McDonald's McHire applicant data exposure

IMPLEMENTED NOT REPORTED; INCIDENT JUNE TO JULY 2025 · RETAIL AND HOSPITALITY · US · BAND F · PARTLY PROVED
VERSION 1.0 · PUBLISHED 20 NOVEMBER 2026 · UPDATED 20 NOVEMBER 2026 · FACTS CHECKED 20 NOVEMBER 2026

Security researchers found that McHire, the AI chatbot hiring site used by McDonald's franchisees, accepted the password 123456 on a test account and exposed applicant chat records. Paradox.ai, which runs it, confirmed the flaws and fixed them within hours; it says only five candidates' data was viewed, by the researchers.

ABOUT THIS SYNOPSIS

This is MarLuc's summary and grading of publicly available sources, for information only. It is not investment, legal, financial or professional advice, and should not be relied on for any decision. Readers must validate it against the original sources and, where appropriate, challenge its conclusions.

Facts and figures are as reported by the sources listed below, which may be incomplete, self-reported or out of date. Check the original source before relying on any figure.

The impact band, proof marker and SEAM view are MarLuc's opinion. The organisation is not a MarLuc client and has not reviewed or endorsed this synopsis. Names and trademarks belong to their owners.

NOTICE WORDING LAST UPDATED 16 NOVEMBER 2026

AT A GLANCE

What went wrong: Weak oversight or controls.

AI and automation used: Conversational AI hiring assistant ('Olivia') by Paradox.ai on the McHire site; the researchers said it seemed locked to pre-set responses. The failure was in the platform's ordinary web security..

Implemented: Not reported; incident June to July 2025. Grade: band F, Failure, Partly proved.

Headline result, as reported: Researchers reached McHire applicant records with the password 123456 in June 2025; Paradox.ai confirmed and fixed the flaws, and says five candidates' data was viewed

1 · The case

The facts, as reported by the 5 sources listed at the end. Where a source is silent, the field says "Not reported".

Organisation

McDonald's (McHire, run by Paradox.ai). McDonald's, the US fast food company. McHire is the recruitment site used by 90% of its franchisees, by the researchers' account, built and run by the US hiring software firm Paradox.ai. Canvas block: 8. Governance and risk. Also 6. Data and

Business challenge

The challenge. Not reported. McHire handles high-volume hourly hiring: applicants chat with a bot named Olivia that collects contact details and shift preferences and gives a personality test, by the researchers' account.

How it was addressed. Ian Carroll and Sam Curry looked at McHire after seeing complaints on Reddit about the bot giving nonsensical answers. On a login link for Paradox staff they tried the username and password 123456 and became administrators of a test restaurant, with no multifactor authentication, per Wired. An internal API then let them change an applicant ID number and see other applicants' names, emails, phone numbers, addresses and chats. They estimated more than 64 million records could be reached. They found no published security contact and emailed staff directly, disclosing to Paradox and McDonald's on 30 June 2025. The credentials stopped working that evening and Paradox confirmed both issues fixed on 1 July. Paradox said the test account had not been used since 2019 and should have been decommissioned, and that its penetration tests had not found the flaw. McDonald's told Wired it was disappointed by this unacceptable vulnerability from a third-party provider. [1] [2] [3] [4] [5]

Who implemented it

Paradox.ai (Software vendor): Built and ran the McHire platform and the Olivia chatbot, and fixed the flaws..
Traitify (Software vendor): Powered the personality test in the McHire application flow, per the researchers..
Workday completed its acquisition of Paradox on 1 October 2025.

Technology (SEAM pillar E)

SEAM types: not established; the sources do not say how the system works. Deployment: Vendor SaaS. Vendors and products: Paradox.ai, Traitify, McHire, Olivia (Paradox conversational AI).

Where it was built in: McHire, a Paradox-run client instance for McDonald's, where applicants chat with Olivia and restaurant owners review and step into conversations through an administration interface; a Traitify personality test is part of the flow, per the researchers.

What changed

Before: a Paradox test account with the password 123456 and an API that returned any applicant's record by ID. After: the credentials were revoked, the API was patched, and Paradox said it would publish a security contact and start a bug bounty programme. [1] [2] [3] [4] [5]

Cost of failure

Not reported. No fine, settlement or compensation is reported in the sources. Remediation reported by Paradox: test credentials revoked, the API endpoint patched, a security contact address and a bug bounty programme.

What it saved

Not reported [1] [2] [3] [4] [5]

Governance and control

Paradox said it takes responsibility for the issue, that its penetration tests had not found it, and that the test account should have been decommissioned. McDonald's said it would hold third-party providers to its data protection standards. KrebsOnSecurity reported that malware on a Paradox administrator's device in Vietnam had exposed reused, weak passwords for Paradox accounts of several Fortune 500 clients; Paradox said few were still valid and that it has required single sign-on with multifactor authentication for partners since 2020. No regulator or court action is reported.

S2 · Accountable owner · Claimed
Paradox said it takes responsibility for the issue; McDonald's said it mandated Paradox to fix it and will hold third-party providers to its data protection standards. No named owner is reported. [2] [3]

A1 · Safe use · Not reported
Not reported.

A2 · Human in the loop · Evidenced
The researchers saw that restaurant owners can view and step into Olivia's conversations, and their own application appeared to await human review. [1]

A3 · Monitoring and assurance · Missing (independent source shows it was absent)
A test account unused since 2019 was still live with the password 123456, and Paradox says none of its penetration tests had found the API flaw. [1] [2] [3]

A4 · Vendor AI · Missing (independent source shows it was absent)
McDonald's called the flaw an unacceptable vulnerability from a third-party provider; KrebsOnSecurity reported weak, reused Paradox passwords for several clients' accounts exposed by malware. [3] [4]

A5 · Agent controls · Not reported
No agents described.

A6 · Standards and regulation · Not reported
No regulator or court action is reported in the sources.

What worked, what did not, what is unproven

WORKED

– Once the right people were reached, the flaws were fixed within hours: the credentials stopped working the same evening and Paradox confirmed the fix the next day, by the researchers' account.

DID NOT

– A test account with the password 123456, unused since 2019, was still live, and none of Paradox's penetration tests had found the API flaw, by Paradox's own account.

– The researchers found no published way to report a security problem and had to email staff directly.

– McDonald's described the flaw as an unacceptable vulnerability from a third-party provider.

– KrebsOnSecurity reported that a Paradox administrator's device was infected with password-stealing malware at the end of June 2025, exposing reused passwords for client accounts.

UNPROVEN

– How many applicants were exposed: the researchers estimated more than 64 million records; Paradox says most chat records held no personal information and only five candidates' data was

– Whether anyone other than the researchers used the flaws: Paradox says its records show no third-party access.

– Whether McDonald's changed its contract or oversight of Paradox: Not reported.

Timeline

2019 Paradox test account with a legacy password last logged into, by Paradox's account [2]

Jun 2025 Researchers log in with 123456 and find an API flaw; they disclose it to Paradox and McDonald's on 30 June [1]

Jul 2025 Paradox confirms the flaws are fixed on 1 July and publishes its account on 9 July [2]

Jul 2025 KrebsOnSecurity reports malware on a Paradox administrator's device exposed company passwords [4]

Oct 2025 Workday completes its acquisition of Paradox [5]

2 · Grade and SEAM assessment

MarLuc's opinion, made on the evidence above. How cases are graded: marluc.co.uk/case-studies/how-we-rate

Level of change and impact

Claimed: Not applicable. Grade: F, Failure. Proof: Partly proved. Level of change: Not graded.

No level assessed: band F, a security failure in a live AI hiring platform that exposed applicant data to outsiders. The vendor admitted the failure; the scale is disputed.

Band F because applicants' personal data in a live AI hiring system was open to anyone who found two basic flaws, and outsiders did view it; the vendor admitted the failures and McDonald's called the vulnerability unacceptable. The marker is Partly proved: the flaws are confirmed by the vendor, but the scale of exposure is disputed and no regulator or court has made findings. No fine, compensation or other cost is reported.

The SEAM view and lessons learnt

The failure sat in the vendor's basic security: an old test account and an unchecked API sat on a system holding millions of applicant conversations. High-volume hiring tools gather contact details from people who are waiting to hear from an employer, which the researchers said would make the data valuable for phishing. Before copying the approach, a leadership team should ask how it checks the security of a hiring vendor that holds applicant data under its brand, and who answers for that data when the vendor fails.

1. Audit hiring vendors' security, including test accounts and access controls.
2. Require a published security contact and a bug bounty from vendors.
3. Collect and keep only the applicant data the hiring step needs.

Evidence

Score 2 of 4. Independent researchers' findings confirmed by the vendor and reported by Wired and KrebsOnSecurity; the scale of exposure is disputed and no regulator or court has ruled.

Evaluation method. Independent security researchers' disclosure, confirmed by the vendor's own statement and McDonald's statement to Wired; Wired contacted two exposed applicants, who confirmed their applications. No regulator or court finding.

Sources disagree. The researchers estimated more than 64 million applicants' data could be retrieved and Wired reported as many as 64 million records; Paradox says the records were chat interactions, not job applications, that most held no candidate personal information, and that seven records were downloaded, five with personal data. Paradox says the incident affected one client instance; KrebsOnSecurity reported separate exposure of passwords for Paradox accounts of other Fortune 500 clients, which Paradox said were mostly no longer valid. The researchers say 90% of McDonald's franchisees use McHire; Wired says many of them do.

Status. Closed for the June 2025 flaws, which Paradox says were fixed by 1 July 2025. No regulator or court action is reported. Workday completed its acquisition of Paradox on 1 October 2025.

3 · Original sources

Read these in full. To challenge a fact or a grade, use the contact form at marluc.co.uk or the link on https://marluc.co.uk/case-studies/mcdonalds-mchire-paradox-applicant-data-exposure

[1] Ian Carroll: Would you like an IDOR with that? Leaking 64 million McDonald's job applications (July 2025)
https://ian.sh/mcdonalds

[2] Paradox: Responsible Security Update (July 2025)
https://www.paradox.ai/blog/responsible-security-update

[3] Wired: McDonald's AI Hiring Bot Exposed Millions of Applicants' Data to Hackers Who Tried the Password '123456' (July 2025)
https://www.wired.com/story/mcdonalds-ai-hiring-chat-bot-paradoxai/

[4] KrebsOnSecurity: Poor Passwords Tattle on AI Hiring Bot Maker Paradox.ai (July 2025)
https://krebsonsecurity.com/2025/07/poor-passwords-tattle-on-ai-hiring-bot-maker-paradox-ai/

[5] Workday: Workday Completes Acquisition of Paradox (October 2025)
https://newsroom.workday.com/2025-10-01-Workday-Completes-Acquisition-of-Paradox

McDonald's (McHire, run by Paradox.ai) website: https://www.mcdonalds.com

Version 1.0 · Published 20 November 2026 · Updated 20 November 2026 · Facts checked against sources 20 November 2026 · Downloaded 26 November 2026. This PDF may be out of date: the latest version, and a way to report an error or a better source, is at https://marluc.co.uk/case-studies/mcdonalds-mchire-paradox-applicant-data-exposure

VERSION HISTORY

v1.0 20 November 2026 First published