

RETROSPECTIVE OSINT CASE STUDY, FULL REPORT

Could a background check have seen it coming?

The recording device found in OpenAI's executive boardroom, September 2026

The engineer charged in the case, Abdulrahman Alfozan (عبدالرحمن الفوزان)

REPORT DATE	14 October 2026
INFORMATION AS OF	14 October 2026
PURPOSE	Case study for employers in technology, industry and security, and for HR
PREPARED BY	ProfCheck

Prepared from public sources only. The person discussed has been charged in a federal criminal complaint. He has not been convicted and is presumed innocent.

1. The answer in brief

On 13 October 2026 the US Department of Justice announced the arrest of an OpenAI engineer. He is charged with planting a covert audio recording device in the company's executive conference room in San Francisco [1][2]. This review answers one defined question: **was there information online, before he was hired and while he worked there, that a background check should have raised?**

We fixed the method before the search, as in our earlier case study on Flydubai flight FZ1073. We checked two dates: the day before he joined OpenAI (July 2025, per the complaint [2]), and the day before the device was installed (about 28 September 2026). We read the findings through two lenses, kept apart: the US government's insider-risk indicators [3][4], and ProfCheck's own method. We also ran 23 Google searches limited to pages dated before the hiring date, to see what a check run then would have returned [5].

QUESTION	AT HIRING (JULY 2025)	DURING EMPLOYMENT (BEFORE 28 SEP 2026)
Was there public information about him online?	Yes. LinkedIn, GitHub, X, conference talks, papers, a venture fund's announcement of February 2025, and Saudi media profiles.	The same, and an X profile that listed OpenAI and the fund side by side.
Would a reasonable check have found it?	Yes. A name search with an employer's name returns his profiles and the fund announcement at the top. One record, on Meta, is found only by searching his code history on GitHub.	The same.
Was there negative conduct?	No. No criminal record, no sanctions, no hostility to an employer, no support for violence, none of ProfCheck's behavioural indicators.	No.
Were there red flags under ProfCheck's method?	Yes, two. Employment dates contradicted by a public record. An outside role held alongside a full-time job, which is a conflict of interest if it was not disclosed.	Yes, the same two. The fund role continued while he worked at OpenAI.

The red flags were public before he was hired. Under ProfCheck's method, a contradiction between the employment dates a candidate presents and a public record is an indicator of unreliability. The same applies to an outside role or interest that the employer was not told about, if that was the case. Neither proves wrongdoing. Both are red flags that should have been resolved through a clarification with the candidate before a hiring decision: ask him to explain the dates, ask him to list his outside roles in writing, and verify the answers with the former employers.

Our conclusion. A ProfCheck report at hiring would have raised both red flags and handed the employer two specific questions. Whether the answers would have changed the decision cannot be known. The report would not have shown anything about the act itself. The warning signs described in the complaint were inside the building: camera footage, searches in the company's own systems, and questions put to a chatbot. No background check from public sources reaches those.

2. The event and what is known

The charge. He was arrested on 9 October 2026 and appeared in federal court in San Francisco on 13 October. He is charged with one count of using, or attempting to use, a device to intercept oral communications (18 U.S.C. 2511(1)(b)), punishable by up to five years in prison and a fine of up to USD

250,000 [1][2]. The Department of Justice does not allege that a foreign government was involved [1]. At the first appearance he was remanded to custody, and a detention hearing was set for 19 October 2026 [6][7].

Figure 1

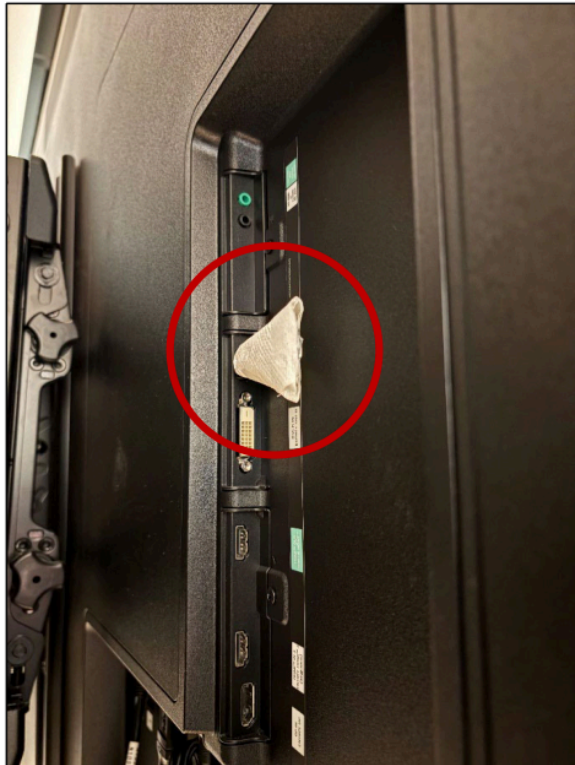


Figure 2 (Recording Device 1)



The device as shown in the criminal complaint: behind the television, wrapped in toilet paper (left), and unwrapped (right) [2].

What the complaint alleges [2]:

- **The device.** On or about 30 September 2026, company staff found a device inserted into a USB port at the back of a television in the executive conference room. It was a Seeed XIAO ESP32-S3 Sense, a thumb-sized board with a microphone and a memory card, wrapped in toilet paper. Its firmware appears to have been compiled on 28 September 2026, and the card's contents appear to have been encrypted.
- **The room.** Only executives and their assistants can book it. It is used for leadership meetings and briefings with government officials and business partners. He had no authority to enter it.
- **Camera footage.** He was near the room on ten dates between 8 and 29 September 2026.
- **Internal searches.** Between 17 August and 16 September 2026 he asked a workplace productivity agent about the company's buildings, meeting rooms, room calendars, and where leadership and external partners meet.
- **A chatbot account.** An account associated with his spouse, which shared device identifiers, IP use and path names with his own account, was used between 24 and 30 September 2026 to ask how to build a continuous audio recorder with live listening, Wi-Fi control and an encrypted memory card [8].
- **The second device.** On 5 October 2026 a camera, installed by then, recorded him checking behind the television. The same day, security staff opened a bag he had left in a printer room and found a second, similar device with his wallet and ID. On 6 October he collected the bag, reported missing items, and did not mention the device.

The company. OpenAI said that it used its own models to trace the device to him, that it has seen no sign that model weights, source code or customer data were taken, and that he was fired [9][10][11].

Identity. The Department of Justice names him as Abdulrahman Alfozan, 35, a Saudi national [1]. The complaint says he was educated in the United States, has been a permanent resident since September 2020, and has worked at the company as an engineer since about July 2025 [2]. His own X profile gives his name in Arabic as عبدالرحمن الفوزان [12]. Media reports describe his role as engineer on the product team [13] [14], or as engineering lead on the agents platform, from his LinkedIn and X profiles [15][16].

7. Since in or around July 2025, ALFOZAN—a foreign national who was educated in, and who since September 2020 has been a legal permanent resident of, the United States—has worked as an engineer at Company 1.

Paragraph 7 of the complaint: the start date at the company and his status in the United States [2].

3. How we checked

The question in three parts. For each of the two dates we asked separately:

- did the material **exist** publicly;
- would a reasonable check have **found** it;
- would an analyst who did not know the outcome have **read it as a red flag**.

Keeping these apart prevents a review written after the event from concluding that everything was obvious.

Indicators fixed in advance. Before the search we wrote down what to look for:

- **Insider-risk indicators.** We used the US Department of Defense's list of potential risk indicators for insider threats [3] and the national security adjudicative guidelines [4]. We kept only the indicators that rest on conduct and that a public record can show: a past dismissal, a security or compliance breach, misuse of IT, criminal or financial proceedings, outside activity in conflict with an employer, false hiring information, hostility to the employer, and support for violent extremism.
- **What we left out on purpose.** Those lists also include citizenship, the citizenship of a spouse, travel abroad and contact with foreigners. These are protected grounds. ProfCheck does not treat them as indicators, and neither does this review. Nationality, religion and political opinion were recorded only where a fact required it, and never coded as negative.
- **ProfCheck's method.** It covers sanctions, links to terrorism or foreign intelligence, criminal activity, financial issues and conflicts of interest, conduct on social networks, and verification of the employment history. It also marks four behavioural indicators: demeaning attitudes toward women, hostility to foreigners, imposing religious norms with justification of violent punishment, and deliberate deception.
- **Red flags of unreliability.** Under ProfCheck's method, two things are red flags to be resolved by clarification with the candidate: a contradiction between the employment dates the candidate presents and a public record, and non-disclosure of a conflict of interest, if there was one. This rule was written into the case file after the research, at the owner's instruction. It changes how the findings are classified, not what was searched or found.
- **Capability is not intent.** Public engineering work on audio, wireless devices or encryption counts as context. It is a red flag only if it shows recording people without consent.

Rules

- **Attribution.** An account is attributed to him only when at least two independent details match. His LinkedIn, GitHub and X accounts link to each other, and named outlets cite them [16][17].
- **Proof of time.** An item counts as visible before a date only if the platform's own date is confirmed by an independent record: an archive capture or a dated third-party record.

- **Conduct.** Public sources only: no logins, no contact with any account, and no research on relatives.

Sources searched.

- English, Arabic and Hebrew media.
- The court docket and the complaint.
- LinkedIn through a scraper that leaves no trace and needs no login.
- GitHub's public interface, including a search of all commits by his username [18].
- Academic, speaker and employer pages.
- X, Instagram, Threads, Hacker News and YouTube.
- The Wayback Machine and Software Heritage.
- The official sanctions lists of the US, UN, EU and UK.
- Federal court records and company registers.
- **The simulation:** 23 Google searches limited to pages dated on or before 30 June 2025, run through a commercial search interface [5].

4. His accounts, and how sure we are

ACCOUNT	WHAT IT SHOWS	ATTRIBUTION
LinkedIn, alfozan	Career from 2012 to the present; OpenAI as current employer; the venture fund as a part-time role [19]	High. Same handle as GitHub and X; cited by named outlets [16]
GitHub, alfozan	Company field "OpenAI"; personal projects; contributions to OpenAI and Meta repositories [17]	High. Links to his X account
X, @alfozan	Account since 2009; name in English and Arabic; bio listing OpenAI and the fund [12][20]	High. Linked from GitHub and Instagram
Instagram, alfozan	Private; posts not visible [21]	High, not reviewed
Hugging Face, Hacker News	No relevant content [22][23]	High

We set aside dozens of accounts and records of other people named Alfozan or Al-Fawzan. They include a senior religious scholar, a Saudi family business group, and a claimant in a 2022 English lawsuit.

5. The career, as presented and as recorded

PERIOD	ROLE	SOURCES
2011 to 2016	MIT, computer science and engineering, on a Saudi state university scholarship	[19][24][25]
2012 to 2016	Internships at Akamai, SAP and Microsoft; a start-up in 2015	[24]
2017 to 2022 (as presented)	Facebook / Meta, senior systems engineer, data platform	[19][26][27]
By 2021	Co-founder of a consultancy serving Saudi companies and institutions, alongside the Facebook job	[28][29][30]

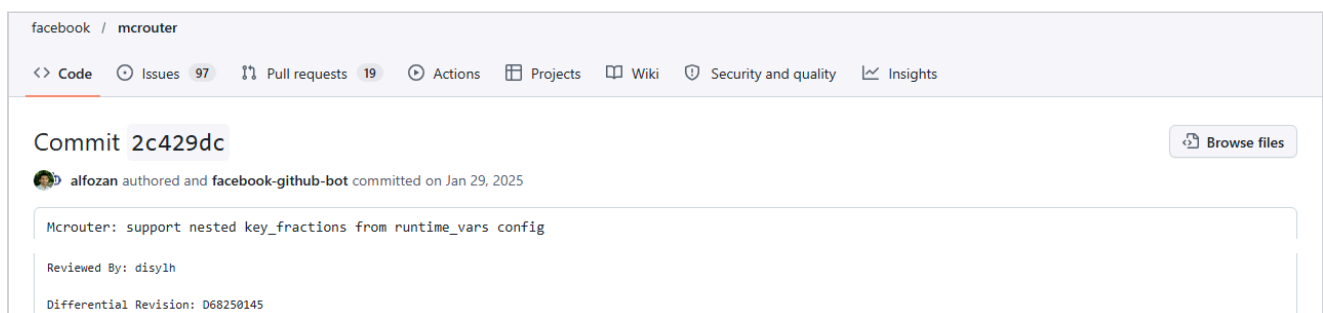
PERIOD	ROLE	SOURCES
2019 to 2020	Co-author of an academic paper on the Gradio tool, alongside the Facebook job	[31]
2022 to August 2025 (as presented)	Nash, founding engineer	[19][32]
2023 to 2025	UC Berkeley, master's degree in data science, online	[33]
February 2025 onward	Raed Ventures, a Saudi venture fund, venture partner (part-time)	[19][32] [34]
July 2025 (complaint) or September 2025 (LinkedIn) onward	OpenAI, engineer; "engineering lead, agents platform" on his profiles	[2][19]

There are no unexplained gaps. There is one contradiction (section 6) and one set of overlapping roles (section 7).

6. Red flag 1: employment dates contradicted by a record

What the candidate presented. On LinkedIn, Meta ends in 2022, and Nash runs from 2022 to August 2025 [19]. On 8 February 2025 the venture fund announced that he was "currently" a founding engineer at Nash and had "previously" spent five years at Meta [32].

What the record shows. On 29 January 2025, ten days before that announcement, an internal Meta code change was published in Meta's open-source repositories. Its author is "Abdul Alfozan", with a meta.com email address, and GitHub links the commit to his account [35]. It carries the marks of Meta's internal process: an internal review number (D68250145), a named Meta reviewer, and references to an internal project document and internal configuration paths. It is not an outside contribution. The Software Heritage archive holds a snapshot of the repository from 1 February 2025 that contains the commit [36]. So the record was public, and provably so, about five months before he joined OpenAI.



The commit on GitHub: authored by "alfozan", published on 29 January 2025, with Meta's internal review number [35].

← Back
8 Feb 2025

RAED VENTURES WELCOMES NEW VENTURE PARTNER – ABDULRAHMAN ALFOZAN

Abdulrahman is a seasoned professional with extensive experience in tech startups, entrepreneurship, and scaling technology companies. Currently, he is a Founding Engineer at Nash and previously spent five years at Meta (Facebook) as a Senior Engineer, specializing in machine learning and data platforms. He also held roles at Microsoft and SAP and studied computer science and engineering at MIT.

The fund's announcement of 8 February 2025: "Currently, he is a Founding Engineer at Nash and previously spent five years at Meta" [32].

What it could mean. The record does not say which of these is true:

- a second period at Meta, or a contract, that the profile does not list;
- Meta and Nash held at the same time;
- access to Meta's systems on some other basis.

We did not find any other Meta commit by him after 2019 [18]. One record is not proof of a false profile.

A smaller inconsistency of the same kind. The complaint says he has worked at OpenAI since about July 2025 [2]. SFGATE reported August [37], and his LinkedIn says September, with Nash running until August [19]. On 21 August 2025 the fund's website still described him as "currently a Founding Engineer at Nash" [38]. If the complaint's date is right, his public profile shows the OpenAI start two months late and Nash overlapping it.

Under ProfCheck's method, this is a red flag. The dates the candidate presents are contradicted by a public record. That is an indicator of unreliability, to be resolved by clarification with the candidate before a decision:

1. Ask him for the exact dates of his employment at Meta, including any later period or contract.
2. Ask whether he held Meta and Nash, or Nash and OpenAI, at the same time, and whether each employer knew.
3. Verify the dates directly with Meta and Nash.

7. Red flag 2: outside roles and conflicts of interest

The venture fund.

- In February 2025, while at Nash, he joined Raed Ventures, a Riyadh venture fund that invests in technology start-ups, as a venture partner. The fund announced it in English and Arabic [32][34][39], and his LinkedIn lists it as a part-time role from 2025 onward [19].
- **The role continued after he joined OpenAI.** His X profile on 28 June 2026 listed his OpenAI team and the fund side by side [20]. On 20 February 2026 the fund's website introduced him as "Engineering Lead at OpenAI" [40].

The consultancy.

- While a Facebook employee, he co-founded a consultancy that offered technical services to Saudi companies and institutions. He described it in a Saudi television interview [29][30].
- The consultancy's own profile document lists him by his Facebook title [28].

What is not known.

- Whether he disclosed these roles to Facebook, to Nash or to OpenAI, and whether any employer approved them, is not public.
- He announced the roles himself, so this is not concealment from the public.
- Disclosure to an employer is a separate matter.

Under ProfCheck's method, this is a red flag. An investment role at a venture fund held alongside an engineering lead role at an AI company is a potential conflict of interest. Non-disclosure, if it occurred, is an indicator of unreliability. The clarification with the candidate:

1. Ask him to list in writing every outside role, investment, advisory position and consulting engagement.
2. Ask whether each one was disclosed to, and approved by, the employer at the time.
3. Make disclosure and approval of the fund role a condition of the offer.

8. Other points to verify

The degree. His 2016 LinkedIn profile reads "Candidate for Bachelor of Science". The current profile lists the MIT years without a degree type [19][24]. We found no public record of the degree being awarded, and nothing that contradicts it. A routine degree check with the candidate's consent settles this. On its own it is not a red flag.

9. What we checked and found clean

- **Sanctions.** No match on the official US, UN, EU and UK lists, in Latin or Arabic script. A control name was found on each list, which shows the search worked [41][42][43][44]. OpenSanctions and INTERPOL's public notices returned only other people [45][46].
- **Courts and companies.**
 - No criminal, civil or bankruptcy case under his name before this one [47].
 - A 2019 petty-offense case in San Diego against an "Alfouzan" carries no given name. It is not attributed to him.
 - He holds no officer role in any company register we could search [48].
- **Social networks.**
 - We read 262 of the 284 posts on his X account [12]. None shows hostility to an employer or to the United States. None supports violence or extremism. None fits ProfCheck's four behavioural indicators.
 - One political reply he deleted in 2020 is an opinion, and is not coded.
- **Technical work.**
 - His public projects include radio and embedded-systems work from his student years, and personal software tools [17].
 - No public project, post or question about covert recorders, ESP32 boards or encrypted recordings appears before either date [18].

Seen in hindsight only. In December 2020 he wrote: "The weakest link in the security chain is the human element" [49]. Read today it sounds pointed. In context it was a reply to a friend whose WhatsApp account had been hijacked, followed by a link to WhatsApp's two-step verification page. We did not code it.

10. Where the warning signs actually were

Every warning sign about the act itself comes from inside the company [2]:

- **Physical access.** Camera footage put him near a room he had no right to use, ten times in three weeks.
- **System use.** He searched the company's own systems for meeting rooms, calendars, and where executives meet.
- **Tool use.** An account linked to him asked a chatbot to design a covert, encrypted, remotely monitored recorder, in the days before and after the installation.

Signs of this kind are what an internal insider-risk program can see: access control, camera footage, and the logs of internal tools. A background check from public sources cannot see them. The two tools answer different questions. One asks who is being hired. The other asks what an employee is doing.

11. Rewinding the search: what a check at hiring would have found

We ran 23 Google searches limited to pages that Google dates on or before 30 June 2025, to see what a check run then would have returned [5]. The results are in Appendix A.

- **The name with an employer's name** ("Meta", "Facebook", "Nash", "Raed") returned his own pages within the first results: the fund's announcement, his GitHub, X and Instagram, his conference talk and his paper. The fund role, the basis of red flag 2, was the first or second result.
- **The name alone** returned news about other people: Google dropped the quotation marks.
- **The name in Arabic** returned mostly a senior religious scholar and other people with the same name. It also returned Saudi television items about "the first Saudi engineer at Facebook", which are about him.
- **The commit at Meta**, the basis of red flag 1, did not appear in any Google search. Only a search of his code history on GitHub, by username, finds it [18].
- **A warning about the method.** One article about the arrest came through the date filter with a wrong date of 2004. Google's date filter is not a time machine. Archive captures are the reliable evidence.

What this means for a check. Name searches find what a person publishes about himself. The contradiction came from a source that names do not reach: the record of his own code. For engineers and other technical candidates, ProfCheck now checks public code history against the stated employment dates as part of every background check.

12. The indicators, one by one

Insider-risk indicators (conduct-based items only) [3][4]:

INDICATOR	BEFORE HIRING	DURING EMPLOYMENT
Dismissal, suspension or reprimand at a previous employer	Not found	Not found

INDICATOR	BEFORE HIRING	DURING EMPLOYMENT
HR complaints, or hostile talk about a former employer	Not found	Not found
Security or compliance violation	Not found	Not found
Outside employment or activity in conflict with an employer	Present: the fund role; the consultancy while at Facebook	Present: the fund role while at OpenAI
Public misuse of IT	Not found	Not found
Criminal proceedings, violence, criminal affiliations	Not found	Not found
Financial crime, bankruptcy, liens, judgments	Not found	Not found
Contact with a foreign intelligence service	Not found	Not found
False hiring information	Red flag, not proven: Meta dates contradicted by a commit	Red flag, not proven: OpenAI start month
Civil judgments against him	Not found	Not found
Ill-will toward the employer or the government	Not found	Not found
Support for violent extremism	Not found	Not found

ProfCheck's method:

DOMAIN	BEFORE HIRING	DURING EMPLOYMENT
Sanctions and blacklists	Clean	Clean
Links to terrorism or foreign intelligence	Not found	Not found
Criminal activity	Not found	Not found
Financial issues and conflicts of interest	Red flag: outside roles; disclosure unknown	Red flag: the fund role held while at OpenAI
Social networks (four behavioural indicators)	None	None
Employment verification	Red flag: dates contradicted by a record	Red flag: dates contradicted by a record

13. Lessons for employers

1. **Verify employment dates against records, not against the CV.** A LinkedIn profile is the candidate's own account. For technical candidates, the public history of their code is a record, and it carries dates and employer domains.
2. **Ask about outside roles in writing, at hiring and every year.** Investments, venture roles, advisory work, consulting and board seats all count. A role announced in public is not the same as a role disclosed to

the employer.

3. **Treat a red flag as a question with a deadline, not as a verdict.** A contradiction or an undisclosed role calls for a clarification and a verification. The answer decides.
4. **Search in the candidate's languages.** The consultancy and the scholarship were documented in Arabic sources.
5. **Keep checking after hiring.** The fund role stayed visible, on his own profile, throughout his employment. Periodic monitoring of public sources would have shown it.
6. **A clean public record is not a clean bill of insider risk.** The signs of the act were internal. A background check at the door and an insider-risk program inside the building do different jobs. An organisation that holds sensitive information needs both.

14. Limits of this review

- **Not reviewed:**
- Instagram is private [21].
- Facebook was not reviewed.
- A 93-minute Arabic interview, uploaded on 24 September 2026, was read only through automatic captions [50]. The parts read held nothing negative.
- **Not accessible** to a public-source review: California county court indexes [51][52], the federal PACER system [53], California's company register [54] and Google Scholar [55].
- **LinkedIn on the two dates.** LinkedIn blocks the Wayback Machine, so the exact content of his profile on the two dates cannot be proven. The fund's pages and other captures stand in for it.
- **What the commit shows.** It shows account use under an employer's domain, not his employment status. Only the employers can confirm the dates.
- **The source of the facts.** All facts about the act come from the complaint, which states allegations. They have not been tested in court.
- **The date of this review.** The story is still developing. Facts as of 14 October 2026.

About ProfCheck

ProfCheck runs OSINT background checks on candidates, employees, suppliers and business partners, from public and lawful sources only.

What a ProfCheck check covers

- Sanctions, blacklists, and links to terrorism or to BDS
- Indications of criminal activity
- Activity on social networks, including translation from Arabic with its cultural context
- Verification of contact details
- Gaps in employment history and contradictions between the CV and public records
- For technical candidates, the public history of their code, checked against the stated employment dates
- In the extended check, also financial problems and conflicts of interest

How we work

- **Every finding carries a link** that the client can open and verify.
- **Namesakes are separated explicitly.** A hit is attributed only on more than one matching detail.
- **Searches cover the candidate's languages and usernames**, and include archives of deleted content.
- **A finding is reported with its context and level of certainty.** Red flags come with the question to put to the candidate. The report does not recommend or disqualify; the decision stays with the employer.
- **Reports are delivered in Hebrew or English**, usually within three business days of receiving the full details.

Beyond the standard check: a focused social-media check, OSINT investigations by project, and workshops for recruiters and security officers.

ProfCheck | profcheck.co

Appendix A. The simulation queries

All queries were run on 14 October 2026 through SerpAPI's Google engine, limited to pages dated on or before 30 June 2025 [5]. "His pages" counts distinct results that belong to him or are about him.

#	KIND	QUERY	RESULTS	HIS PAGES	WHAT FILLED THE RESULTS
EN1	Name, English	"Abdulrahman Alfozan"	10	0	News about other cases; Google dropped the quotes
EN2	Name, English	"Abdulrahman Alfozan" engineer	9	0	News about other cases
EN3	Name, English	"Abdulrahman Alfozan" Meta OR Facebook	10	9	Fund announcement (Feb 2025), Instagram, GitHub, Google Scholar, X, YouTube, the Spark talk, the Gradio paper
EN4	Name, English	"Abdulrahman Alfozan" Nash	10	4	Fund announcement and the fund's LinkedIn post; two posts on X
EN5	Name, English	"Abdul Alfozan"	10	0	Other people with a similar name
EN6	Name, English	"Abdulrahman Al-Fozan"	10	1	His MIT class page; the rest are other people
EN7	Name, English	"Abdulrahman Alfozan" Raed	10	5	Fund announcement, fund post, GitHub, a 2018 interview, the Spark talk; one article about the arrest leaked through with a wrong date
EN8	Name, English	"Alfozan" MIT engineer	7	2	His MIT class page and his Google Scholar profile
AR1	Name, Arabic	"عبدالرحمن الفوزان"	9	0	A religious scholar and other people with the same name
AR2	Name, Arabic	"عبدالرحمن الفوزان" فيسبوك	9	6	Saudi TV and Al Arabiya items on the first Saudi engineer at Facebook; the fund's Arabic announcement
AR3	Name, Arabic	"عبد الرحمن الفوزان" وادي السيليكون	10	0	Other people with the same name
AR4	Name, Arabic	"عبدالرحمن الفوزان" مهندس	9	0	Other people with the same name
AR5	Name, Arabic	"رائد عبدالرحمن الفوزان"	10	0	A family business and other people with the same name
HD1	Username	"alfozan" github	10	2	His GitHub and a post on X; projects he contributed to
HD2	Username	"alfozan.io"	0	0	No results
HD3	Username	"@alfozan"	10	7	GitHub, Instagram, three posts on X, a 2018 interview, a post that tags him

#	KIND	QUERY	RESULTS	HIS PAGES	WHAT FILLED THE RESULTS
SO1	Inside a network	site:linkedin.com "Abdulrahman Alfozan"	10	0	Unrelated pages: the engine ignored the site filter
SO2	Inside a network	site:github.com alfozan	10	0	Unrelated pages: the engine ignored the site filter
SO3	Inside a network	site:twitter.com alfozan	10	0	Unrelated accounts
SO4	Inside a network	site:raed.vc Alfozan	10	0	Unrelated videos: the engine ignored the site filter
TG1	Targeted	"Abdul Alfozan" mcrouter OR hhvm	10	0	No trace of the 2025 Meta commit
TG2	Targeted	"Saudi Silicon Valley" Alfozan	0	0	No results
TG3	Targeted	"Alfozan" consulting Saudi government	10	0	A Saudi holding company with the same family name

Sources

A. Sources checked, with findings

Sources that returned information used in this report.

- [1] Saudi National Arrested for Installing Surreptitious Audio Recording Device at OpenAI. US Department of Justice, Office of Public Affairs | press release, 13 Oct 2026 | accessed 2026-10-14.
<https://www.justice.gov/opa/pr/saudi-national-arrested-installing-surreptitious-audio-recording-device-openai>
- [2] United States v. Alfozan, criminal complaint and affidavit, case 3:26-mj-71329. US District Court, Northern District of California (via CourtListener RECAP) | court filing, 8 Oct 2026 | accessed 2026-10-14.
<https://storage.courtlistener.com/recap/gov.uscourts.cand.480828/gov.uscourts.cand.480828.1.0.pdf>
- [3] Insider Threat: Potential Risk Indicators (PRI), job aid. Center for Development of Security Excellence (CDSE), US DoD | guidance; Wayback Machine capture of 2 Feb 2025 | accessed 2026-10-14.
https://web.archive.org/web/20250202055921/https://www.information.marines.mil/Portals/224/Docs/BTAC/CDSE_insider_threat_indicators_job_aid.pdf
- [4] Security Executive Agent Directive 4: National Security Adjudicative Guidelines. Office of the Director of National Intelligence | directive, 2017; Wayback Machine capture of 11 Oct 2026 | accessed 2026-10-14.
<https://web.archive.org/web/20261011002813/https://archive.dni.gov/files/NCSC/documents/Regulations/SEAD-4-Adjudicative-Guidelines-U.pdf>
- [5] Google search through SerpAPI, 23 queries limited to pages dated on or before 30 Jun 2025. SerpAPI | search interface, run 14 Oct 2026 | accessed 2026-10-14.
<https://serpapi.com/search-api>
- [6] Minute entry: initial appearance, 13 Oct 2026. US District Court, N.D. California (via CourtListener RECAP) | court filing, 13 Oct 2026 | accessed 2026-10-14.
<https://storage.courtlistener.com/recap/gov.uscourts.cand.480828/gov.uscourts.cand.480828.5.0.pdf>
- [7] United States v. Alfozan, docket 3:26-mj-71329. CourtListener (Free Law Project) | court docket | accessed 2026-10-14.
<https://www.courtlistener.com/docket/74958115/united-states-v-alfozan/>
- [8] An OpenAI employee allegedly used a chatbot to help plant a recording device at the office. WIRED | news, 13 Oct 2026 | accessed 2026-10-14.
<https://www.wired.com/story/an-openai-employee-allegedly-used-a-chatbot-to-help-plant-a-recording-device-at-the-office/>
- [9] OpenAI statement on the arrest. OpenAI Newsroom on X | post, 13 Oct 2026 | accessed 2026-10-14.
<https://x.com/OpenAINewsroom/status/2110095403198849132>
- [10] FBI arrests OpenAI employee accused of planting hidden recording device in conference room. TechCrunch | news, 13 Oct 2026 | accessed 2026-10-14.
<https://techcrunch.com/2026/10/13/fbi-arrests-openai-employee-accused-of-planting-hidden-recording-device-in-conference-room/>
- [11] OpenAI employee arrested on suspicion of hiding a recording device in the management boardroom (Hebrew). mako (N12) | news, 14 Oct 2026 | accessed 2026-10-14.
https://www.mako.co.il/news-world/2026_q4/Article-fffb47799831a1026.htm
- [12] @alfozan, X profile. X | profile | accessed 2026-10-14.
<https://x.com/alfozan>
- [13] OpenAI employee arrested over hidden recording device. CNN | news, 13 Oct 2026 | accessed 2026-10-14.
<https://www.cnn.com/2026/10/13/business/openai-recording-device>
- [14] OpenAI employee arrested for allegedly hiding a sophisticated recording device in its office (Arabic). CNN Arabic | news, 14 Oct 2026 | accessed 2026-10-14.
<https://arabic.cnn.com/middle-east/article/2026/10/14/openai-employee-arrested-for-allegedly-hiding-a-sophisticated-recording-device-in-its-office>
- [15] FBI arrests OpenAI employee charged with planting secret recording device in conference room. Fortune | news, 13 Oct 2026 | accessed 2026-10-14.
<https://fortune.com/2026/10/13/fbi-arrests-openai-employee-charged-planting-secret-recording-device-conference-room/>

- [16] Who is Abdulrahman Alfozan? Saudi OpenAI engineer's LinkedIn in focus after arrest. Hindustan Times | news, 14 Oct 2026 | accessed 2026-10-14.
<https://www.hindustantimes.com/world-news/us-news/who-is-abdulrahman-alfozan-saudi-openai-engineers-linkedin-in-focus-after-arrest-over-hidden-recording-device-fbi-director-kash-patel-reacts-101791926669433.html>
- [17] alfozan, GitHub profile (company field: OpenAI). GitHub | profile | accessed 2026-10-14.
<https://github.com/alfozan>
- [18] GitHub commit search by author alfozan. GitHub REST API | search, 14 Oct 2026 | accessed 2026-10-14. Run through the API endpoint api.github.com/search/commits?q=author:alfozan; the link opens the same search on the website (sign-in may be required).
<https://github.com/search?q=author%3Aalfozan&type=commits>
- [19] Abdulrahman Alfozan, LinkedIn profile (read through a no-login scraper on 14 Oct 2026). LinkedIn | profile | accessed 2026-10-14.
<https://www.linkedin.com/in/alfozan>
- [20] @alfozan, X profile, Wayback Machine capture of 28 Jun 2026 (bio lists OpenAI and Raed). Internet Archive | archived profile | accessed 2026-10-14.
<https://web.archive.org/web/20260628025905/https://x.com/alfozan>
- [24] The same LinkedIn profile, Wayback Machine capture of 22 Jan 2016. Internet Archive | archived profile | accessed 2026-10-14.
<https://web.archive.org/web/20160122141043/https://www.linkedin.com/in/alfozan>
- [25] Abdul Alfozan's page, MAS.863 How to Make (Almost) Anything, 2012. MIT Center for Bits and Atoms | class page | accessed 2026-10-14.
<https://fab.cba.mit.edu/classes/863.12/people/alfozan/>
- [26] Abdulrahman Alfozan, speaker page, Spark + AI Summit (Facebook). Databricks | archived page, 15 Sep 2019 | accessed 2026-10-14.
<https://web.archive.org/web/20190915140028/https://databricks.com/speaker/abdulrahman-alfozan>
- [27] Saudi Young Professionals in Silicon Valley (interview). Arab Gulf States Institute in Washington | analysis, 26 Mar 2018 | accessed 2026-10-14.
<https://agsi.org/analysis/saudi-young-professionals-in-silicon-valley/>
- [28] Saudi Silicon Valley Tech Consulting (company profile listing him as a Facebook senior systems engineer). saudisiliconvalley.com | PDF, 2021 | accessed 2026-10-14.
<https://saudisiliconvalley.com/SaudiSiliconValleyTechConsulting.pdf>
- [29] Profile of Eng. Abdulrahman Alfozan and the consultancy he co-founded (Arabic). Ajel | news, 15 Feb 2023 | accessed 2026-10-14.
<https://ajel.sa/local/3vgl8yz0dv>
- [30] Jusoor, episode 21: Eng. Abdulrahman Alfozan (Arabic). Saudi TV on YouTube | video, 13 Apr 2023 | accessed 2026-10-14.
<https://www.youtube.com/watch?v=aKFhaFPgQxo>
- [31] Gradio: Hassle-Free Sharing and Testing of ML Models in the Wild (co-author). arXiv | paper, Jun 2019 | accessed 2026-10-14.
<https://arxiv.org/abs/1906.02569>
- [32] Raed Ventures welcomes new venture partner, Abdulrahman Alfozan. Raed Ventures | announcement, 8 Feb 2025 | accessed 2026-10-14. Wayback Machine capture of 23 Mar 2025:
<https://web.archive.org/web/20250323022105/https://raed.vc/news/raed-ventures-welcomes-new-venture-partner-abdulrahman-alfozan/>
<https://raed.vc/news/raed-ventures-welcomes-new-venture-partner-abdulrahman-alfozan/>
- [33] Abdulrahman Alfozan, MIDS 2025 alumni page. UC Berkeley School of Information | profile | accessed 2026-10-14.
<https://www.ischool.berkeley.edu/people/abdulrahman-alfozan>
- [34] Raed Ventures welcomes Eng. Abdulrahman Alfozan as investment partner (Arabic). Raed Ventures | announcement, 10 Feb 2025 | accessed 2026-10-14.
<https://raed.vc/ar/news/%d8%b1%d8%a7%d8%a6%d8%af-%d9%81%d9%86%d8%aa%d8%b4%d8%b1%d8%b2-%d8%aa%d8%b1%d8%ad%d8%a8-%d8%a8%d8%a7%d9%86%d8%b6%d9%85%d8%a7%d9%85-%d8%a7%d9%84%d9%85%d9%87%d9%86%d8%af%d8%b3-%d8%b9%d8%a8%d8%af%d8%a7/>

- [35] [Commit 2c429dc in facebook/mcrouter: 'Mcrouter: support nested key_fractions from runtime_vars config', authored by Abdul Alfozan \(meta.com address\), 29 Jan 2025](#). GitHub | code commit | accessed 2026-10-14. The author's email domain is read from the GitHub API record of the commit; the local part is not reproduced.
<https://github.com/facebook/mcrouter/commit/2c429dc8029ff8e5da8227f72176134be1a9c558>
- [36] [Software Heritage archive of the same commit; the archive's snapshot of github.com/facebook/mcrouter on 1 Feb 2025 points to it](#). Software Heritage | archive record | accessed 2026-10-14.
<https://archive.softwareheritage.org/swh:1:rev:2c429dc8029ff8e5da8227f72176134be1a9c558>
- [37] [FBI arrests OpenAI engineer in SF](#). SFGATE (syndicated on Yahoo News) | news, 13 Oct 2026 | accessed 2026-10-14.
<https://www.yahoo.com/news/us/articles/fbi-arrests-openai-engineer-sf-232528978.html>
- [38] [Raed Ventures team page, Wayback Machine capture of 21 Aug 2025 \('currently a Founding Engineer at Nash'\)](#). Internet Archive | archived page | accessed 2026-10-14.
<https://web.archive.org/web/20250821032650/https://raed.vc/>
- [39] [Raed Ventures is pleased to welcome Abdulrahman Alfozan](#). Raed Ventures on LinkedIn | post, 8 Feb 2025 | accessed 2026-10-14.
https://www.linkedin.com/posts/raedvc_raed-ventures-is-pleased-to-welcome-abdulrahman-activity-7294073016039141377-oVDO
- [40] [Raed Ventures team page, Wayback Machine capture of 20 Feb 2026 \('Engineering Lead at OpenAI'\)](#). Internet Archive | archived page | accessed 2026-10-14.
<https://web.archive.org/web/20260220070939/https://raed.vc/>
- [49] [@alfozan, reply of 1 Dec 2020 \('The weakest link in the security chain is the human element'\)](#). X | post | accessed 2026-10-14. Wayback Machine capture of the same day:
<https://web.archive.org/web/20201201232329/https://twitter.com/alfozan/status/1333914323937161216>
<https://x.com/alfozan/status/1333914323937161216>
- [50] [Abdulrahman Alfozan: from the Mawhiba programme to OpenAI \(Arabic, 93 minutes\)](#). Identity Capital podcast on YouTube | video, uploaded 24 Sep 2026 | accessed 2026-10-14.
https://www.youtube.com/watch?v=u1Dq_g-d9XI

B. Sources checked, no findings

Sources searched that returned no relevant record on the date shown. A no-findings result covers only that source, that query and that date.

- [22] [Alfozan, Hugging Face profile](#). Hugging Face | profile | accessed 2026-10-14.
<https://huggingface.co/Alfozan>
- [23] [alfozan, Hacker News profile](#). Hacker News | profile | accessed 2026-10-14.
<https://news.ycombinator.com/user?id=alfozan>
- [41] [OFAC Specially Designated Nationals and consolidated non-SDN lists](#). US Treasury | official list, downloaded 14 Oct 2026 | accessed 2026-10-14.
<https://sanctionslistservice.ofac.treas.gov/api/PublicationPreview/exports/SDN.CSV>
- [42] [UN Security Council Consolidated List](#). United Nations | official list, downloaded 14 Oct 2026 | accessed 2026-10-14.
<https://scsanctions.un.org/resources/xml/en/consolidated.xml>
- [43] [EU Financial Sanctions Files, consolidated list](#). European Commission | official list, downloaded 14 Oct 2026 | accessed 2026-10-14.
https://webgate.ec.europa.eu/fsd/fsf/public/files/csvFullSanctionsList_1_1/content?token=dG9rZW4tMjAxNw
- [44] [UK Sanctions List](#). Foreign, Commonwealth and Development Office | official list, downloaded 14 Oct 2026 | accessed 2026-10-14.
<https://sanctionslist.fcdo.gov.uk/docs/UK-Sanctions-List.csv>
- [45] [OpenSanctions search](#). OpenSanctions | database | accessed 2026-10-14.
<https://www.opensanctions.org/search/?q=Abdulrahman%20Alfozan>
- [46] [INTERPOL public Red and Yellow Notices](#). INTERPOL | database | accessed 2026-10-14.
<https://www.interpol.int/en/How-we-work/Notices/Red-Notices/View-Red-Notices>
- [47] [CourtListener search of federal court records \(RECAP and opinions\)](#). Free Law Project | database | accessed 2026-10-14. Apart from this case, one 2019 petty-offense docket in San Diego, 'United States v. Alfouzan', carries no given name and is not attributed to him.
<https://www.courtlistener.com/?q=%22Abdulrahman%20Alfozan%22~5&type=r>

- [48] OpenCorporates officer search. OpenCorporates | database | accessed 2026-10-14.
<https://opencorporates.com/officers?q=Alfozan>

C. Sources checked, not accessible

Sources that could not be queried or retrieved (blocked, login or captcha, not publicly searchable). These are NOT 'no findings'; fallbacks tried are noted.

- [21] alfozan, Instagram account (private). Instagram | profile | accessed 2026-10-14.
<https://www.instagram.com/alfozan/>
- [51] San Francisco Superior Court online case index (bot challenge). Superior Court of California, San Francisco | database | accessed 2026-10-14.
<https://webapps.sftc.org/ci/CaseInfo.dll>
- [52] Santa Clara County Superior Court public portal (access denied). Superior Court of California, Santa Clara | database | accessed 2026-10-14.
<https://portal.sccscourt.org/search>
- [53] PACER Case Locator (login required). US Courts | database | accessed 2026-10-14.
<https://pcl.uscourts.gov/>
- [54] California Secretary of State bizfile search (blocked). California Secretary of State | database | accessed 2026-10-14.
<https://bizfileonline.sos.ca.gov/search/business>
- [55] Google Scholar author search (sign-in required). Google | database | accessed 2026-10-14.
https://scholar.google.com/citations?view_op=search_authors&mauthors=Abdulrahman+Alfozan