

How to spot a fake job background check fee

[Read online: https://cyberguardlab.com/blog/employment-background-check-fee-scam](https://cyberguardlab.com/blog/employment-background-check-fee-scam)

Published October 15, 2026 | Updated October 15, 2026

Short answer

A fake job background check fee is a demand that you pay for your own background screen, drug test, or "onboarding portal" before you start work. The payment is the scam: once you send gift cards, a wire, crypto, or a payment-app transfer, the job vanishes and the money is gone. A real screen works the other way around. The employer orders and pays for the report from a consumer reporting agency, and under the Fair Credit Reporting Act (FCRA) it must first give you a standalone written disclosure and get your written authorization. This page covers that fee and how a lawful screen differs from it. CyberGuardLab publishes these checklists on its own editorial schedule. A handful of product pages on this site earn affiliate commissions, which can affect which suites appear in the optional list at the end; every warning sign and step below is free to use, and paid links appear only in that labeled section.

Advertising disclosure: CyberGuardLab is an independent comparison site. We are not TotalAV, Norton, Bitdefender, McAfee, or Avast. If you buy through our links, we may earn a commission, which can affect ranking and placement.

Independent US household comparison site. Not the vendor. Paid links below may earn a commission. Confirm first-year price, renewal, device limit, and refund terms at checkout.

CYBERGUARDLAB · GUIDE

How to spot a fake job background check fee

A real employer orders and pays for your screening.



Short answer

Do not pay for your own background check to get a job. In a lawful screen, the employer is the customer of the background screening company: it signs up with the agency, certifies its purpose, and pays for the report. Your part is to read a disclosure and sign an authorization, not to fund anything. A request to cover a "screening fee" with gift cards, wires, crypto, or a payment app is a hard stop.

How the fee demand usually unfolds

- * An offer arrives quickly. A message, chat interview, or ad leads to an offer with little real vetting. The FTC's January 2023 business blog on employment scams describes fake online interviews and phony onboarding portals.
- * A "screening" step appears with a bill. You are told a background check, drug screen, or portal login must be paid before you start. The FTC's job-scams article and consumer.gov's Job Scams Explained both say: if someone asks you to pay to get a job, that is a scam.
- * No real disclosure or authorization form shows up. Instead of a standalone FCRA disclosure and a consent signature, you get an invoice, a payment link, or a "screening vendor" chat handle.
- * Payment is steered to methods that are hard to reverse. Gift cards, cryptocurrency, a payment app, or a wire service - methods consumer.gov compares to cash.
- * Identity data is collected along with the fee. The fake portal asks for your Social Security number, a license photo, and bank details "for payroll."
- * After you pay, the contact disappears. No report is ever run, no job starts, and the fee is not refunded.

Warning signs that the "background check" fee is fake

What you notice | What official guidance says | What to do

Paid link

Norton 360 | See the Norton first-year offer



[See the Norton first-year offer](https://cyberguardlab.com/norton)

Offer page: <https://cyberguardlab.com/norton> Hop: <https://trysecurities.com/offer/norton?dtm=gg&cid=>

You must pay before screening begins | FTC: anyone who asks you to pay for the promise of a job is a scammer | Stop; do not send money

Fee must be paid with gift cards, crypto, a payment app, or a wire | consumer.gov: scammers insist on those methods because they are hard to reverse | Refuse; report the contact

No standalone disclosure, no authorization form, just a payment link | FTC: a company using a background report must tell you in writing and get your written permission | Ask for the disclosure and the agency's name; walk away if none exists

The "screening company" has no website, address, or dispute process you can find | FTC: you can ask the agency for a copy of your report and dispute errors with it directly | Look up the agency yourself before sharing anything

Placement firm demands an advance fee from you | FTC: honest placement firms typically charge the company, not the candidate | Walk away from the fee request

SSN or bank info requested before any real interview | FTC background-checks article: SSN or banking info on an early application is a red flag | Do not provide it; report if you already did

Who pays for a legitimate background check?

The company that orders the report pays for it. A consumer reporting agency sells background reports to the business that requests them, and that business must certify a permissible purpose before the agency releases a report. The applicant is the subject of the report, not the buyer. If you are told to pay the agency, or a person claiming to represent it, treat that as a scam signal.

How a lawful FCRA background check works

A lawful screen follows a fixed sequence of notices. The FTC's Employer Background Checks and Your Rights page and its business guidance describe it this way:

Stage | What the company must do | What a fee scam does instead

Before the report | Give you a clear written disclosure in a standalone document and get your written authorization | Sends

an invoice or payment link

Ordering | Certifies its purpose to the consumer reporting agency and pays for the report | Asks you to pay a "vendor" directly

Before a negative decision | Sends a pre-adverse action notice with a copy of the report and "A Summary of Your Rights Under the Fair Credit Reporting Act" | Asks for more money to "clear" a problem

After a negative decision | Sends an adverse action notice naming the agency and explaining your right to dispute and to get a free copy | Goes silent

How to spot a fake job background check fee

Use these six checks before you send money or open an "onboarding" payment page.

- * Treat any pay-to-start fee as a stop sign. The FTC says never pay for the promise of a job. A bill labeled "background check" or "drug screen" that you must cover yourself is that kind of fee.
- * Ask for the FCRA disclosure and authorization. A lawful screen starts with a standalone written disclosure and your signed authorization. A payment request is not a consent form.
- * Ask which consumer reporting agency runs the check. Get the agency's name, then find its website and phone number yourself. A real agency explains how to request your file and dispute errors.
- * Confirm the company and recruiter on your own. Search the name with "scam," "review," or "complaint," as the FTC recommends. Use a phone number or careers page you found yourself, not the link the stranger sent.
- * Refuse gift cards, wires, crypto, and payment-app "fees." consumer.gov says scammers insist on these because they work like cash. Requests to buy equipment with a promise of reimbursement are a related ploy.
- * Protect identity data and keep a paper trail. Do not put your Social Security number or bank details on an early application, the FTC warns. Save every message, portal screenshot, and payment instruction for your report.

If you already paid or shared personal data

- * Contact the company you used to send the money right away, report the fraud, and ask whether the transfer can be reversed.
- * If you paid with a gift card or a Zelle / Cash App transfer, tell that issuer or app immediately; recovery is often limited, but early reports still matter.
- * If the "company" also sent a check and asked you to forward part of it, treat it as a fake check scam and talk to your bank.
- * If you gave a Social Security number, bank account, or driver's license image, start a recovery plan at IdentityTheft.gov (Report identity theft).
- * Report the incident at ReportFraud.ftc.gov (How to report a scam to the FTC) and consider a separate filing at IC3.gov.

Free habits before any screening step

- * Treat cold LinkedIn or email pitches as unverified until you confirm them (LinkedIn recruiter phishing).
- * Tell a trusted person about any request for an up-front payment before you act on it.
- * Keep browser dangerous-site warnings turned up (Turn on enhanced Safe Browsing in Chrome) before opening unfamiliar portal links.
- * Never "hold" a position by buying gift cards at a store checkout.

What this page is not

This guide is only about a pre-start fee framed as a background check, drug test, or onboarding-portal charge, and how it differs from a lawful FCRA screen.

Broader fake-offer patterns are covered in How to spot a job offer scam. Check-cashing tricks belong in How to spot a fake check scam and How to spot a mystery shopper check scam. Benefits-claim impostors are in How to spot an unemployment benefits scam. Inbox links that mimic HR mail are better checked with How to spot a phishing email. Nothing here is legal advice; for FCRA rights, rely on the FTC pages in Sources and consult an attorney when you need counsel.

Optional paid security suites

Spotting a fake screening fee is a reading-and-refusal problem, not a software problem. If you were already shopping for device or identity-oriented suites, these are the only paid links in this article:

- * Norton plans: device protection with identity options on higher tiers (paid link; check renewal pricing).
- * Bitdefender plans: a pick when independent lab scores drive your shortlist (paid link).
- * TotalAV plans: compare on household device count and first-year price (paid link; read the renewing rate).
- * McAfee plans: one subscription across several phones and PCs (paid link; confirm the device cap).
- * Avast plans: useful if your household already runs Avast and prefers to stay (paid link).

Skipping every paid option is a sound choice.

FAQ

Can a real employer make me pay for my own background check?

No. The company that orders the report pays the consumer reporting agency. The FTC says anyone who demands payment for the promise of a job is a scammer.

What does the Fair Credit Reporting Act require before a background check?

The company must give you a clear written disclosure in a standalone document and get your written authorization before ordering a report from a consumer reporting agency.

What happens if a background report leads to a rejection?

You first get a pre-adverse action notice with a copy of the report and a Summary of Your Rights. After the decision, you get an adverse action notice naming the agency and explaining how to dispute errors.

How can I tell if a screening company is real?

Get its name, then find its website and phone number yourself. A real consumer reporting agency explains how to request your file and dispute errors. It does not collect fees from you through gift cards or payment apps.

Why do scammers want gift cards or crypto for a "screening fee"?

Because those methods are hard to reverse. consumer.gov explains that scammers insist on gift cards, cryptocurrency, payment apps, or wire services for that reason.

I already paid or gave my Social Security number. What should I do first?

Contact the payment provider immediately and ask about reversing the transfer, then report at ReportFraud.ftc.gov. If you shared identity details, use IdentityTheft.gov and consider filing at IC3.gov.

Sources

- * Job Scams (FTC Consumer Advice)
- * Employer Background Checks and Your Rights (FTC Consumer Advice)
- * Background Checks: What Employers Need to Know (FTC Business Guidance)
- * Taking the "ploy" out of employment scams (FTC business blog, Jan 25, 2023)
- * Job Scams Explained (consumer.gov)
- * ReportFraud.ftc.gov
- * IdentityTheft.gov
- * Internet Crime Complaint Center (FBI IC3)

Also read

- * Work-from-home reshipping scams
- * Fake W-2 phishing emails
- * Credit freeze vs identity monitoring
- * IRS Identity Protection PIN