October 1, 2024

Credit Card Policy | For US Staff

POLICY OWNER:	Controller, Finance
POLICY APPROVED BY:	Chief Finance Officer, Finance
POLICY CONTACT:	travel_entertainment@water.org

Policy Contents

I. Policy Overview

Policy Statement

This policy establishes guidelines for the issuance, use, and management of company-issued credit cards. The purpose is to ensure appropriate use of company funds, maintain financial control, and comply with relevant regulations.

This Policy is guided by the organization's Global Standards of Business Conduct and Delegation of Authority. Further, this policy ensures the organization follows the Internal Revenue Code and applicable Treasury Regulations, as well as other external statutory and regulatory requirements.

Purpose

Issuance of Credit Cards

- The corporate credit card is meant to allow employees access to efficient, flexible, and alternative means of payment for approved expenses.
- Company credit cards may be issued to employees with frequent business-related expenses.
- The Finance Department is responsible for issuing credit cards, maintaining records of issued cards, and setting credit limits.

Authorized Use

- Company credit cards are to be used exclusively for business-related expenses (travel, lodging, meals, and other approved purchases).
- Staff should seek invoicing and purchasing terms from vendors. Use of credit cards for purchases is not preferred.
- Personal use is strictly prohibited.

Expense Reporting

- Cardholders must submit detailed expense reports monthly with original receipts for all applicable transactions.
- Expense reports must be reviewed and approved by the cardholder's manager and the Finance Department.
- Discrepancies or unauthorized transactions must be reported immediately to the Finance Department.

Compliance and Monitoring

- The Finance Department will regularly monitor credit card usage to ensure compliance with this policy.
- Cardholders must comply with all relevant company policies, including the "Global Standards of Business Conduct" and "Delegation of Authority" policies, as well as local laws regarding expense reporting and taxation.

Consequences of Misuse

- Misuse of a company credit card, including personal use or failure to provide adequate documentation, may result in disciplinary action.
- The company can recover any unauthorized expenses from the cardholder.

Card Security

- Cardholders are responsible for safeguarding their company credit card and immediately reporting any loss or theft to the Finance Department and credit card company.
- Card details must not be shared with unauthorized individuals.

Termination or Resignation

- Upon termination or resignation, the cardholder must return the company credit card to the Finance Department.
- Outstanding expenses must be reconciled prior to the cardholder's last day of employment.

Applicability

This policy applies to all Water.org US staff members who possess a Water.org-issue company credit card.

Governance

The **Finance Department** is the owner of this policy and is responsible for administering, reviewing, and making recommendations for updates or changes to this policy in alignment with business needs.

Violations

It is the expectation of Water.org that direct supervisors proactively manage their direct reports' compliance with this Policy. Non-compliance, from an employee or a direct supervisor, may result in progressive disciplinary actions consistent with the organization's established HR procedures.

II. Policy

1. Use + Financial Responsibility

- Corporate credit cards are authorized for business-related travel and purchases as defined in the Travel & Entertainment Policy and related policies.

- Cardholders and supervisors must adhere to this policy to minimize fraudulent or inappropriate use.
- Purchases must be within budget and properly approved.
- The corporate credit card is to be used only for official business expenditures, not personal expenses.
- Cardholders must provide itemized receipts for applicable transactions over $50, submitted with expense reports within 45 days.
- The organization will pay for the total balance by the due date for each company-approved charge by the cardholder.

2. Credit Limits

- The credit limit will be guided by the Delegation of Authority and adjusted based on business need, travel frequency, and budget.
- Cardholders will be notified of their credit limit and how to access their account information to monitor the monthly credit card balance and identify disputed and/or fraudulent charges.
- To request a temporary credit limit adjustment, cardholders should contact the Finance Department at least 24 hours before the increase is needed.
- Permanent credit limit adjustments are subject to review by Controller and require written justification from the cardholder's direct supervisor emailed to finance@water.org.

3. Ownership + Cancellation

- The corporate credit card may not be transferred, assigned to, or used by anyone other than the designated cardholder.
- The cardholder is accountable for all activity on the corporate credit card. The organization may suspend or cancel cards at any time.
- All credit card rewards, including cash back and points, earned through company expenses belong to the company. However, reward programs such as airline miles or hotel points may be assigned and claimed by individuals.

4. Disputed Items

- Cardholders are responsible for reviewing and resolving erroneous charges, returns, or adjustments to ensure proper credit is given on subsequent statements. Disputed transactions must be resolved with the bank and the merchant. The cardholder must immediately notify the bank for resolution and inform the Finance Department as well. See Appendix A | Fraud + Disputed Transaction Procedures.

5. Lost or Stolen Card

- Lost or stolen cards must be reported immediately to the bank and the Finance Department. See Appendix A – Fraud + Disputed Transaction Procedures.

6. Safekeeping

- Newly issued cards should be signed immediately upon receipt. Card numbers should not be saved or stored in online accounts. Expired cards should be cut in half and discarded. The cardholder should make certain that the card is returned to them after each charge and verify the name on the back of the card.
- Cardholders should beware of imposter notifications and verify the authenticity of communication, contact information and procedures by the bank before responding to email and/or text-based notifications. See Appendix B – Safekeeping Best Practices. email and/or text-based notifications. See Appendix B – Bank of America Safekeeping Best Practices

7. Cash Advances

- Cash advances on company credit cards are strictly prohibited unless prior approval is obtained from the Chief Financial Officer (CFO).

III. Approval and Responsibility

Employee Responsibilities

- Employees should not use the credit card for any purchases without being authorized by their supervisor.
- The corporate credit card is to be used only for official business expenditures, not personal expenses.
- Cardholders must provide itemized receipts for applicable transactions over $50, submitted with expense reports within 45 days.

Direct Supervisor Responsibilities

It is the expectation of Water.org that direct supervisors proactively manage their direct reports' compliance with this Policy.

IV. Additional Resources

Contact for Support

Please contact travel_entertainment@water.org or the Controller with any questions.

Related Policies

Global Standards of Business Conduct

Delegation of Authority

V. Appendices

Appendix A | Bank of America Fraud + Disputed Transaction Procedures

III. Appendices

Appendix A| Bank of America Fraud + Disputed Transaction Procedures

BANK OF AMERICA

Dealing with fraudulent and disputed transactions

What is a fraudulent transaction?

- It is a charge made to a credit card account that has not been authorized by the cardholder.
- The cardholder will not be liable for transactions deemed to be fraudulent as long as they have been reported within the stipulated time period.

Reporting a fraudulent transaction

- Contact Bank of America, using the number provided on the back of your card, to report any fraudulent activity as soon as it is discovered – no later than 60 days from the date of the statement reflecting the transaction(s).
- Additionally, Bank of America's fraud monitoring team assists in detecting fraud and out-of-pattern spending. As a result, suspicious activity may result in a Fraud Alert email or outbound call to a cardholder.

What now?

- Once you have contacted Bank of America, we will open a fraud claim for investigation. We will also close your existing card to prevent any additional fraudulent transactions from occurring and will issue you a new card immediately.
- We will provide you with a temporary credit for the fraudulent amount, which can take 1-2 billing cycles to appear on your account. We strive to resolve your fraud claim within 90 days and once a final decision is taken, you will receive a letter informing you of what action has been taken.

Contact Bank of America

Contact Bank of America immediately to report any fraudulent activity using the number provided on the back of your card. You may also reference the Global Cardholder Contact List.

U.S. All cardholders:	888 449 2273
	602 379 8753 (collect)
Fraud Claim Status:	800 714 5923
Disputes (non-fraud):	855 521 1795

Cardholder servicing is available 24 hours from Monday-Friday. Limited support such as lost/stolen card and cardholder emergencies are provided on the weekends.

What is a disputed transaction?

- It is a charge from a merchant that you have previously transacted with, but the merchant may have charged you an inaccurate amount/an additional charge without your permission, or you feel that the services or merchandise received is not what you paid for.
- Always contact the merchant first to attempt to resolve. If it is not resolved with the merchant, please contact Bank of America to raise a dispute case using the number provided on the back of your card – and in no event greater than 60 days from the statement reflecting the transaction(s).

Handling a disputed transaction

- Always contact the merchant first to attempt to resolve.
- Ask the merchant to issue a credit or refund for the transaction(s) in question.
- Ask for confirmation and/or cancellation numbers for your reference, if any.
- Ask about the time it will take to receive the refund.
- Keep any emails to and from the merchant.

If you've contacted the business that processed the transaction in question and you still have a concern, contact Bank of America's cardholder servicing team using the number on the back of your card for assistance. Our team will gather any necessary information and open a dispute case.

You can expect to hear back from our Disputed Transaction Services (DTS) team within five working days. We may require more information from you or the merchant before we proceed with the case. You will receive an email to confirm what action has been taken once the case is resolved.

When should you dispute a transaction?

- Cancelled subscription payments but you were still charged.
- Haven't received goods/services.
- Duplicated transaction.
- Transaction amount differs from invoice/receipt amount.
- Defective merchandise.
- Once a dispute is raised, Bank of America will freeze the disputed amount on your card, and the amount will not be required for payment until you receive a final decision.

Appendix B| Bank of America Safekeeping Best Practices

BANK OF AMERICA

How to avoid imposter scams

As our daily reliance on digital communication steadily increases, scammers are evolving their tactics to exploit the trust we've built for online and other financial services. Imposter scams are on the rise and are currently the most commonly reported fraud, with approximately 985,000 complaints in 2021 according to the Federal Trade Commission.

Imposter scams typically begin with an anomalous email (commonly known as phishing), a phone call from a falsified number (vishing), an unsolicited text (smishing) or a social media message. The communications appear to be from trusted professionals such as bank representatives, lawyers or government officials. To make them appear more authentic, the perpetrators may even pose as your current relationship manager, or representatives of companies you already have relationships with.

By creating fraudulent websites using legitimate information they've harvested from online sources, these scammers lure clients and potential prospects into providing confidential information with the intention of committing financial fraud.

Best Practices

Imposter scams are successful because of how much legitimate information scammers can mine from publicly available information on the web, enabling them to convincingly impersonate a professional or simulate a professional's website. But by following these best practices, you can protect yourself and others:

- Verify all anomalous communications or requests for payments or personal information by double-checking the sender information and by independently confirming the source using a verified phone number from an official website, bill or statement.
- Don't rely on caller ID to determine if a caller is legitimate.
- Never send payments to anyone without independently verifying their identity.
- Never give sensitive information, such as account numbers, over the phone or through a website unless you are sure of who you're interacting with.
- Cut off contact at any point with someone you suspect is impersonating a professional.

In addition, being proactive and coming up with a mutually understood defense against imposter scams with your professional contacts can be an effective way to decrease your chances of falling victim.

If you receive any suspicious email or text message that appears to be from Bank of America, forward it to us at abuse@bankofamerica.com.

Remember: Don't transfer money or make payments as a result of an unexpected phone call or text. Bank of America will never ask you to share your banking credentials or one time passcode or ask you to send account or company information over text, over email or online.