cardholders. Four of these benefits include Customer Service, Travel Assistance, Insurance Coverage and Excess Lost or Damaged Luggage Coverage.

To answer any inquiries regarding cardholder benefits, please call the following numbers:

- U.S. Bank Customer Service 800.344.5696
- 701.461.2042 (*International Collect Calls Accepted*)

These numbers are also located on the back of the Corporate Card.

Our toll-free number is staffed 24 hours a day, 365 days a year and provides access to an Automated Response Unit designed for touch-tone response to basic cardholder inquiries. Cardholders always have the option of speaking directly to a U.S. Bank Customer Service Representative. To access a U.S. Bank Customer Service Representative immediately, press the asterisk (*) key twice.

By using the automated response unit, cardholders can:

- Activate their account
- Report a lost or stolen card
- Check current balance, credit line, last five transactions and payment information
- Set up and make a Tele-Payment on their account

Cardholder Verification

Our customer service representatives will go through a cardholder verification process to make sure that they are speaking with the cardholder. Below are a few data points that may be included in the verification process.

The cardholder should be able to correctly answer two of the questions below which would be reflected in their cardholder profile in our system:

- **Zip Code:** Zip code where the statement is mailed
- **Home or Business Phone:** Information included in cardholder profile
- **Employee ID:** If this field is populated in your program
- **Password**
- **Cycle Date:** When the statement is generated
- **Date of Birth**
- **Last Statement Balance:** On last statement
- **Amount of Last Payment:** Last payment made
- **Single Purchase Limit:** Need to ask Program Administrator
- **Cycle Limit:** Need to ask Program Administrator

Travel Assistance

[Visa Assistance Center 800.VISA.911 \(800.847.2911\)](#)

[International Collect 303.967.1096 \(Collect Calls Accepted\)](#)

[MasterCard Assistance Center 800.MC.ASSIST \(800.847.2911\)](#)

[International 636.722.7111 \(Collect Calls Accepted\)](#)

The list below outlines the type of assistance available through the Corporate Card program. Additional

details can be provided in the Guide to Card Benefits document which can be obtained from your Relationship/Account Manager or Account Coordinator team.

Medical Assistance Services

- Medical referral
- Medical transportation and evacuation
- Medical and hospital expense payment
- Prescriptions

Travel Assistance Services

- Business document delivery
- Urgent message service
- Emergency ticket replacement
- Guaranteed hotel/motel reservation service
- Pre-trip assistance
- Translation assistance

Emergency Services

- Card replacement
- Cash disbursement
- Medical referral assistance
- Transportation assistance
- Bail bond assistance

NOTE: The Assistance Center provides assistance and referral services only. Cardholders are responsible for the cost of any medical or legal services, transportation, cash advances, or other goods or services arrange.

Insurance Coverage

The U.S. Bank Corporate Card Program offers car rental insurance coverage assistance programs: Claims must be reported and/or filed via the guidelines below:

- **Visa:** 800.VISA.911 or visa.com/visaclaim
 - **Visa:** reported within 45 days, file a claim within 90 days and submit all documentation with 365 days from date of loss
- **MasterCard:** 800.MC.ASSIST
 - **Mastercard:** reported within 30 days and submit documentation within 180 days from date of loss
- Insurance applies to rental cars that are rented using a U.S. Bank Corporate Card
- Collision Damage Liability (CDL) protection should be declined at the rental agency
- The coverage applies to any repairs or loss of use charges that are assessed
- Rental period must not exceed 31 days
- This coverage does not apply to most trucks or luxury vehicles
- Coverage applies in most countries, please see the brochure for specifics

Automatic Worldwide Travel Accident Insurance

U.S. Bank Corporate Cardholders, Central Travel System account users, their spouses and children* who are traveling worldwide for business purposes are automatically insured against accidental bodily injuries that are the sole cause of death or dismemberment arising from an accident that occurs while riding in, boarding, or alighting from any aircraft on land or water conveyance that is a common carrier** licensed to carry passengers for the hire including regularly scheduled licensed common carrier charter flights, provided the entire travel fare(s) has been charged to the U.S. Bank Corporate Card account.

NOTE:

* Unmarried dependent children under age 19 (23 if a full-time student at an accredited college or university).

** Common Carrier does not include a conveyance operated for sport, recreation and/or sightseeing activities or for any aircraft or device for aerial navigation except as expressly provided in the policy.

To obtain a copy of the Designation/Change of Beneficiary form, please call Robinson International at 312.726.2575 or write to Robinson International Inc. 135 South LaSalle Street, Chicago, IL 60603

Filing a Travel Accident Insurance Claim

Claims for benefits must be filed within 90 days after the loss occurs.

1. Representative of deceased/injured cardholder contact:

Robinson International, Inc.
200 South LaSalle St
Suite 2060
Chicago, IL 60604

2. The insurance carrier will mail appropriate forms to the representative of the deceased/injured cardholder.
3. The representative of the deceased/injured cardholder completes the required form(s) and provides the insurance carrier with proof of loss (i.e., copy of death certificate or a physician's report), as well as proof the ticket was purchased with the U.S. Bank Corporate Card (i.e., copy of the monthly billing statement or copy of sales slip).
4. The insurance carrier will process the claim in a time frame consistent with the timeliness of receipt and completeness of claim information and complexity of the claim.

Excess Lost/Damaged Luggage Coverage

U.S. Bank will reimburse a cardholder if the common carrier's payment for lost or damaged luggage is less than the cardholder's claim. This is called Excess Lost/Damaged Luggage Coverage.

U.S. Bank provides Excess Lost/Damaged Luggage Coverage for both checked and carried-on articles when the cardholder's ticket is charged to a U.S. Bank Corporate Card or Central Travel System account. Consideration of reimbursement from U.S. Bank will be made only if the common carrier acknowledges the claim and makes a monetary reimbursement.

Cardholders are eligible to receive excess reimbursement for the cost of replacement luggage and its contents up to the lesser of:

1. The amount paid to the cardholder by the common carrier, or
2. \$1,250

Total combined payment will not exceed claim amount.

Excess Lost/Damaged Luggage Coverage Exclusions

This benefit does not cover:

- Animals
- Any other conveyances or appurtenances except bicycles
- Contact lenses, eyeglasses, hearing aids
- Artificial teeth, dental bridges
- Prosthetic limbs
- Money, securities, credit cards



- Tickets, documents
- Cameras
- Sporting equipment
- Business items
- Art objects
- Electronic equipment
- Luggage held, seized, quarantined, or destroyed by customs or a government agency

Filing an Excess Lost/Damaged Luggage Claim

Please email Client Services to file a claim.

Provide a copy of the common carrier's claim form, a list of items lost with the corresponding value and copies of the checks issued by the common carrier.

Provide a copy of the cardholder's charge slips as proof that the common carrier ticket(s) were charged and paid for on a U.S. Bank Corporate or Central Travel System account.

Liability Waiver Insurance

The Liability Waiver Program was created to protect U.S. Bank clients from losses associated with cardholder misuse. This program waives certain charges when an employee misuses their Corporate or Purchasing Card privileges.

Under this program your company is insured for any waive-able charges made by a terminated employee, or on an account that is currently cancelled for delinquency or other reasons. An Insurance Claim cannot be filed until the account is closed.

Non-terminated employees whose accounts are 120 days delinquent will be closed and a claim may be filed at that time. Claims for terminated employees may be filed as soon as six weeks after the account is closed. The account must be at least 60 days past due for claim eligibility and a claim must be filed within 90 days of the termination date.

Insurance Documentation

U.S. Bank will automatically send to Program Administrator(s) the documentation required to process a claim for all eligible accounts.

This documentation includes the following:

- **The Employee Account Cancellation Notification** – Your company is required to send a letter to the terminated/cancelled cardholder to protect the company from unauthorized charges.
- **Affidavit of Waiver Claim Form** – This document is used to confirm the claim amount.
- To expedite the filing process, U.S. Bank will prefill the form with available data. Your company must complete and return this form to U.S. Bank. U.S. Bank will also attach a copy of the waive-able charges.

The Importance of Filing Every Potential Claim

Every recovery received from the Visa Liability Program is credited to your company's employee cardholder credit loss rebate. Recoveries received after charge-offs are credited back to the rebate at 100% upon receipt of payment.

Financial Extracts, File Delivery and Data Feeds

Access Online allows your organization to extract the data you need in the most efficient, convenient format, providing a wide variety of financial extract options to meet your specific integration requirements.

General ledger extracts

General ledger extracts directly integrate with your general ledger system and you can control where transactions are allocated, how extracts are structured and when data is delivered. General ledger extracts can be sent daily and/or at cycle.

Files and financial extracts can be encrypted using PGP, and transmission methods include HTTPS, FTP, SFTP or Direct Connect. Additionally, U.S. Bank offers secure mailboxes via Access Online Data Exchange. U.S. Bank offers two primary output file types in the United States including Statement Billing Files (SBF) and the standard commercial card file which contains transaction information, account, hierarchy, level II and level III data for both corporate and purchasing card programs. This file type also supports the inclusion of allocation data from Access Online. Files can be transmitted on a daily or cycle (monthly) basis.

File Transmission

If your organization currently receives files and requires a file to be retransmitted, our Managed File Services team can assist with next steps. Please contact the Managed File Services (MFS) team at 800.765.9549, option 1 and please provide the file name or mailbox ID.

Third-Party Expense Management Feeds

If your organization is interested in setting up a feed for a third-party expense management system such as Concur, Chrome River or Certify, please contact your Relationship or Account Manager. They will provide documentation to initiate the process.