

RESEARCH

HOW NORTH KOREA OUTSOURCES JOB FRAUD AT SCALE

DPRK operators are paying gig workers five to ten cents a job application, plus a bonus per interview secured. An account of that bidding network from inside its Discord channels, and of the Gmail architecture that keeps applying separate from impersonating.

CONTENTS

HOW NORTH KOREA OUTSOURCES JOB FRAUD AT SCALE

Origins of the Investigation and How Access Was Obtained	3
The Bidding Network and How It Operates	3
Device Constraints and Organizational Structure Among Bidders	4
Internal Disputes Over Pricing, Quotas, and Bid Qualification	4
How Application Accounts Are Created and Managed	6
Inside the Shared Documents Extracted from the Network	7
The Use of AI and Programs to Achieve Efficiency	8
Indicators of Compromise	9

EDITOR'S NOTE

This investigation was conducted using open-source intelligence techniques, including the monitoring of GitHub profiles linked to previously identified DPRK-affiliated actors, to surface new indicators and associated infrastructure. Infiltration of the associated Discord groups, servers, and direct message channels was conducted passively — I did not compromise any systems or participate in any form of fraud. Some indicators associated with identified personas are being withheld intentionally as a deliberate effort to collect additional indicators; employers who believe they may have been impacted by one of these individuals are encouraged to reach out directly to intel@haydenmckenzie.com.

Origins of the Investigation and How Access Was Obtained

This investigation originated from the open-source monitoring of GitHub profiles that were associated with a cluster of accounts [previously identified](#) as DPRK-affiliated. Routine observation of that cluster for new activity and associated accounts surfaced a GitHub profile linked to one of the profiles in the previously mentioned article.

Using identifiable information derived from those profiles, as well as some social engineering, access was obtained to Discord servers, groups, and direct message threads associated with the individual. Materials collected through that access included chat logs, operational spreadsheets, screenshots of documents, and a tutorial video demonstrating how bidders use AI to submit applications efficiently.

During an initial review of the Discord servers, one post from the subjects account was notable as it proved that their profile was being used for more than just bidding. The account had requested assistance with the following:

"I am looking for a reliable and trustworthy individual to assist with moving items from my company office to my personal residence."

This request is documented here not for its significance in the bidding network, but to demonstrate that each of these accounts are used for a variety of tasks.

The Bidding Network and How It Operates

The core component here is an outsourced service used to speed up the application process by using cheap labor.

Rather than applying to jobs themselves, the DPRK workers (I'll call them "buyers") recruit third-party "bidders" to submit applications on their behalf. These bidders are not contractors in any legal sense, they are gig workers that are paid per application submitted.

The rates I observed ranged from **\$0.05 to \$0.10 per application**, with the variance determined by a few factors:

- **Interview rate:** The percentage of submitted applications that result in an interview invitation. Bidders with higher interview rates command higher per-bid prices and are eligible to earn bonuses for each interview they score.
- **Spreadsheet upkeep:** More on this below, but bidders are expected to maintain detailed logs of their activity. Accuracy and consistency are priced in.
- **Work history:** Before being brought on, a prospective bidder is expected to provide examples of previous work — essentially a portfolio of prior application campaigns. These portfolios often included work done for *other* personas, and in several cases, bidders shared materials that included their **old personas** — prior fake identities they had managed for previous buyers.

The bonuses rewarded to bidders for scoring interviews ranged from **\$1 to \$3** depending on the company, position, salary, and location. It was often stressed that bidders must apply for remote-only jobs, however, bidders would still get paid a bonus for interviews that offer on-site positions only.

Payments to bidders are made in USDT over the BEP20 network (Binance Smart Chain).

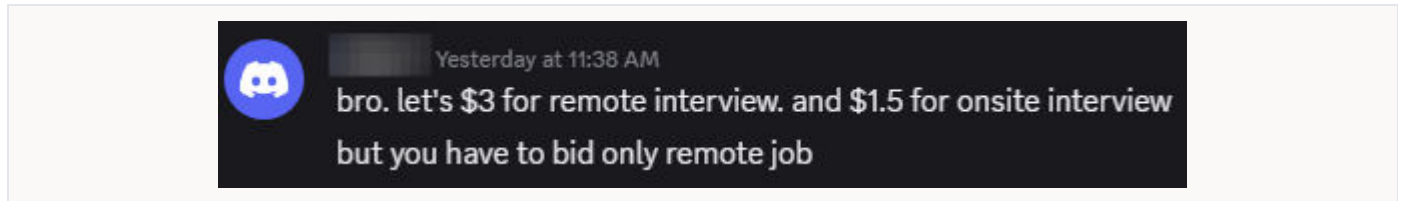


FIG. 01 | Buyer specifies interview bonus rates.

Device Constraints and Organizational Structure Among Bidders

Bidders in this network operated with a variety of hardware and organizational structures. A few of them worked exclusively from mobile devices, conducting all of their activity — including job board navigation and application submissions — through a mobile browser. Some bidders, however, were not operating alone; they managed multiple profiles with the assistance of small teams. The majority appeared to be working independently from a personal laptop or computer.

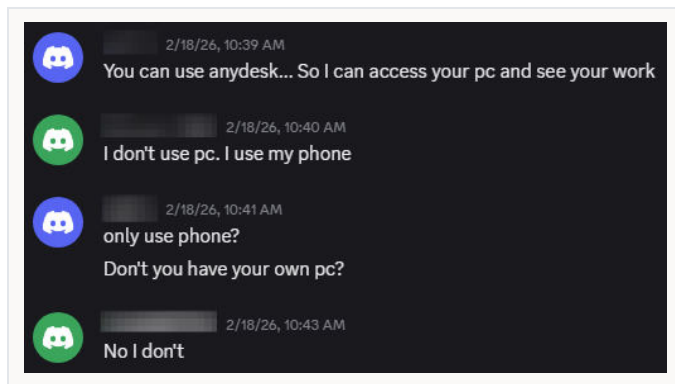


FIG. 02 | Bidder only uses their phone for applications.

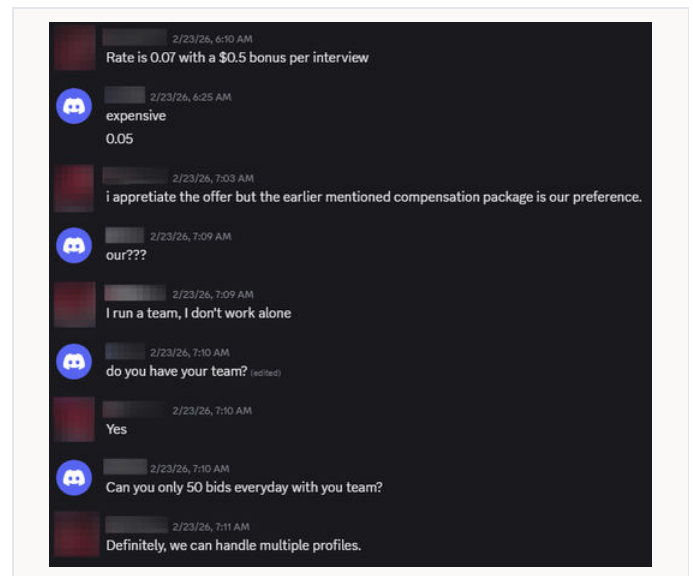


FIG. 03 | Bidder has a team that manages multiple portfolios.

Internal Disputes Over Pricing, Quotas, and Bid Qualification

The per-application rate structure and the interview bonus amounts were a recurring source of conflict. Chat logs documented constant friction between buyers and bidders, with bidders regularly pushing for higher rates and buyers resisting. Disputes centered on the same performance metrics used to set rates — interview yield, spreadsheet accuracy, and resume tailoring — with buyers and bidders frequently disagreeing on whether those benchmarks had been met.

There were also definitional disputes over what constituted a qualifying bid or interview: whether applications submitted to already-closed postings counted, and whether generic submissions without role-specific resume adjustments met the standard.

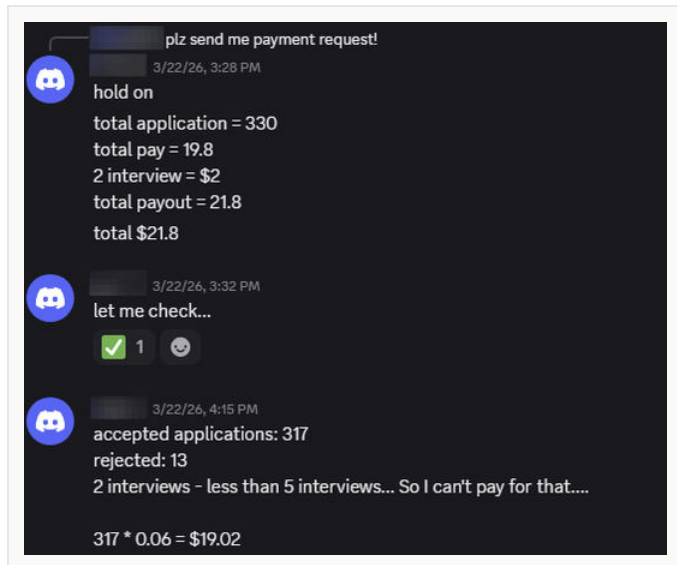


FIG. 04 | Bidder is discussing total payout with the buyer

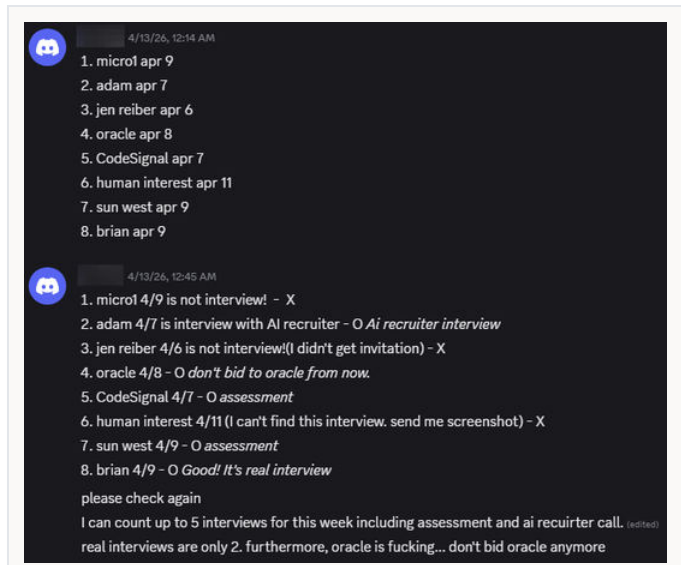


FIG. 05 | Buyer argues with the bidder on the types of interviews scored.

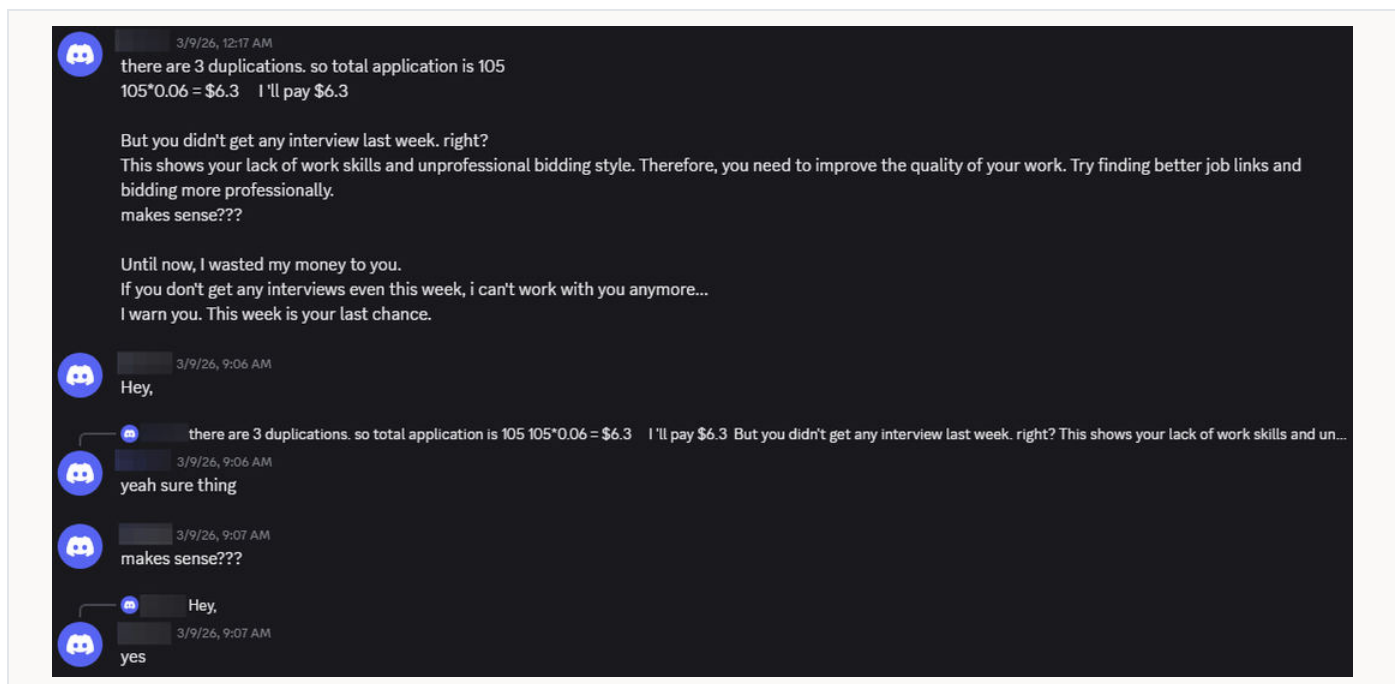


FIG. 06 | Buyer argues with the bidder on quality of work and wasted money.

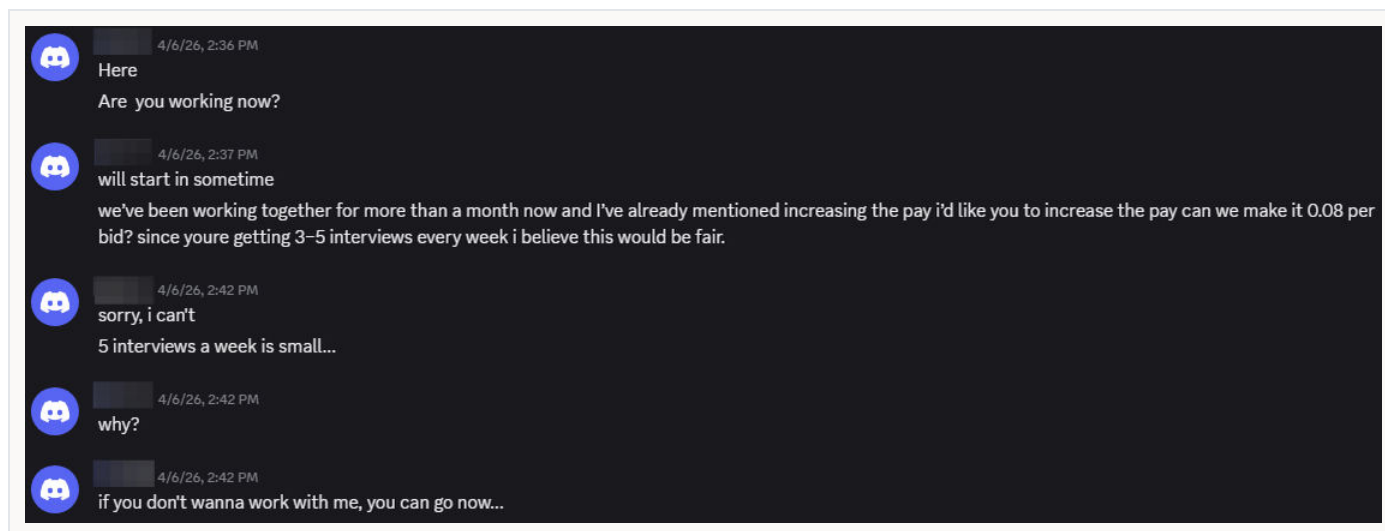


FIG. 07 | Buyer rejects request for a raise based on quality of work and interviews scored.

The bidders were told to focus on positions in software engineering, DevOps, and cloud infrastructure roles. Based on the communications observed, target salary ranges were:

- **Hourly:** \$60–\$70/hour
- **Monthly:** \$8,000–\$12,000/month
- **Annual:** \$120,000–\$150,000+

These figures are consistent with published U.S. government estimates of DPRK IT worker earnings. A single successful placement, maintained for a year, generates more than enough to justify the entire bidder network.

How Application Accounts Are Created and Managed

Their email setup is operationally clever and built by repurposing legitimate Google features for efficiency.

Here's the workflow:

1. **The bidder creates a new Gmail account** for the buyer's persona. This step is specifically assigned to the bidder rather than the buyer for a practical reason: DPRK workers face restrictions on how many Gmail accounts they can create using purchased phone numbers for verification. By pushing account creation to the bidder, the buyer sidesteps that ceiling.
2. **Gmail forwarding is configured** so that all incoming mail to the persona's address — interview requests, application confirmations, recruiter follow-ups — is automatically routed to a **central email address held by the buyer**. The bidder sets this up before handing over the account.
3. **The bidder sends applications as the persona** from that address. All replies flow to the buyer without further involvement from the bidder.
4. **The buyer conducts interviews** using the persona's identity, with the persona's email address, from the central account. The bidder's job is done once the interview is scheduled.

In some instances, the buyer was seen using the bidders freshly created Gmail account to bid on applications themselves — particularly when the bidders performance is subpar. In addition to bidding on applications themselves, they'll occasionally train the bidders if they aren't getting enough business from other bidders.

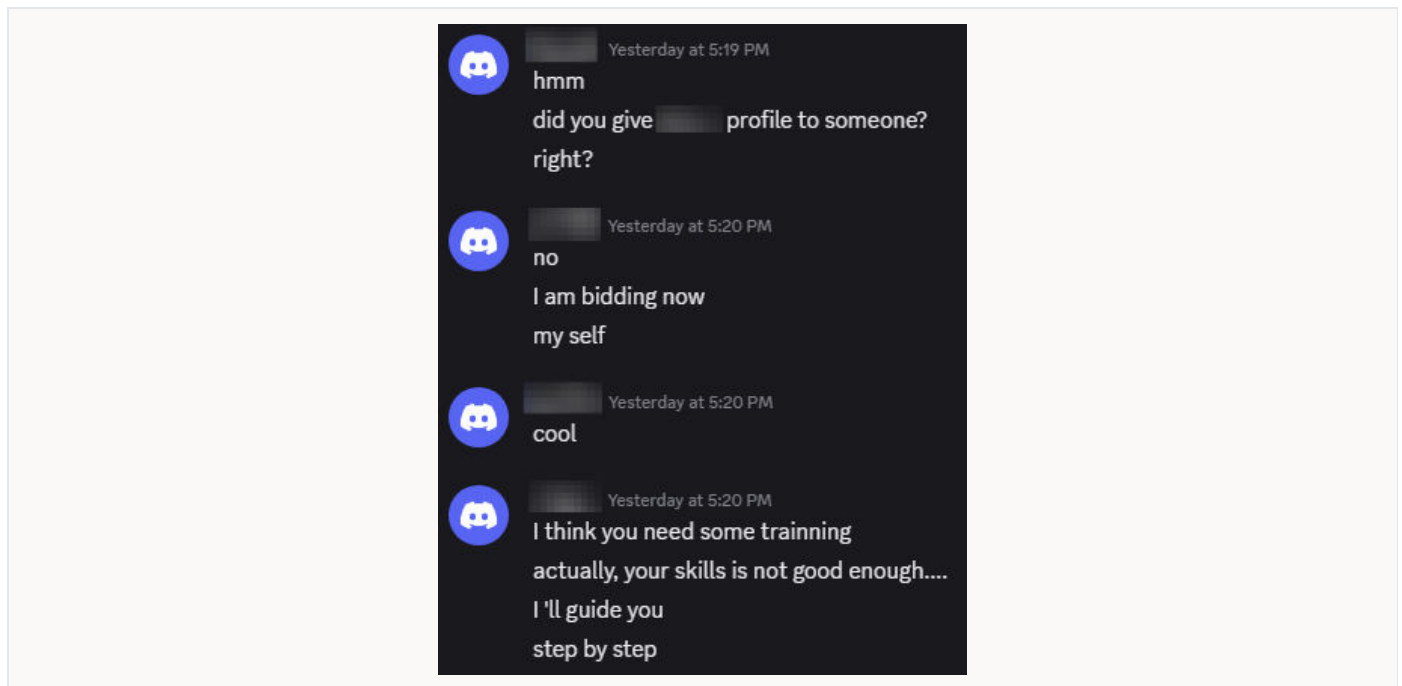


FIG. 08 | Buyer started using the bidders Gmail account to bid on applications themselves then offered to improve their application skills.

This architecture separates the labor of application submission from the labor of impersonation. The bidder never needs to be able to impersonate a senior software engineer. They just need to be able to submit applications at volume and configure a forwarding rule.

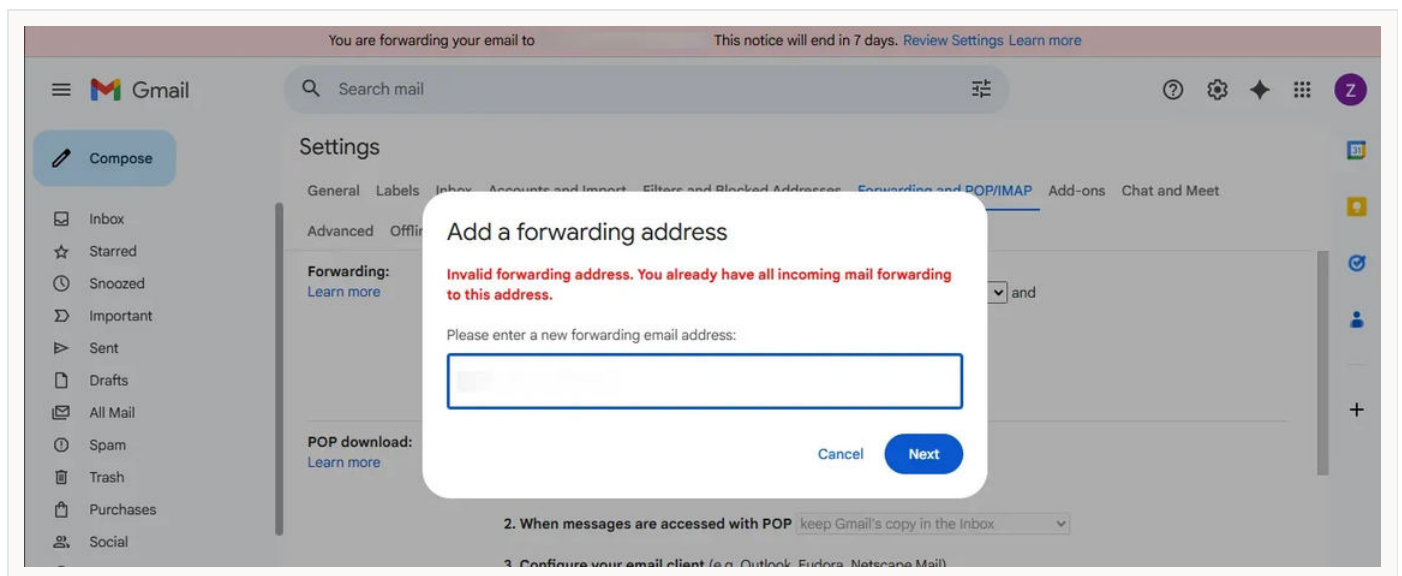


FIG. 09 | 4.2 Screenshot shared between buyer and bidder as there were issues setting up email forwarding.

Inside the Shared Documents Extracted from the Network

The operational documents I was able to extract varied in professionalism and organization.

Their spreadsheets systematically track job applications by sequential number, company, job title, posting URL, tech stack, resume variant, and application status — managed through a structured dropdown and color-coded classification system. In addition, many spreadsheets include bidder assignment and audit columns, indicating clear role separation per bidder.

	A	B	C	D	E	F	G
1	S/N	Job Title	Company Name	Job Description Link	Main Skill / Stack	Resume	Confirmation
140	36	Senior Front-End Web Developer/Engineer - JavaScript/React/NextJS	Integrity Web Consulting	https://jobs.smartrecruiters.com/IntegrityWeb	Front-End / React	Skill	Applied
141	37	Senior Frontend Engineer	CircleIn	https://jobs.smartrecruiters.com/CircleIn/7438	Front-End / React	Skill	Applied
142	38	Senior Front End Application Developer - Javascript / React / Angular	Xenetix Software, LLC.	https://jobs.smartrecruiters.com/XenetixSoftw	Front-End / React	Skill	Applied
143	39	Senior Front End Application Developer	Digital Forge Cyber Assurance Group	https://jobs.smartrecruiters.com/DigitalForge	Front-End / React	Skill	Applied
144	40	Senior Front-end Engineer (Remote)	Flip To, Inc.	https://app.trinethire.com/companies/31689-fl	Front-End / React	Skill	Applied
145	41	Senior Java Microservices Developer	Klap6	https://jobs.smartrecruiters.com/klap6/743998	Java	No Skill	Applied
146	42	Senior Software Engineer, Java Backend	NinjaOne, LLC	https://ninjaone-llc.hirehive.com/senior-sofw	Java	No Skill	Applied
147	43	.Net Full stack Developer w/ Angular & / Sky Solutions LLC.		https://jobs.smartrecruiters.com/SkySolution	C# & .Net	No Skill	Applied
148	44	Senior Software Engineer (C# and .NET)	Cambium Assessment	https://cambiumlearning.wd1.myworkdayjobs	C# & .Net	No Skill	Applied
149	45	Back-End Developer (Java)	RIT Solutions	https://www1.jobdiva.com/portal/?a=xbjdnwgj	Java	No Skill	Applied
150	46	JAVA BACKEND ENGINEER	undisclosed	https://jobs.smartrecruiters.com/Undisclosed	Java	No Skill	Applied
151	47	Backend Developer [Java Spring Boot]	Pandera Systems	https://jobs.smartrecruiters.com/PanderaSyst	Java	No Skill	Applied
152	48	Senior Software Engineer	Shift Left Ltd	https://shiftleft.bamboohr.com/careers/9	Full Stack	Skill	Applied
153	49	Sr. Java Full Stack Developer (Remote)	nanoSoft Consulting	https://nanosoftconsulting.freshteam.com/job	Java	No Skill	Applied

FIG. 10 | An organized spreadsheet used by the bidders to document applications.

%	Company Name	Tr	Job Title	Tr	Job URL	State	Resume	Bidder	Checked	Reason
	Apple		Gen AI Software Engineer		https://www.indeed.com/q-staff-gen-ai-eng				Reject	
	Apple		Staff Machine Learning Engineer – AI In		https://www.indeed.com/q-staff-gen-ai-eng				Reject	
	Apple		AI/LLM Network Software Development		https://www.indeed.com/q-llm-ai-l-kent-wa	Applied			Reject	
	HackerOne		Software Engineer – Applied AI		https://www.indeed.com/q-llm-ai-l-kent-wa	Applied			Reject	
	Meta		Research Engineer – RecSys / ML		https://www.indeed.com/q-llm-ai-l-kent-wa	N/A			Reject	
	Autonomize AI		ML/LLM Engineer – Applied AI		https://www.indeed.com/q-ai-llm-engineer	Applied				
	Sema4.ai		Staff Engineer – AI		https://www.indeed.com/q-ai-engineer-llm	N/A			Reject	
	Waymo		Senior Research Scientist – Foundation		https://www.indeed.com/q-large-language	Applied			Reject	
	Forterra		Senior/Staff AI Engineer – Large Language		https://www.indeed.com/q-large-language	N/A			Reject	
	Zoom		Staff Machine Learning Engineer – Effic		https://www.indeed.com/q-llm-prompt-eng	N/A				
			Job Title		https://www.indeed.com/q-artificial-intellig				Reject	
	ServiceUp		Software Engineer – AI-Driven Workflow		https://www.indeed.com/q-artificial-intellig				Reject	
	NewsBreak		AI Engineer		https://www.indeed.com/q-artificial-intellig				Reject	
	Optum		Senior Software Engineer – AI-Augment		https://www.indeed.com/q-artificial-intellig				Reject	
	Candid Intelligence		Software Engineer – Full Stack		https://www.indeed.com/q-full-stack-ai-eng					
	Stratus Data Systems		Senior AI/ML Software Engineer – Remc		https://www.indeed.com/q-ai-engineer-l-rei				Reject	
	SuperDial		Lead AI/ML Scientist – Remote		https://www.indeed.com/q-ai-engineer-l-rei				Reject	
	Capgemini		Founding AI Engineer – Multimodal & Ag		https://www.indeed.com/q-ai-engineer-llm				Reject	
	Eden Prescott		AI & Agentic Systems Engineer		https://www.indeed.com/q-ai-engineer-llm				Reject	
	Nixon Peabody LLP		Applied AI Engineer – Healthcare LLM		https://www.indeed.com/q-ai-engineer-llm				Reject	
			GenAI Engineer (LLM/RAG)		https://www.indeed.com/q-artificial-intellig				Reject	
			AI/LLM Software Engineer		https://www.indeed.com/q-artificial-intellig				Reject	

FIG. 11 | An organized spreadsheet used by the bidders to document applications.

The Use of AI and Programs to Achieve Efficiency

Among the materials extracted from this investigation is a [screen-recorded video](#) produced by a bidder, apparently recorded to demonstrate their workflow to a prospective buyer. The video documents the full application process for a single role submitted through Workday, one of the most widely used enterprise applicant tracking systems.

The process shown in the video proceeds as follows: the bidder opens ChatGPT and pastes in the job description alongside their current resume, prompting it to identify gaps and suggest tailored language. They then move to ResumeKit — a resume optimization tool designed to match resume content against job description keywords.

From there, the bidder navigates to the Workday application portal, populates the required fields using the tailored resume, and completes the submission.

The video is notable for a few reasons. It demonstrates that at least some bidders are not submitting generic, unmodified applications at volume — they are using widely available AI and resume optimization tools to improve their interview yield on a per-application basis, which is consistent with the tiered pricing structure documented elsewhere in this report.

Appendix | Indicators of Compromise

The following indicators are published to assist security teams, employers, HR platforms, and researchers. This list will be updated as the investigation continues.

Note on email addresses: Email addresses associated with these personas and accounts are being withheld at this time as an active collection effort is ongoing. If you believe your organization may have employed one of these individuals, please reach out directly — contact information below.

If you believe your organization may have employed one of these individuals and would like to request additional information, or if you have information relevant to this investigation, feel free to reach out at intel@haydenmckenzie.com

Hayden McKenzie · Independent Security Researcher

haydenmckenzie.com · intel@haydenmckenzie.com · [Substack ↗](#) · [LinkedIn ↗](#) · [CV ↗](#)