Staying Safe from Impersonation Attempts
At Gordon Food Service, we are committed to protecting our customers, employees, and partners from fraud and scams. Criminals may attempt to impersonate Gordon Food Service or other trusted organizations to gain access to your sensitive information or financial resources. This page provides information to help you identify and report suspicious communications.

Understanding the Risks
Scammers use a variety of tactics to trick individuals into providing personal information, making payments, or granting access to their systems. These attempts can take many forms, but they often share a common goal: to deceive you into taking an action that benefits the scammer.

Impersonators may try to create a sense of urgency or fear, pressuring you to act quickly without thinking. They may also try to build trust by pretending to be a legitimate representative of Gordon Food Service or another organization you recognize. They can seem trustworthy, professional, and legitimate.

Identifying Suspicious Communications
Not all communications appearing to come from Gordon Food Service, even if they have our logo or phone number on them, are legitimate. Here's what to look out for:

- **Unexpected Requests:** Be wary of unsolicited communications asking for personal information (like passwords, bank details, social security numbers), financial transactions, or access to your computer/systems. Legitimate organizations, including Gordon Food Service, will never request sensitive information through email or unsolicited phone calls.
- **Sense of Urgency:** Scammers often try to pressure you into acting immediately, claiming an urgent problem or a limited-time offer. Take your time and don't be rushed into making a decision.
- **Unusual/Unexpected Communication Methods:** Be cautious if you receive a request through an unusual or unexpected channel. For example, if you normally communicate with Gordon Food Service through a specific portal or email address, be suspicious of a request coming from a different source.
- **Poor Grammar and Spelling:** While not always a definitive sign, many scam communications contain noticeable errors in grammar and spelling. It is worth noting that as AI technologies advance, poor grammar and spelling will be less of a “tell-tale” sign, but can still be something to keep an eye on.
- **Inconsistencies:** Look for inconsistencies in the communication. Does the email address or phone number match official Gordon Food Service contact information? Is the tone or style of the communication different from what you expect?

- **Requests for Payment:** Look for requests for payment in unusual forms, for example, a gift card or bitcoin.
- **Too Good to be True:** If an offer appears too good to be true, it is probably a scam.

What to do if You Suspect a Scam

- **Don't Respond**: Do not reply to the suspicious communication or click on any links. Avoid providing any information, especially personal or financial information.
- **Don't Engage**: Do not engage with the requester. If you get a request that seems suspicious, contact the person or company through confirmed communication methods, such as a number on the official website.
- **Verify the Communication**: If you are unsure whether a communication is legitimate, contact Gordon Food Service directly through a known, trusted channel. *Do not use the contact information provided in the potentially suspicious communication.* If you would like to verify if a communication you received is legitimate, fill out the form below
- **Report Suspicious Activity**: Please report any suspected impersonation attempts to Gordon Food Service by filling out the form below. Provide a copy of the email, as well as additional relevant details, including the date, time, method of communication (if not email), and any specific context from the communication. You might also consider contacting your local law enforcement, as well as the Federal Trade Commission.

Fraudulent Domains Used So Far

- gordonfoodsservices[.]com
- gfs-vendors[.]com
- gfsvendors-sharefiles[.]com
- gordonsfoodsservices[.]com
- halpems[.]com
- gordonfoodservicesinc[.]com
- gordonsfoodservices[.]com
- gfsvendorportal[.]com
- gfsvendorsportal[.]com
- gfsvendorpayportal[.]com
- gfsvendorspaymentportal[.]com
- gfsvendorspaymentsportal[.]com
- gfsvendorspayportal[.]com
- gfsapvendoranalysis[.]com
- gfsapvendorsanalysis[.]com
- gfsvendorssupport[.]com
- gordonfoodservice[.]zendesk[.]com
- primepaymentportal[.]com
- gordonfoodinc[.]com
- gfsvendorsapanalysis[.]com
- verification-gfspayments[.]com
- gfsvendorapanalysis[.]com
- auth-gfs[.]com
- gfsvendoranalysis[.]com
- gordonsfoodsservice[.]com
- gfs-apvendorsanalysis[.]com
- apvendorsanalysis-gfs[.]com
- verfication-gfspayments[.]com
- gordonfoodservicellc[.]zendesk[.]com
- documentation-gfsapvendoranalysis[.]com
- gfs-paymentsystem[.]com
- gordonfoodservicellc[.]com
- gfstransportllc[.]com
- gordonfoodservice[.]uno
- gordonfoodservice[.]bond
- verification-gfsvendors[.]com
- gfsvendorsverifications[.]com

SAMPLE FRAUDULENT EMAILS FOR ILLUSTRATIVE PURPOSES

Gordon Food Service

VENDOR DATA INTEGRITY & PAYMENT SECURITY

Vendor Compliance

Date: 14th July 2026

Dear Vendor Partner,

Immediate Action Required: Payment Profile Temporarily Suspended

Our advanced security-monitoring controls for detecting potential business email compromise have identified indicators that the banking information associated with your company's payment profile may have been changed or may no longer match information previously verified with your organization.

As a precautionary security measure intended to prevent the possible misdirection or loss of your company's funds, the payment profile associated with your vendor account has been temporarily suspended.

Current Payment Status

- **All pending and future payments are currently on hold.**
- The payment profile will remain suspended until the required verification process has been completed.
- No payments will be processed or released while the suspension remains active.

Required Action by Accounts Receivable

An authorized member of your Accounts Receivable team must complete a **one-time identity verification** to confirm your banking information. Please use the QR code or the link below to access the secure verification portal.

Verify Your Identity

Scan the QR code with your mobile device, or click the button below

After successful verification, you will be prompted to review and confirm your banking information. If any information appears unfamiliar or incorrect, please contact our Vendor Support team immediately.

If the recipient of this notice is not responsible for managing your company's payment information, please forward this notice immediately to the appropriate Accounts Receivable representative.

Where necessary, the matter may also be escalated internally to your Accounting, Finance, Treasury or Controller department.

Important Security Instructions

- Do not send complete banking information, passwords or authentication codes by email.
- Gordon Food Service personnel will not request your portal password or multifactor-authentication code.
- Carefully report any banking information displayed in the portal that your organization does not recognize.
- Use only your organization's trusted portal access method or an official Gordon Food Service website.

This is a mandatory financial-security requirement and should not be treated as a routine administrative request.

Prompt completion is required to prevent further payment delays and reduce the risk of funds being directed to an unauthorized or incorrect account.

Sincerely,
Vendor Data Integrity & Compliance Team
Gordon Food Service

This message was sent by Gordon Food Service Vendor Compliance.
Please retain this notice for your payment-security records.

From: Gordon Food Service
<vendormanagement@documentation-gfsapvendoranalysis>
Sent: Thursday, March 19, 2026 4:18 PM
To: [redacted]
Subject: Final Notice: Payment Releasing Today to Account Ending 8984 – Immediate Action Required if Incorrect

Gordon FOOD SERVICE

Dear Vendor Partner,

Final Notice: Payment Release Scheduled Today

This is a follow-up to our previous communication regarding the banking update submitted to your account.

*As we have **not received any response or objection**, we are proceeding in accordance with standard processing timelines.*

⚠️ ***Payment Processing Update***

***Payment is being processed today (March 19, 2026)** to the bank account ending in **8984**.*

*If this account **is NOT authorized by your organization**, you must contact us **immediately prior to release** to prevent misdirected funds.*

Once payment is processed, recovery may be delayed and subject to banking procedures.

Immediate Action Required (If Incorrect)

- *Contact us immediately*
- *Confirm the correct banking details*
- *Provide an authorized contact for verification*

URGENT: Contact Vendor Compliance

Contact

Vendor Data Integrity & Compliance Team
Gordon Food Service

If you Believe You've Been Scammed
If you believe you have provided information to a scammer or have been a victim of a scam, take the following steps:

- **Contact Your Company's Security Team:** Immediately contact your company's security team so they can investigate the incident and take further action if necessary.
- **Contact Your Financial Institution:** If you provided financial information, immediately contact your bank or credit card company to report the incident and take steps to protect your accounts.
- **Change Your Passwords:** If you provided passwords or other login credentials, change them immediately for all affected accounts. If you use the same, or a similar, password for any other unrelated accounts, change them as well. Use a password manager along with strong, unique passwords for each account. Ensure multi-factor authentication is turned on for all sensitive accounts.
- **Monitor Your Accounts:** Regularly monitor your bank accounts, credit card statements, and other accounts for any unauthorized activity.
- **Consider a Credit Freeze:** You may want to consider placing a credit freeze on your credit report to prevent scammers from opening new accounts in your name. You can contact the three major credit bureaus (Equifax, Experian, and TransUnion) to request a freeze.
- **File a Report with the Authorities:** Report the incident to the appropriate authorities, such as the Federal Trade Commission (FTC) in the United States (reportfraud.ftc.gov) or your local law enforcement agency.

Staying Informed
Gordon Food Service is committed to keeping our community informed about the latest scam tactics. We will periodically update this page with new information and resources. You can also learn more about common scams and how to protect yourself from the resources that are on the Federal Trade Commission (FTC) website, or other government agencies.

Please submit any suspicious scams or communications in the form here.