Acme Corp Pre-acquisition Due Diligence — Final Report v3

Version v3 Generated Wed, 06 May 2026 20:11:42 GMT Report ID demo-report-1

SUBJECT IDENTIFIERS

NAME	Jordan T. Reeves
EMAILS	jordan.reeves@acmecorp.example, j.reeves@protonmail.example
PHONES	+1 (415) 555-0182
USERNAMES	@@jordanreeves, @jreeves84, @jtr_official
DOMAINS	jordanreeves.example

EXECUTIVE SUMMARY

Executive summary

Tracelight has completed a 32-worker OSINT sweep on Acme Corp Holdings, Inc. and the two named officers (Jordan Reeves, CEO; Priya Anand, CFO). No sanctions, PEP, or adverse-media exposure was detected on any of the three subjects. Three findings warrant attention before LOI signing on 2026-05-30:

1. **Active wage-and-hour class action** against the entity (N.D. Cal., Mendez v. Acme), motion to dismiss pending. Materiality: medium. 2. **Lookalike domain + phishing kit** ('acmecorp-secure.example') registered November 2025, hosting a credential-harvesting page. Brand & customer-fraud risk; recommend pre-close takedown. 3. **CFO personal email present in 2024 Lumma stealer-log dump**, including session cookies for personal banking. No corp credentials in the same dump, but recommend a forced-credential-rotation + step-up MFA across the executive team prior to integration.

All findings below are cited to the originating source. Every claim resolves to one or more rows in the evidence table.

Sanctions, PEP, and adverse media

Both named officers and the entity itself were screened against OFAC SDN, OFAC sectoral, UK HMT consolidated, EU consolidated, and Refinitiv World-Check One. **Zero matches** across all four lists for all three subjects. Adverse-media screening (5-year window) returned no hits.

Litigation

The entity is currently a named defendant in **Mendez et al. v. Acme Corp Holdings** (N.D. Cal., 3:25-cv-04412, filed 2025-09-12). Class certification has not been ruled on; motion to dismiss is pending. Priya Anand is named in

her CFO role (vicarious capacity); no personal liability is currently asserted. The Mendez v. Acme suit is the single most material litigation finding in this package and should be confirmed against management's representations under the seller disclosure schedule.

Cyber & breach posture

23 employee email addresses on @acmecorp.example appear in 14 distinct breaches. The entity's external attack surface is small (5 internet-facing hosts) but includes one out-of-date Confluence host with CVE-2023-22515 surface — recommend remediating before close. A phishing kit targeting Acme employees is currently live on a known credential-harvesting forum. **Recommendation:** initiate domain takedown and force a workspace-wide credential rotation prior to integration.

The CFO's personal email appears in a 2024 Lumma stealer-log dump that included a personal banking session cookie. While no Acme corp credentials are in the same dump, the dump confirms the CFO's primary device was, at some point in 2024, infected with a credential-stealer. Recommend post-close re-imaging or device replacement for both named executives.

Officer credentials and history

CFO licenses are current (CPA-CA, FINRA Series 7 + 63, no disclosures). Both officers' employment histories match the seller's disclosures and S-1 draft tenure dates. CEO has 4 California corporate officer roles (3 active, 1 voluntarily dissolved 2021 in good standing — not a red flag).

Recommendation

Proceed to LOI subject to (a) confirmation of Mendez settlement reserve in the disclosure schedule, (b) takedown of the lookalike domain prior to public deal announcement, and (c) executive-team credential rotation + post-close device re-imaging. None of the findings rise to the threshold of "deal killer" but the Mendez exposure should be priced in.

EVIDENCE TRAIL

MARK-ER	SOURCE	URL
E#1	ofac	https://sanctionssearch.ofac.treas.gov/
E#2	uk_hmt	https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets
E#3	eu_consolidated	https://webgate.ec.europa.eu/fsd/fsf
E#4	ofac	https://sanctionssearch.ofac.treas.gov/

E#5	ofac	https://sanctionssearch.ofac.treas.gov/
E#6	world_check	https://www.refinitiv.com/en/products/world-check-kyc-screening
E#7	ofac	https://sanctionssearch.ofac.treas.gov/
E#8	world_check	https://www.refinitiv.com/en/products/world-check-kyc-screening
E#9	media	https://news.google.com/
E#10	courtlistener	https://www.courtlistener.com/
E#11	courtlistener	https://www.courtlistener.com/
E#12	whois	whois://acmecorp-secure.example
E#13	phishtank	https://phishtank.org/
E#14	haveibeenpwned	https://haveibeenpwned.com/account/panand@gmail.example
E#15	darkweb_index	tor://internal-darkweb-index/
E#16	haveibeenpwned	https://haveibeenpwned.com/PwnedWebsites
E#17	haveibeenpwned	https://haveibeenpwned.com/
E#18	shodan	https://www.shodan.io/
E#19	ssl_logs	https://crt.sh/
E#20	cpaverify	https://www.cpaverify.org/
E#21	finra_brokercheck	https://brokercheck.finra.org/
E#22	linkedin	https://www.linkedin.com/in/jordan-reeves-acme
E#23	linkedin	https://www.linkedin.com/in/jordan-reeves-acme
E#24	linkedin	https://www.linkedin.com/in/priya-anand-cfo
E#25	linkedin	https://www.linkedin.com/in/priya-anand-cfo
E#26	ca_secstate	https://bizfileonline.sos.ca.gov/

This report is generated from automated OSINT collection. Use of this document for FCRA-regulated decisions (employment, housing, credit, insurance) requires recorded subject consent.