

RESEARCH

THE WOMEN BEHIND NORTH KOREA'S IT WORKER OPERATIONS

An exclusive interview with a first-time female operative, alongside day-to-day operations conducted throughout her first three weeks inside a DPRK IT worker cell.

THE WOMEN BEHIND NORTH KOREA'S IT WORKER OPERATIONS

Executive Summary	3
Key Insights	3
Notable Findings	3
Introduction	4
Meet The Team	4
Origins & Locations	5
Key Figures	6
Orientation	7
Assignment	8
Profile Creation	9
Email Significance	10
Pipe Dream	13
MageHire	13
Operations	15
Tracking	16
Company A	16
Initial Interview	17
Interview Preparation	18
AI Assistance	19
Behind The Scenes	20
Rejection	21
Fallout	22
Damage Control	22
Exclusive Interview	24
Conclusion	27
Appendix A: Roles and Terms	28
Appendix C: Indicator Register	28
Previous Reporting	29

MEDIA

This report contains 5 video clips and 1 audio recording that a PDF cannot play. The clips appear here as stills and the recording as a marker. Every one of them plays in full in the online edition of this report:

haydenmckenzie.com/research/dprk-it-worker-cell-part-one

EDITOR'S NOTE

This investigation was conducted by establishing myself within a North Korean worker group through social engineering, which produced invitations to the two Slack workspaces described below. I did not compromise any systems, use any credentials, or participate in any form of fraud. Some indicators associated with identified personas or businesses are being withheld intentionally for privacy reasons; employers who believe they may have been impacted by one of these individuals are encouraged to reach out directly to intel@haydenmckenzie.com.

Executive Summary

The following report tracks a young woman and first-time operative **Jasmine** through her first few weeks inside a North Korean IT worker cell and documents the trainings she received, the personas she was assigned, the account-building tasks she was given, and the live interview she underwent within days of being onboarded. Jasmine was not the only woman in the cell — two others, **Scarlet** and **Whisper**, appear alongside her throughout — and the personas she's tasked with developing focus solely on female attributes. The investigation also uncovers a U.S. staffing agency that fronts the cell's placements, and dives into many hardships the cell faced as a result of Jasmine's presence.

The fraudulent staffing agency uncovered by cell operations is known as **MageHire**, a U.S.-based company that claims to provide AI automation and backend engineering personnel for tech-based startup companies. I maintain with high confidence that MageHire is a front company for this cell and that its CEO, a U.S. citizen, is the cell's American facilitator: he places the operatives with clients under false identities, maintains the client relationships, and covers for operatives when placement opportunities fail.

Key Insights

- Jasmine had **no technical skills and zero interview experience** of any kind, yet within days of arrival she was assigned a persona, handed a two-to-three-week account-building quota, and booked in front of a client CEO.
- She was recruited as a **caller** — an operative chosen for spoken English to attend interviews and client meetings — not a developer. The technical work went to operatives already contracted by the same client.
- She is also **one of three women** assigned to the cell and was tasked with developing hundreds of personas strictly tied to female identities.
- The cell maintains two Slack workspaces: **mphteam**, where the North Korean operatives talk among themselves with no facilitators or brokers present, and **MageHire**, the front-facing workspace where they interact with their U.S. facilitator and run job profiles, interviews, and placements.
- A member list uploaded on August 13 places **nine active operatives in Shenyang and Dalian**, with two former members in Russia, and presents them as Chinese, Japanese, and Russian.
- The cell's own motto for continuous account rebuilding is "**injogogi spirit**," named for a North Korean famine-era dish made from pressed soybean residue, used internally and without translation.

Notable Findings

- A shared workbook staged roughly **1,200 identities across eight country tabs** — every one of them female and one born between 1995 and 1998 — with birthdays generated hundreds of rows ahead of the names that will carry them.
- The ninth tab of the shared workbook, **US_REAL**, holds the date of birth, identification number, home address, phone number, bank account and routing numbers, and credit score of **three real American women**, two of them in Florida.
- Employment histories are generated from a fixed AI prompt whose rules include "**No U.S. companies**," deliberately manufacturing a work history that a North American employer would struggle verifying domestically.

- The persona's entire biography — university, home address, and a timed five-minute interview introduction — were **produced through multiple ChatGPT conversations** and shared to the team channel as resumes were written.
- Two operatives, who've already embedded themselves within their main client, bill Okta and Auth0-related work against that client's own customers, all while one of them states internally that **he has no Auth0 experience at all**.

Introduction

Jasmine Bell arrived in the cell's internal workspace as a new recruit with no work history — which her mentor states directly — and behaves as such: **constant questions, job-related insecurities, panicked apologies, and frequently mentioning that she's not "an adult" yet**. When introducing herself to one of the operatives, she addresses herself as "a new female dev."

Further discussion proved that she was not a developer, and shortly afterwards she corrected herself. The cell splits its operatives into callers and developers: **callers are chosen for spoken English and take the interviews and client meetings, and developers do the technical work behind them**.

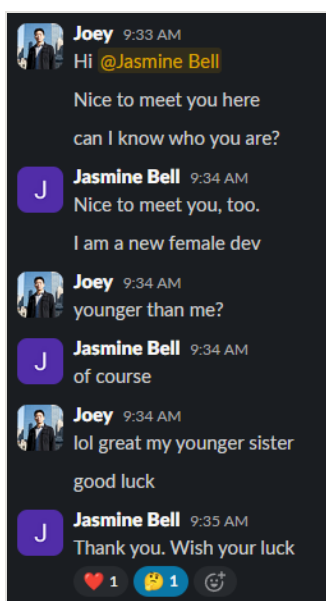


EXHIBIT 01 "A new female dev"

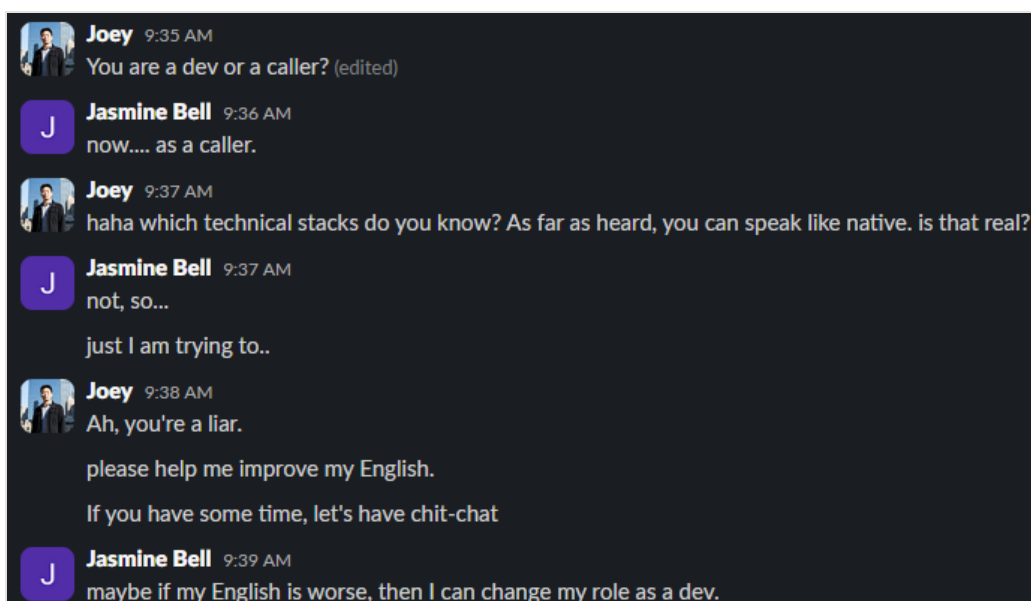


EXHIBIT 02 Caller, not developer

Meet The Team

The cell maintains their own workspace separate from brokers and facilitators. **mphteam** (mphteamworkspace.slack.com) is their internal workspace where every member is North Korean, and no foreign partners are permitted. **MageHire** (magehiregroup.slack.com) is the front-facing workspace, shared with MageHire's CEO, where the cell converses with its U.S. facilitator and maintains job profiles, interviews, and placements; the cell's own team lead calls it "my client's slack."

mphteam's [#general](#) lists **33 members with 8–15 active in a month**, which points to a stack of dormant or retired accounts. Channels include [#english](#) (11 members), [#resume](#) (6), [#used-real-infos](#) (7), and a private [team4](#) (4) — suggesting that there's either been four historical projects or that the cell operates at least four working teams.

Members use cartoon and AI-generated avatars, self-assigned titles ("Senior Recruiter," "SWE," "Odd Eye"), and in several cases duplicate accounts under one name. Three separate accounts carry the name Victor, and two carry Rakal.

Purpose	Internal, operatives only	Client-facing, shared with the facilitator
Created	June 9, 2023	July 16, 2022
Messages (all-time)	27,002	190,583
Monthly active users	8–15	6–10

AS OF SEPTEMBER 15, 2026.

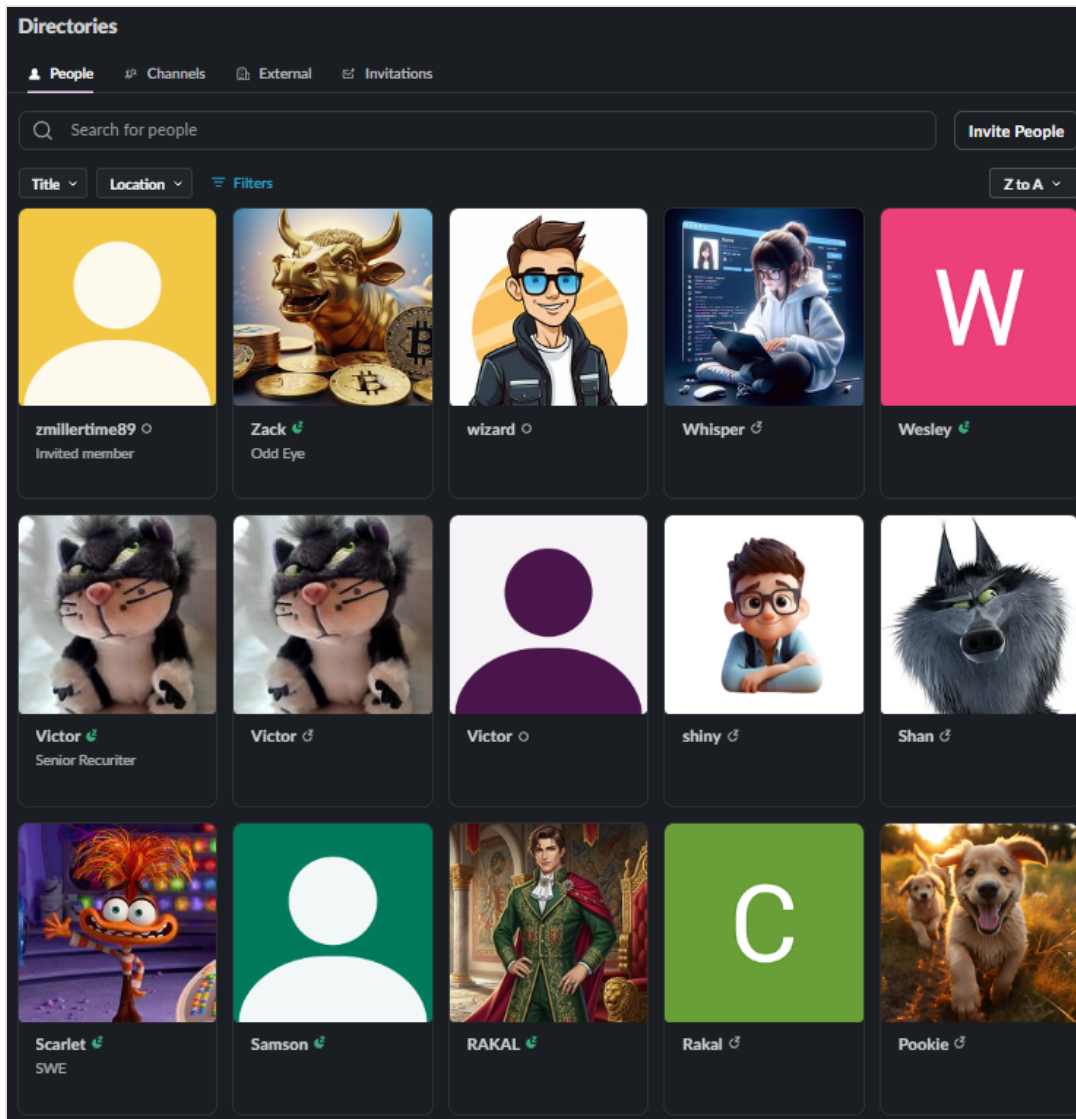


EXHIBIT 03 Member directory

Origins & Locations

The team's lead was observed reposting a member list taken from another operative, captioned as what had been shared with MageHire's CEO, and **documents the origin and location of each member within the cell.**

- **Shenyang, China:** Joy/Joey, Eddie, Timon, Zack
- **Dalian, China:** Leo, Kei, Lucas, Shiny, Shine
- **Russia, no longer active:** Victor, Alex

Stated origins are Chinese, with one Japanese (Kei) and two Russian. These locations are consistent with industry reports, and in my own conversations with North Korean operatives, Shenyang and Dalian were commonly mentioned when talking about team bases.

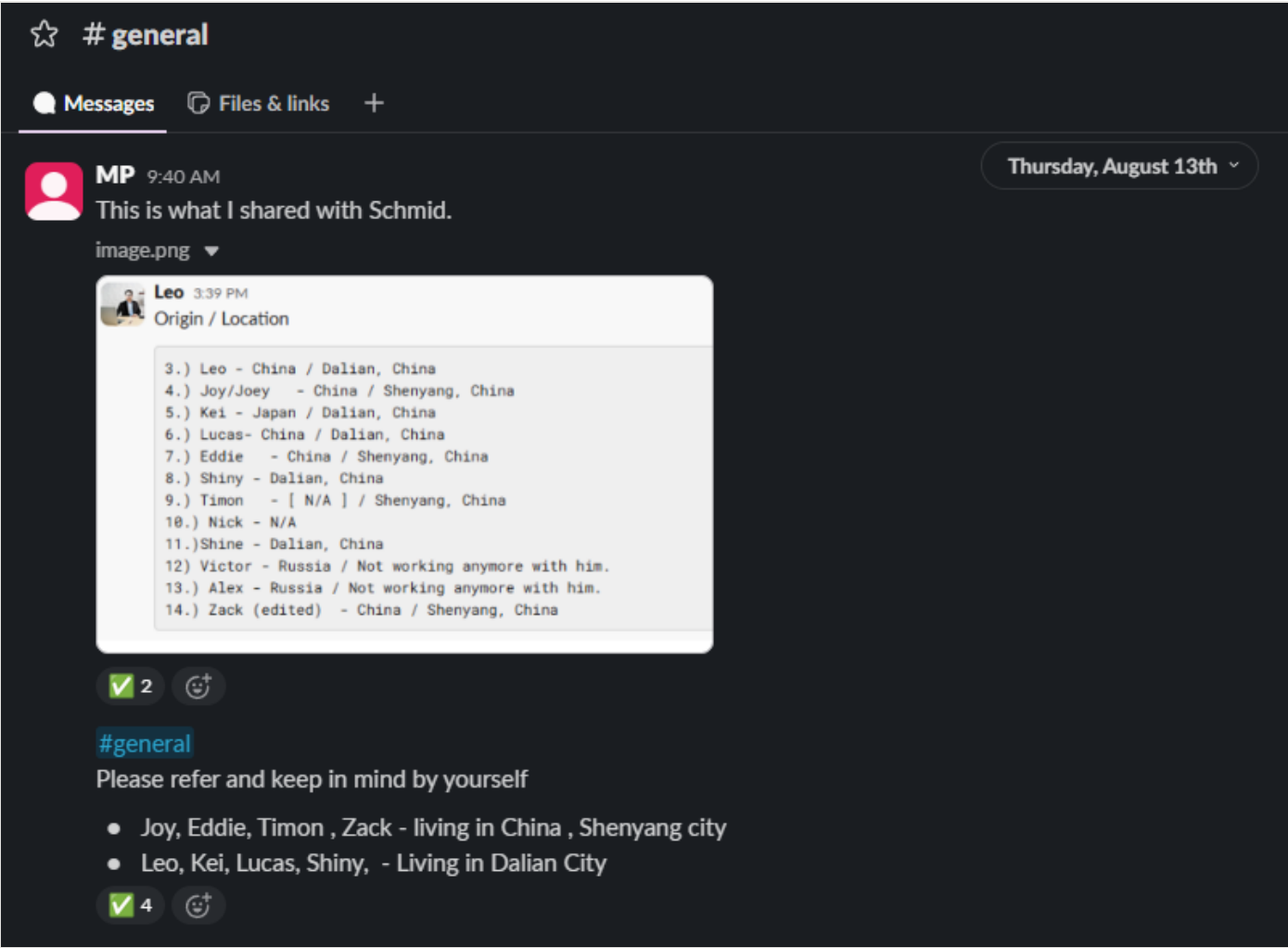


EXHIBIT 04 Stated locations

Key Figures

HANDLE	ROLE IN THE OPERATION
MP	Team lead. Assigns Jasmine's work and holds the cell's line to MageHire's CEO
Dark	Runs account creation, proxies, and profile generation inside mphteam
Leo	Team leader in the MageHire workspace, listed in Dalian — and presented publicly as MageHire's CTO
Joey	Placed at the client, listed in Shenyang
Kei Haruto	Placed at the client, listed as Japanese, in Dalian

HANDLE	ROLE IN THE OPERATION
Scarlet	Operative. Ten months in before her own first live interview, and Jasmine's closest peer
Whisper	Operative. Appears as a friend of Jasmine's; role in the operation unclear
Jasmine Bell	First-time caller, and the subject of this report
Schmid Payen	The cell's U.S. facilitator. Runs MageHire, holds the client relationships, and is not a member of mphteam

Their work moves through a short and efficient chain of command. It appeared that **MP was responsible for maintaining the cell's relationship with MageHire's CEO** and relays all of his demands back to the cell. The CEO is the cell's American face and typically only talks to placed developers in the MageHire workspace.

Newcomers are looked after by the operatives who arrived before them. Scarlet, whose own first interview with a real person came only after ten months in the cell, **tells Jasmine she is lucky to be starting where she did**. Members are also encouraged to practice their English on material posted in the `#english` channel: six *Friends* transcripts, shared by one member in March 2025.

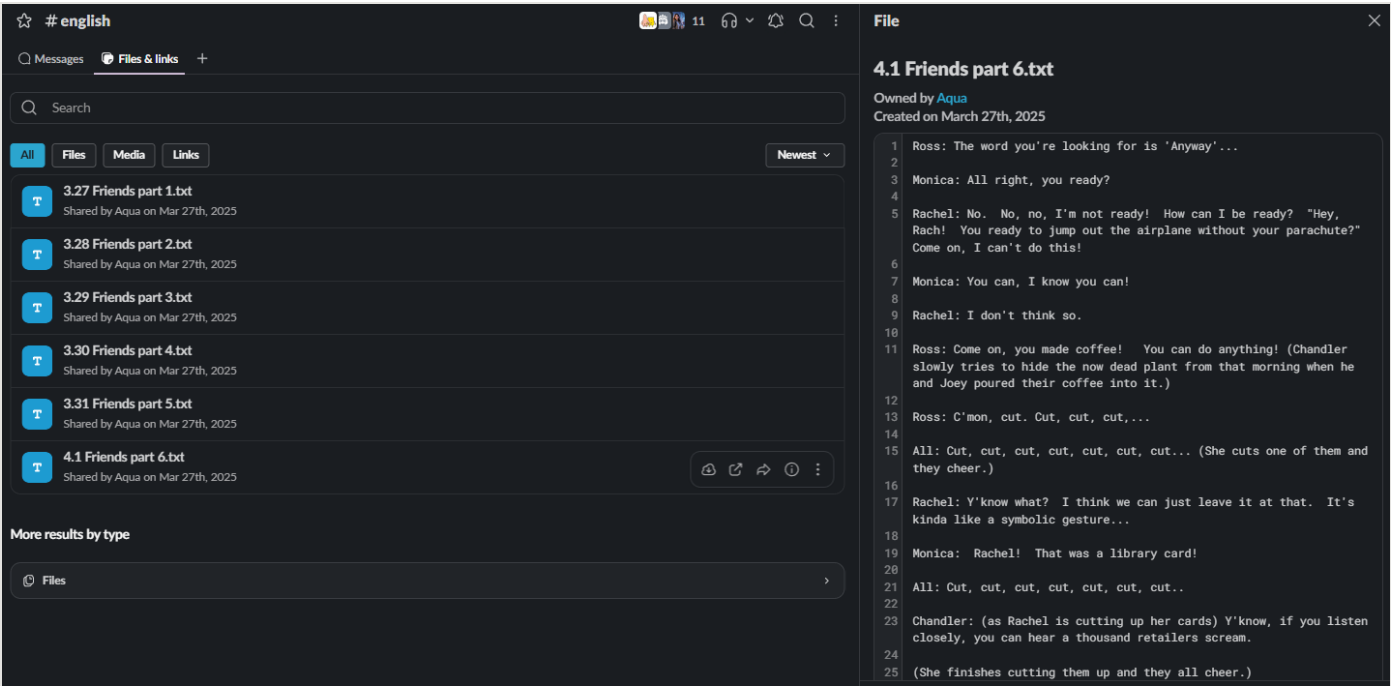


EXHIBIT 05 English study material

Orientation

Jasmine's onboarding happened in mphteam, and most of it happened in the `team4` channel, under Dark. This channel is where the team keeps its goals and objectives, works through payments and deadlines, and uploads files and spreadsheets the cell runs on — **Jasmine's training material among them**. It's important to note that `team4` is strictly used for DPRK operations and does not discuss activity associated with MageHire. In the last couple of weeks the following training samples, originally meant for Jasmine, were collected and analyzed:

- Best practices for bidding on and building mailboxes for future LinkedIn profiles
- Guides for building a persona and keeping it consistent across every account it holds

- ChatGPT logs, used both for persona biographies and for interview scripts
- Setup and correct use of ixBrowser, the proxied browser the accounts live in
- SlyNumber registration and configuration for account verification purposes
- Interview preparation materials before a call, and the coaching after it
- Instructions and best practices for establishing a cryptocurrency wallet

Jasmine was not expected to know anything upon arrival; discussion between members show that she was simply **expected to follow guides, ask for assistance, and produce accounts in bulk.**

Additionally, Jasmine never had the opportunity to create her own identity, instead, she was forced to pick from a predetermined list of names provided by the team's lead. Once she had selected "Jasmine Bell" to be her alias, she was asked to change the name listed on her current email address — this shows that **MP's set of names were strategically used to maintain Jasmine's current email address** which already started with the initials `jib.....@gmail.com`.

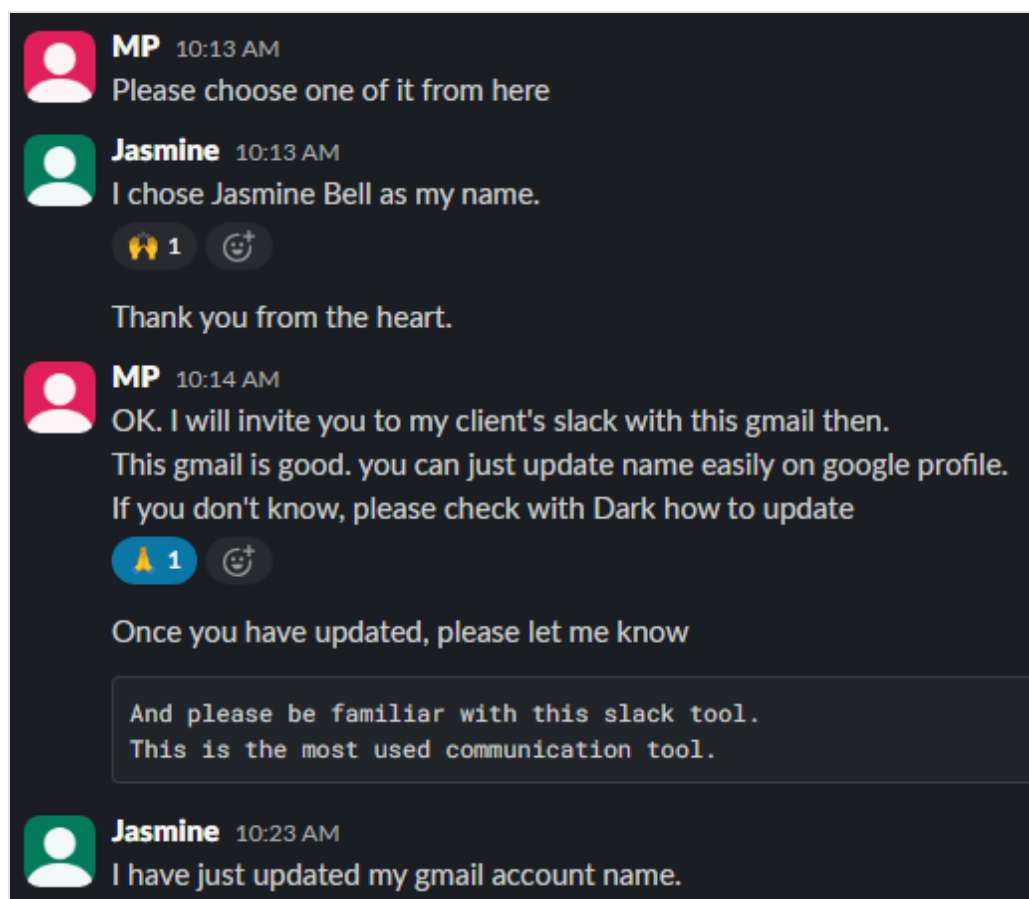


EXHIBIT 06 Choosing a persona

Assignment

Shortly after being onboarded, Dark handed Jasmine her first assignment: build mailboxes and LinkedIn profiles that will be used for future applications. He acknowledges that it will be boring, but explained why tasks like these were important. When an operative gets offered a job, having a backlog of profiles to choose from helps significantly with the verification process. It's typically too troublesome trying to creation U.S.-based LinkedIn profiles — which is why Dark asks Jasmine to focus on European identities. He states that after fifteen to twenty days, it'll start to pay off.

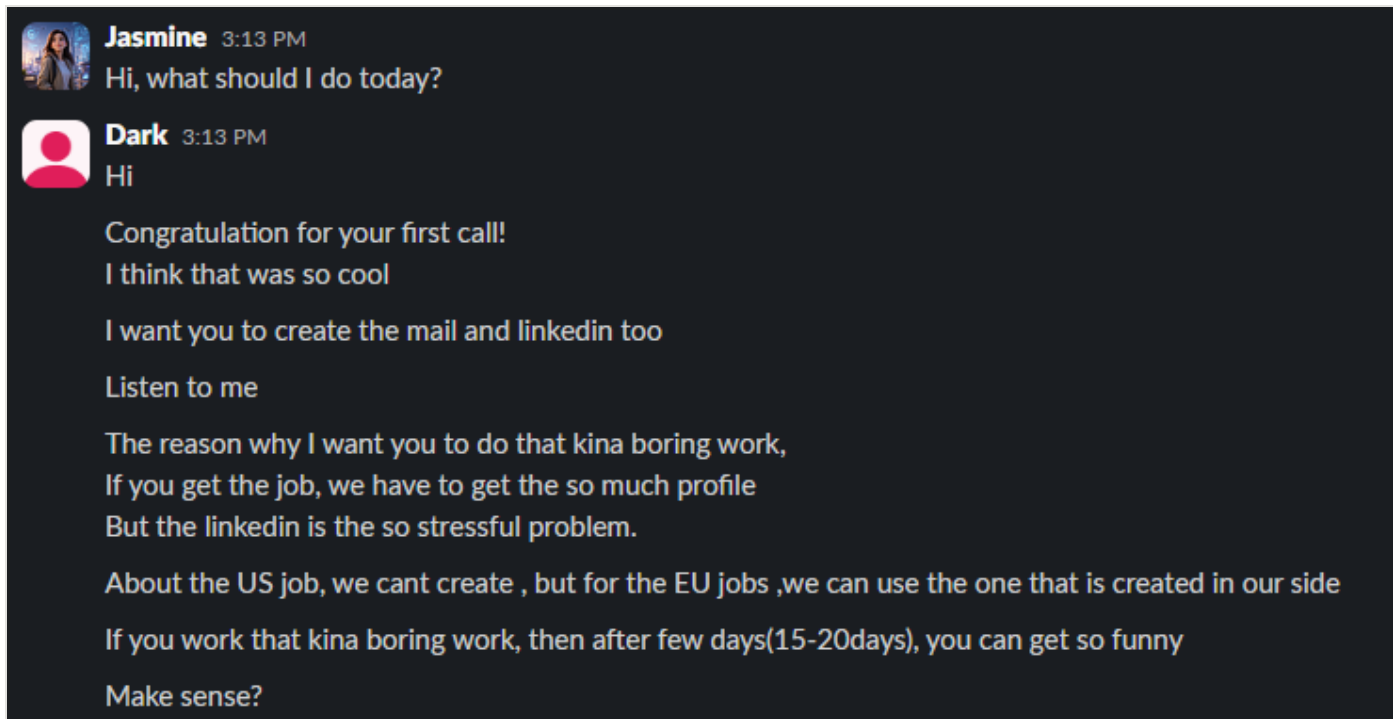


EXHIBIT 07 The first assignment

Profile Creation

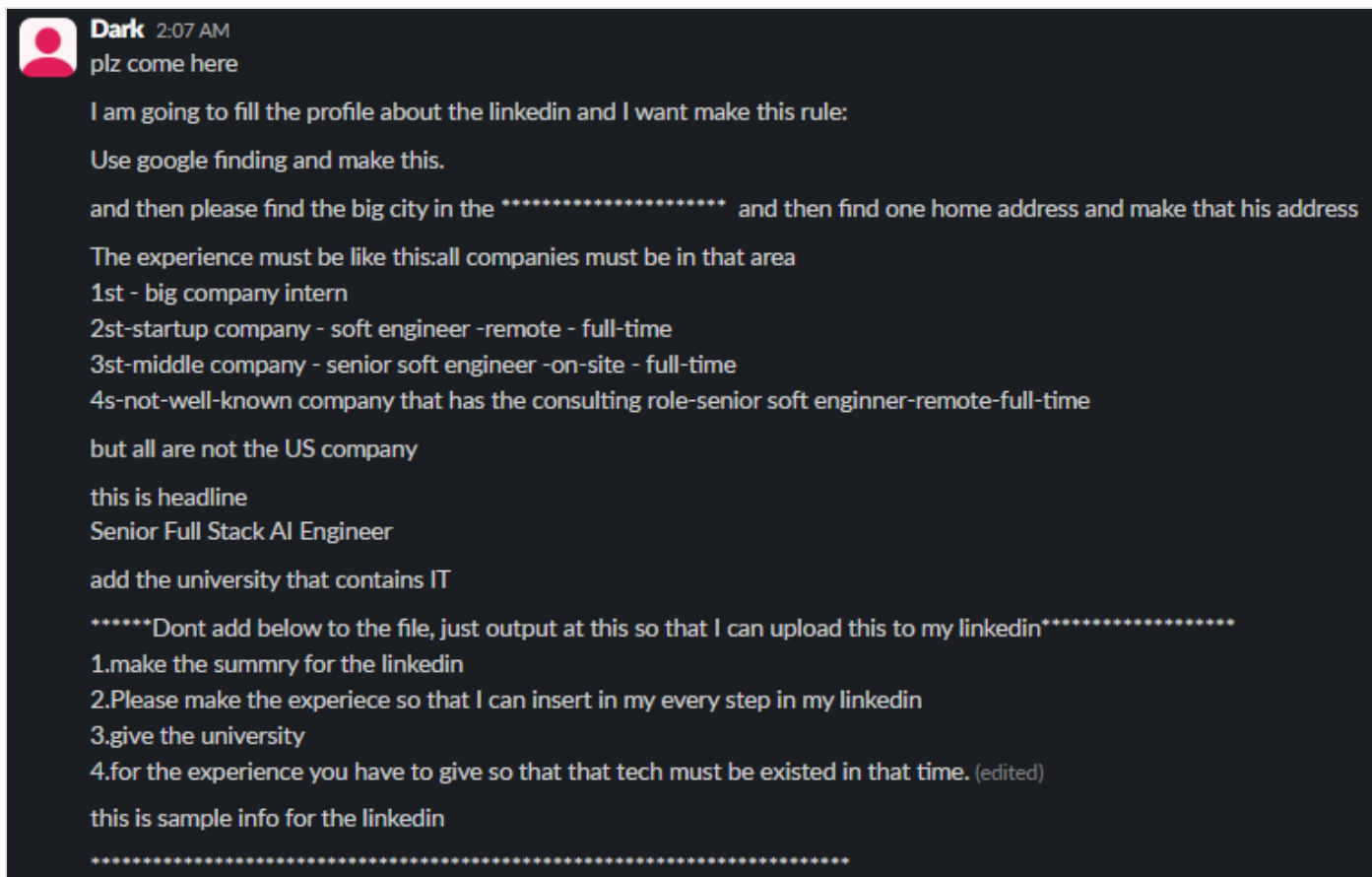


EXHIBIT 08 The profile rules

Dark's rules for profile creation are **written as a prompt for an AI tool**, of which turns up again later in this report:

- Pick a big city, find a real residential address there, and use it as the persona's address
- Build four roles, all in that metro area: intern at a big company; remote software engineer at a startup; on-site senior engineer at a mid-size company; remote senior consulting role at a lesser-known firm
- No U.S. companies
- Headline: "Senior Full Stack AI Engineer"
- Add a university with an IT program
- Make sure every technology listed existed at the time of the role

Each rule addresses a way in which the cell may have been caught before: the four-role ladder gives a plausible career arc, a single metro area to keep it consistent, a real residential address, and rule guards to prevent obvious mistakes. "No U.S. companies" is the rule that stands out the most — **it manufactures an employment history a North American employer may have trouble verifying domestically.**

Email Significance

A persona's primary email address is notably important as it's used for 2FA and acts as a recovery address for everything else hanging from it. These types of emails don't typically appear on job applications: **one email yields only one LinkedIn profile, and when that profile is banned the email burns with it.**

Jasmine ran **more than twenty Outlook registrations through a single Gmail before Microsoft began demanding a phone number.** According to `team4`, **SlyNumber** is used for purchasing and maintaining phone numbers.

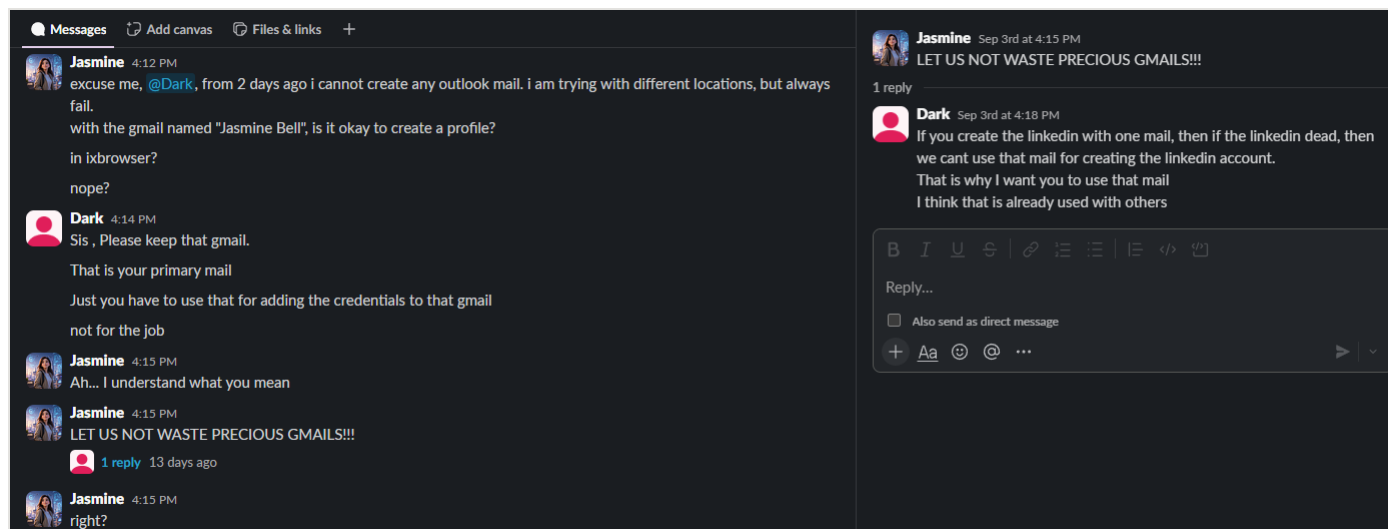


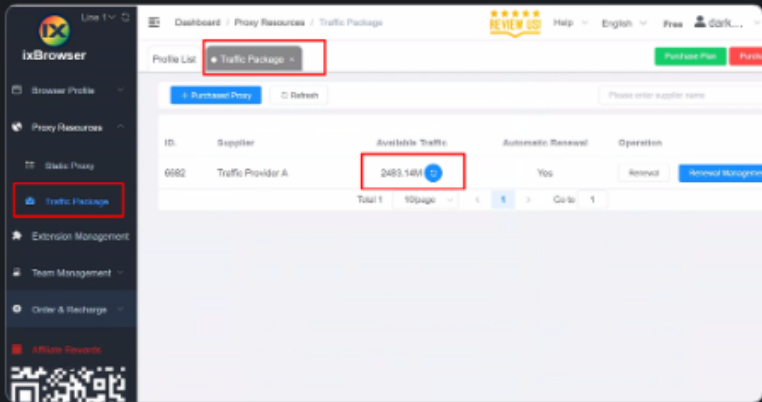
EXHIBIT 09 One email, one LinkedIn

Accounts live inside ixBrowser, which isolates each persona in its own browser profile behind its own metered proxy, so one platform ban does not spread. Dark's instruction was to check the traffic balance daily, since an empty package takes every profile with it — and in the same message he offers to top up the SMS-verification service against her email.

Payment for these services are primarily made using cryptocurrency, with **some operatives opting to use stolen credit card or banking information** — one set of card details posted in the workspace carried a Louisiana billing address.

Dark 2:05 AM
please check this every day

image.png



If the traffic package is used all, then you can lose all the accounts, so must check every day

then if possible, I will deposite the money top the SMS site with you gmail and then you can get the sms as you wish

at first, come here

I will let you know what you have to do

asap

EXHIBIT 10 Check it every day

Jasmine 12:52 PM
yeap

Dark 12:52 PM
how many linkedin do you create?

Jasmine 12:52 PM
6

my network connection state is not very good,

Dark 12:52 PM
check the traffic package for the ixbrowser

if you dont have any for that , you must deposite asap

Jasmine 12:53 PM
no, I still have 617.06M

is that enough storage? (edited)

Dark 12:54 PM
no, okay, I will deposite for now, if neccessary

EXHIBIT 11 Proxy traffic remaining

Jasmine 4:55 AM
hi

would you help me?

Dark 4:55 AM
what?

Jasmine 4:58 AM
i created over 20 outlook emails, and i used jb**** gmail for every security code. outlook says that i should try with this gmail next week, or shift the other email.

Dark 4:58 AM
so?

Jasmine 4:59 AM
may i lend an other gmail just for verification code reception? (edited)

Dark 4:59 AM
nope (edited)

Jasmine 5:00 AM
you mean "No way!"?

you mean just wait for next week?

or you mean no problem, go ahead?

excuse me, i didn't catch you, what do you mean? (edited)

Dark 5:01 AM
hey?

I am not your "hey"?

EXHIBIT 12 Refused a second address

These counts represent all the profiles and identities Jasmine produced in the first couple weeks:

WORKBOOK TAB	IDENTITIES STAGED	OUTLOOK ACCOUNTS	LINKEDIN PROFILES
Finland	642	5	3
Poland	103	13	11
Netherlands	100	10	0
UK	99	10	1
Australia	88	1	0
Estonia	83	14	0
US	61	2	0
Japan	50	2	0
Eight country tabs	1,226	57	15
US_REAL	3 real identities	—	—

DATE MODIFIED CLUSTERS ON 9.7 – SEPTEMBER 7, THE DAY HER FIRST BATCH OF PROFILES WAS REVIEWED AND FOUND DEAD.

Three patterns were observed throughout the spreadsheet:

- **Every birthday falls between 1995 and 1998**, putting each identity at 28 to 31 — inside the 28-to-35 band previously mentioned in their identity lifecycle documents.
- **Not a single identity in the workbook is male.** Across all eight country tabs, every row is a woman.
- **Japan adds a romanized pronunciation**, an Americanized surname (佐藤 結衣 becomes "Yui, Taylor"), and a "Feeling" column for the impression each should create: "Elegant, intelligent." "Professional, reliable." "Classic Japanese feeling."

The **US_REAL** page holds information on three real American women: date of birth, identification number, home address, phone numbers, personal email, employer, job title, bank name, account and routing numbers, and credit score. Two live in Florida, one of them in Jacksonville, whose first name is Jasmine and whose personal email contains "bell."

Jasmine submitted four finished LinkedIn profiles for review on September 7, and Dark came back to say every one of them had already been banned. He treated the loss as ordinary — the platforms take profiles down faster than the cell can build them, so the answer is simply to build more. **The cell has a name for working that way: "injogogi spirit."**

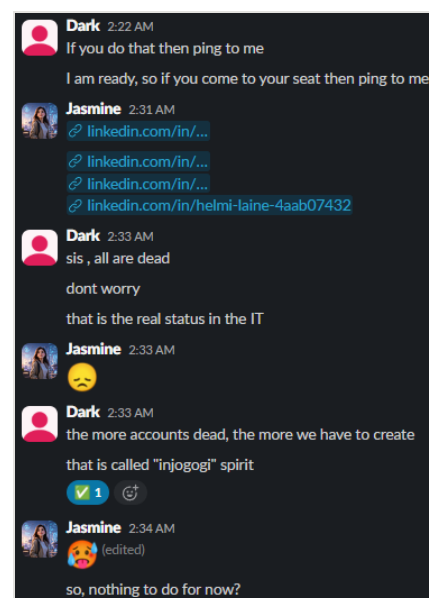


EXHIBIT 13 "Injogogi spirit"

Pipe Dream

In the same conversation, Jasmine asked how to get a "sil-In," which roughly translates to a real foreign facilitator. Dark's response suggest that Jasmine find a man she is interested in; start a conversation; "and then make [them] so crazy to you." In previous articles, "real guy" was used to describe willing American collaborators.

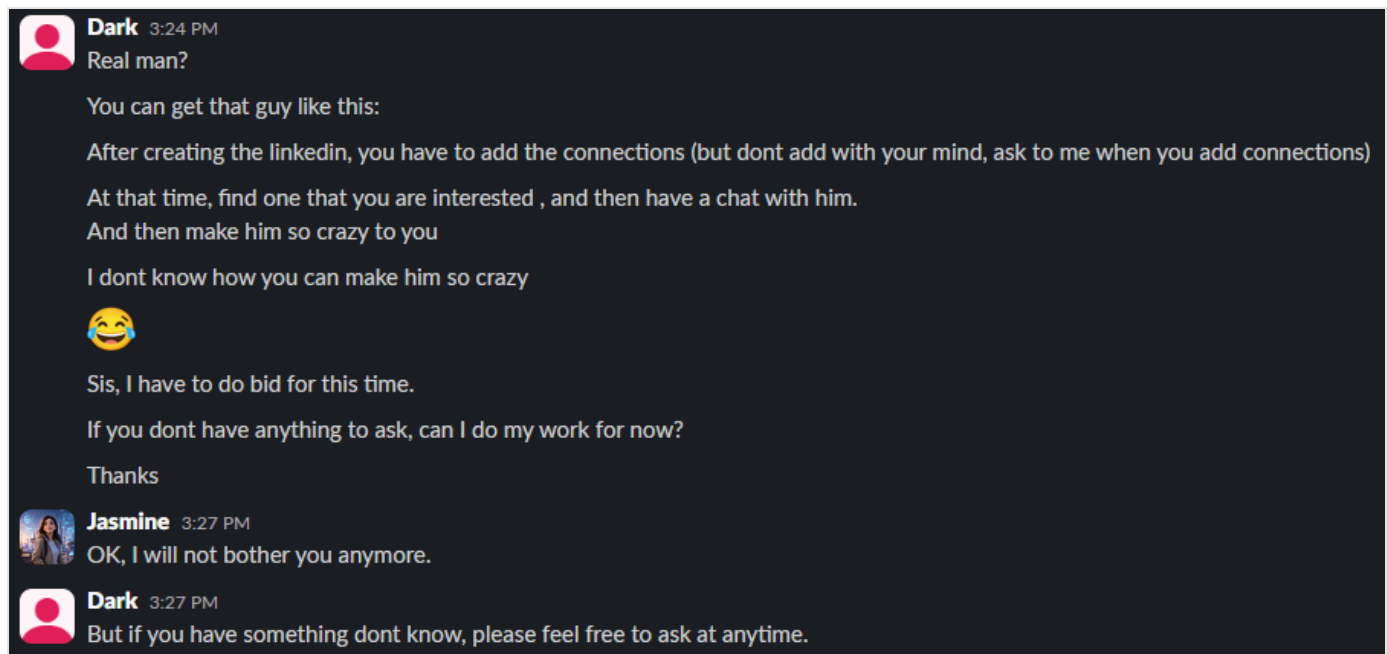


EXHIBIT 14 Recruiting a "real foreigner"

MageHire

MageHire (magehiregroup.slack.com) is the front-facing workspace, created in July 2022 with 190,583 messages and 6–10 monthly active users. It is **where the cell keeps its job profiles, its interview scheduling, and its placements**, and it is the only place the cell and its American facilitator interact with each other.

MageHire presents itself like any other conventional staffing firm: a team leader, senior and staff software engineers, and a CEO titled "**CEO-SALES-MARKETING.**"

MageHire's CEO is **Schmid Payen**, a U.S. citizen based in New York who runs MageHire and deals with its clients directly. His professional footprint spreads across dozens of sites, each carrying a different version of his experience and employment history depending on where you find it. He is also not the only Payen in the workspace: a second, Rodrigue — addressed in channel as @Rio — works beside him.

In July 2025, Payen became a father and shared his excitement with the operatives in the MageHire workspace. Additionally, he sent an audio message asking each of the operatives to request time off due to the occasion.

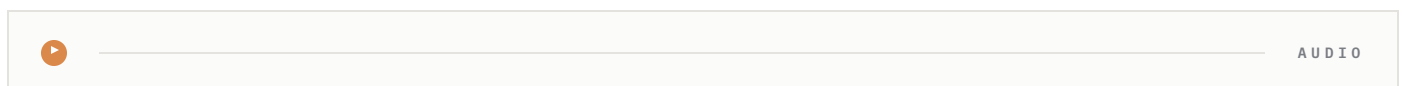


EXHIBIT 15 Payen's voice message — audio, available in the online edition

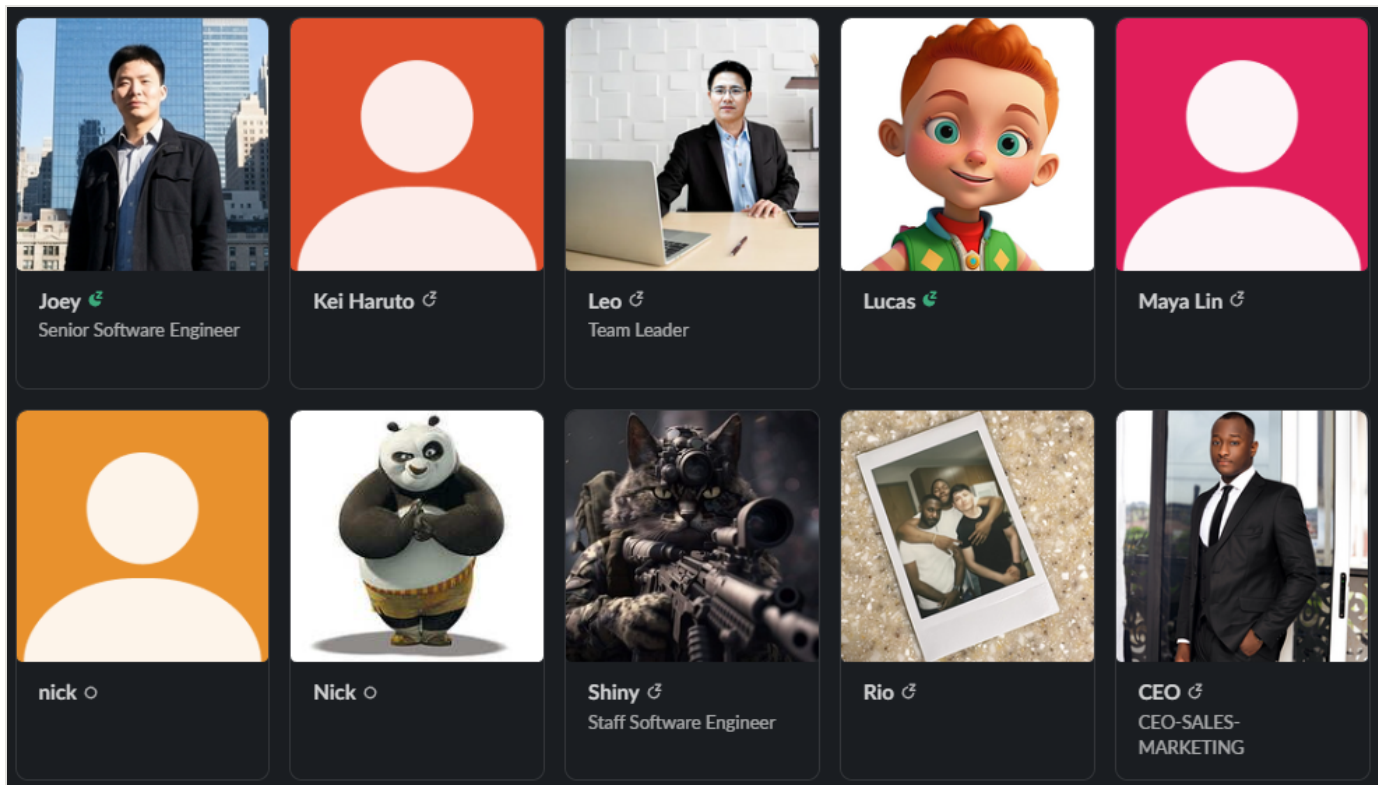


EXHIBIT 16 MageHire directory

MEDIA

This report contains 5 video clips and 1 audio recording that a PDF cannot play. The clips appear here as stills and the recording as a marker. Every one of them plays in full in the online edition of this report:

haydenmckenzie.com/research/dprk-it-worker-cell-part-one

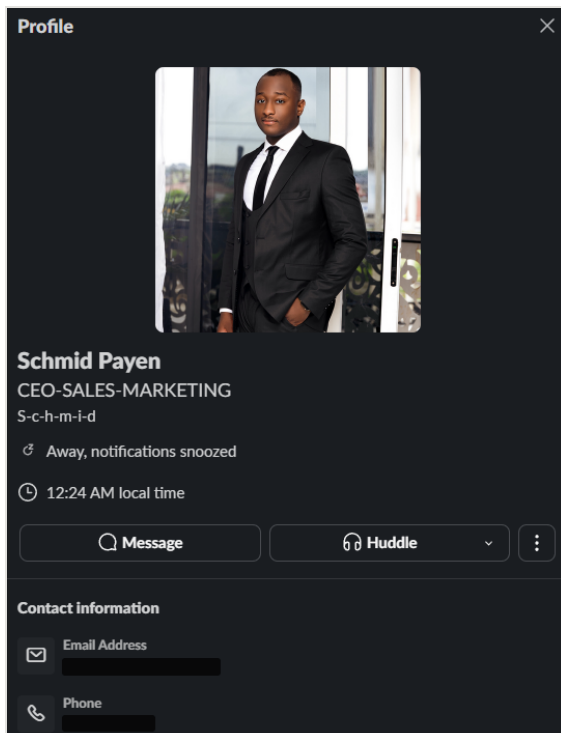


EXHIBIT 17 Payen's profile

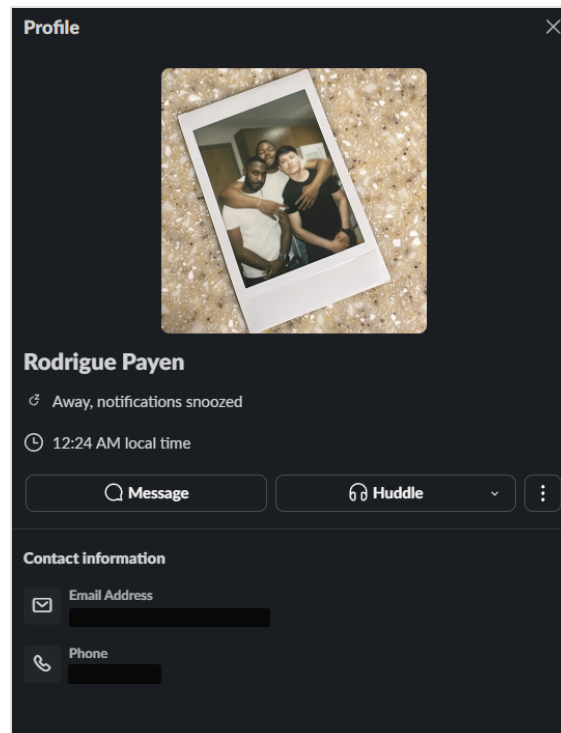


EXHIBIT 18 A second Payen

Operations

Each day opens with a check-in — **operatives post the client meetings they are carrying so the rest of the team knows what is covered, and the CEO plans around that list.** His complaint, made in channel, is that he cannot take on more clients unless those times reach him by 8 or 9 AM — he wants to cover client calls Monday to Friday and leave everything else, communications included, to the team. His team leader agrees and proposes a daily standup at 8:40.

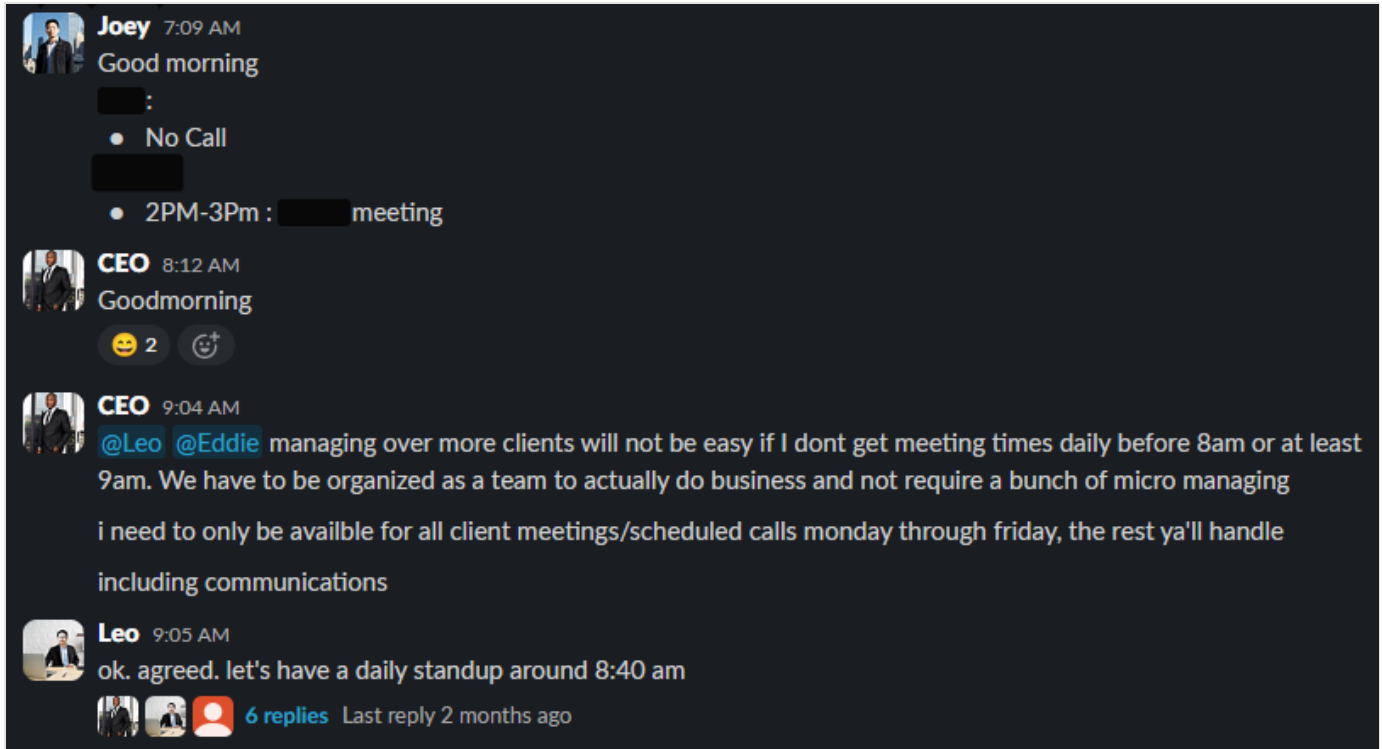


EXHIBIT 19 The morning check-in

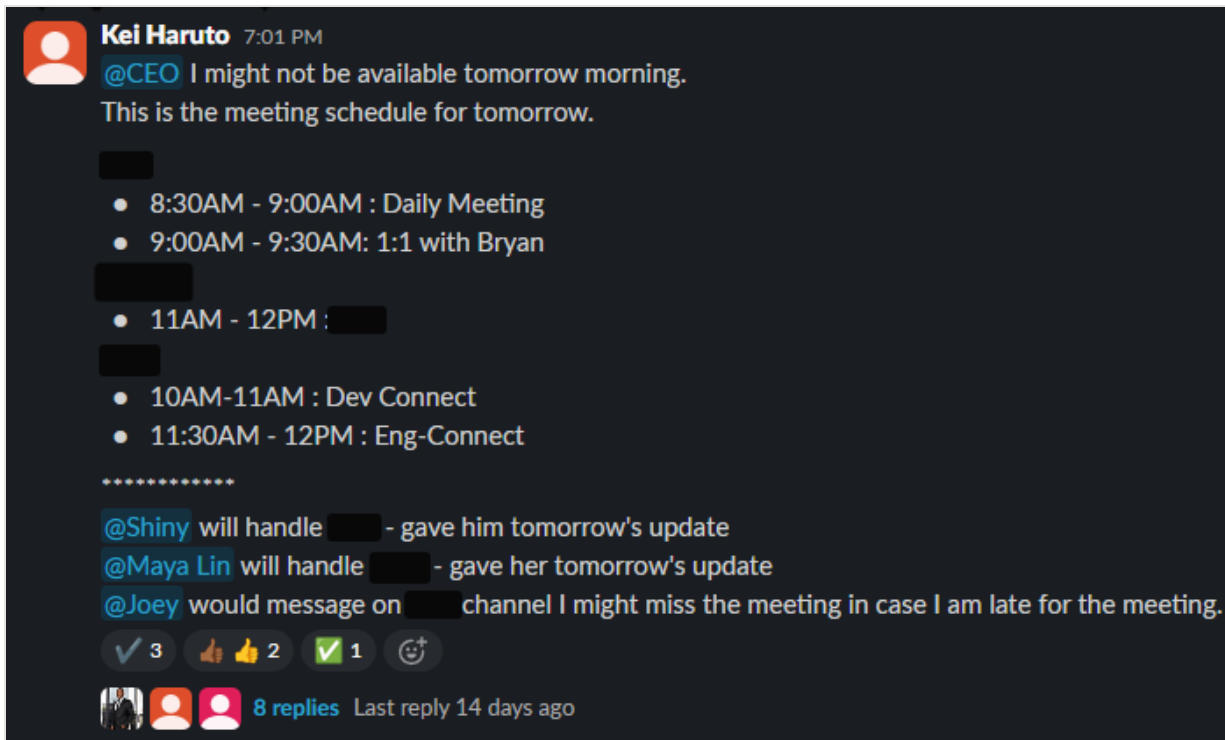


EXHIBIT 20 Handing off meetings

The check-ins also show how the cell covers for itself. **One operative posts a full next-day schedule across three clients, flags that he may be unavailable in the morning, and hands each meeting to a named colleague** — one of whom will "message on the xxx channel in case I am late for the meeting."

These schedules give a better sense of how much the operation is actually running. The client names that appear across the morning posts are separate engagements being run in parallel by a handful of operatives, with meetings passed between them when one is unavailable.

Tracking

The operatives **maintain monthly spreadsheets tracking per-client billing hours** — one developer's hours, by client:

MONTH	CLIENT A	CLIENT B	CLIENT C	CLIENT D	TOTAL
June 2026	5.5	4	0.5	—	10
July 2026	13	4	3	—	20
August 2026	11	38	4	3	56

Company A

At this company's request, their name has been withheld throughout the report and will appears as Company A. It is an identity and access management consultancy, selling Okta implementation, IAM health checks, managed services, access reviews, and Auth0/CIAM work to its own enterprise customers.

Two of the cell's operatives were involved directly with that work. Their client email addresses (joy.huang@, kei.haruto@) appear beside client staff on calendar invites. In the client's own Slack channel the team was told, "All of your job titles will be IAM Engineer," with seven steps for installing a matching email signature.

When the client migrated off Microsoft to Okta and Google, the operatives migrated with everyone else. The access problem created by that was easily solved: in the job channel, **the MageHire CEO posted one-time codes for each developer in turn** — "967506," then "sharing for joy first then you," then "766791" — because the second factor lands on his device.

The client also collected device attestations — this completed form uploaded to the MageHire workspace names the CEO, lists one MacBook Pro 16-inch, and is dated August 6, 2026.

Complete one attestation per company device you use. Submit at onboarding and re-confirm at least annually or whenever your device or its security settings change.

Personnel & Device Information

Full name	Schmid Payen
Role / title	Schmid Payen
Device make & model	MacBook Pro 16"
Operating system & version	macOS 26.5.2
Serial number / asset tag	YFCFM9WDFV
Date	8/6/2026

EXHIBIT 21 The device attestation

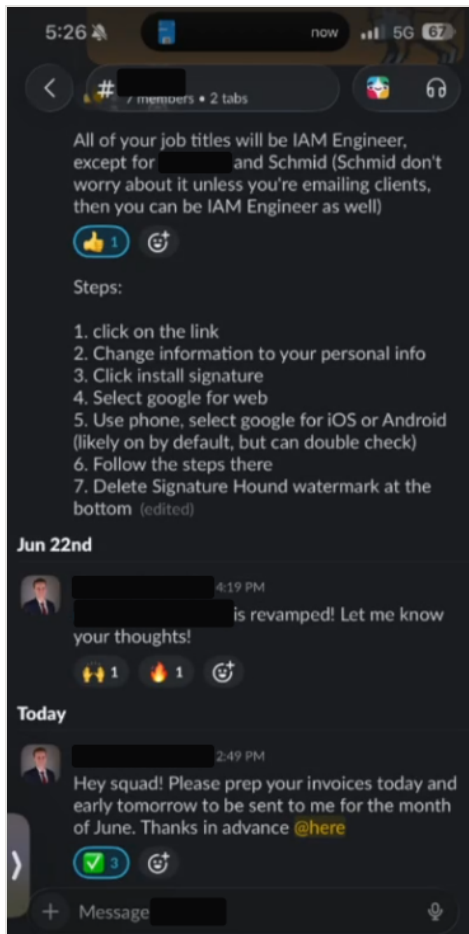


EXHIBIT 22 "IAM Engineer"

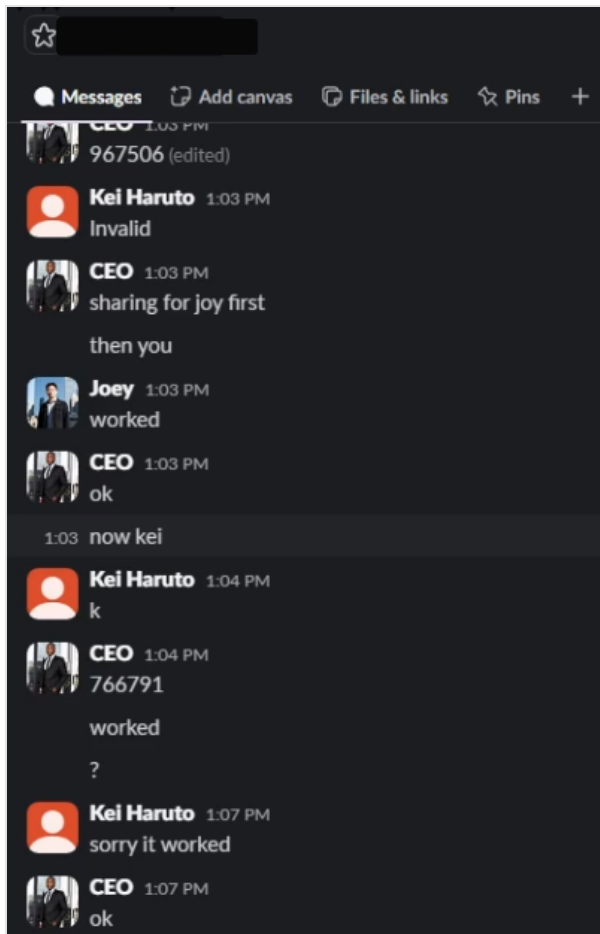


EXHIBIT 23 Passcodes by Slack

Remote access issues happened occasionally as derived from multiple discussions about accountability and consistency:

"anydesk is not working." — "Try it now." — "Internet wasn't working."

"Please check the pc again for me." — "Please." — "Try it now. The WiFi was turned off."

Initial Interview

Two of the cell's developers were already working for Company A when it came back to MageHire with another request: a **systems administrator for a two-month engagement at one of its own clients, covering Okta, patch management through NinjaOne, Azure, and VLAN configuration on Meraki equipment**. MageHire's CEO answered that he had **"strong coverage for this."** A screenshot of the requirements then landed in the cell's workspace, carrying a single instruction for Jasmine: "Please create new resume based on above requirement."

Additionally, on August 31 the client asked whether MageHire also had a Microsoft expert for a tenant-to-tenant migration. MageHire's CEO confirmed the incoming administrator had hands-on experience across Entra ID, Exchange Online, SharePoint and OneDrive, and domain cutovers. **Three days later, Jasmine forwarded her resume, tailored for both roles, to MP for review.**

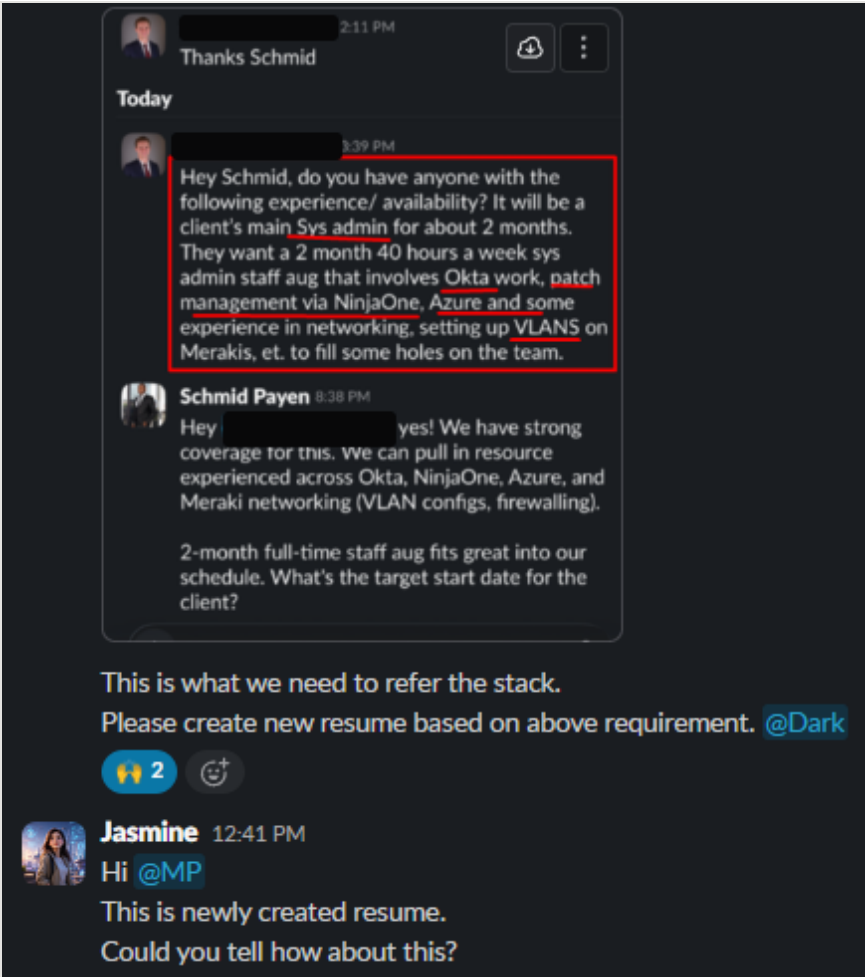


EXHIBIT 24 The requirements

Interview Preparation

The resume was produced in FlowCV on September 3. It follows Dark's six rules almost exactly with every entry mapping to either something the client asked for or to a rule from the profile guide in team4 .

REQUIREMENT OR RULE	RESUME ENTRY
Okta	Listed under Cloud & Identity
NinjaOne, patch management	Listed under Endpoint & Systems Management
Azure	Present in three of four roles
Meraki, VLANs	Cisco Meraki VLAN configuration, most recent role
Microsoft migration (asked August 31)	Microsoft 365, Entra ID
Rule: intern at a big company	IT Infrastructure Intern, NCS Group, 2018–2019
Rule: engineer at a startup	Software Engineer, PatSnap, 2019–2021
Rule: senior engineer, mid-size company	Senior Systems Engineer, ST Engineering, 2021–2024
Rule: senior consulting role, lesser-known firm	Senior Systems Engineer Consultant, Win-Pro Consultancy, 2024–2026

Rule: no U.S. companies, one metro

All four positions in Singapore

Rule: university with IT program

Bachelor of Computing, National University of Singapore

THE NAMED ORGANIZATIONS ARE NOT IMPLICATED. THE CLIENT WAS LATER UNABLE TO CONFIRM THE PERSONA HAD WORKED AT ANY OF THEM.

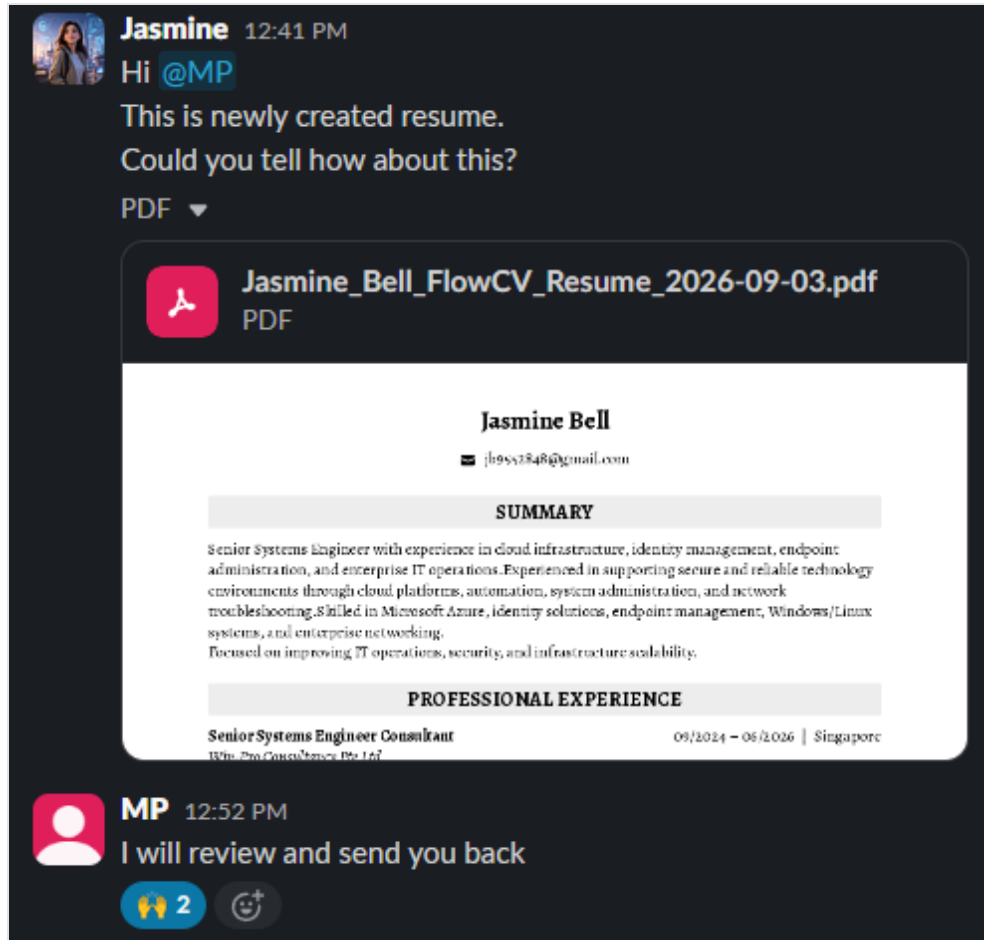


EXHIBIT 25 The resume, sent for review

AI Assistance

The resume was not the only thing written that morning. On September 3, a ChatGPT conversation was shared in team4 in which **the persona's entire life story was produced**. The prompt, in the first person, gives the tool one sentence of backstory — lived in Singapore, moved to Florida — and asks it to pick a famous university with a computer science program, invent a home address, and write a five-minute introduction for a call. It did all three: first a Florida version built around the University of Central Florida, then, on request, a Singapore version built around the National University of Singapore, complete with a "Bachelor of Computing" and timed talking points.

The NUS degree on the resume the client received, the Singapore-to-Florida narrative that explained an all-Singapore work history for a candidate supposedly living in Jacksonville, and the introduction she opened the interview with all trace to this chat. **The degree it suggested is what Company A later tried to verify and could not.**

Before the call, Jasmine rehearsed the generated introduction against **MockWise**, an AI interview platform that plays the interviewer and grades the answer. **Her preparation for a live client meeting was a biography invented by one AI tool and practised against another.**

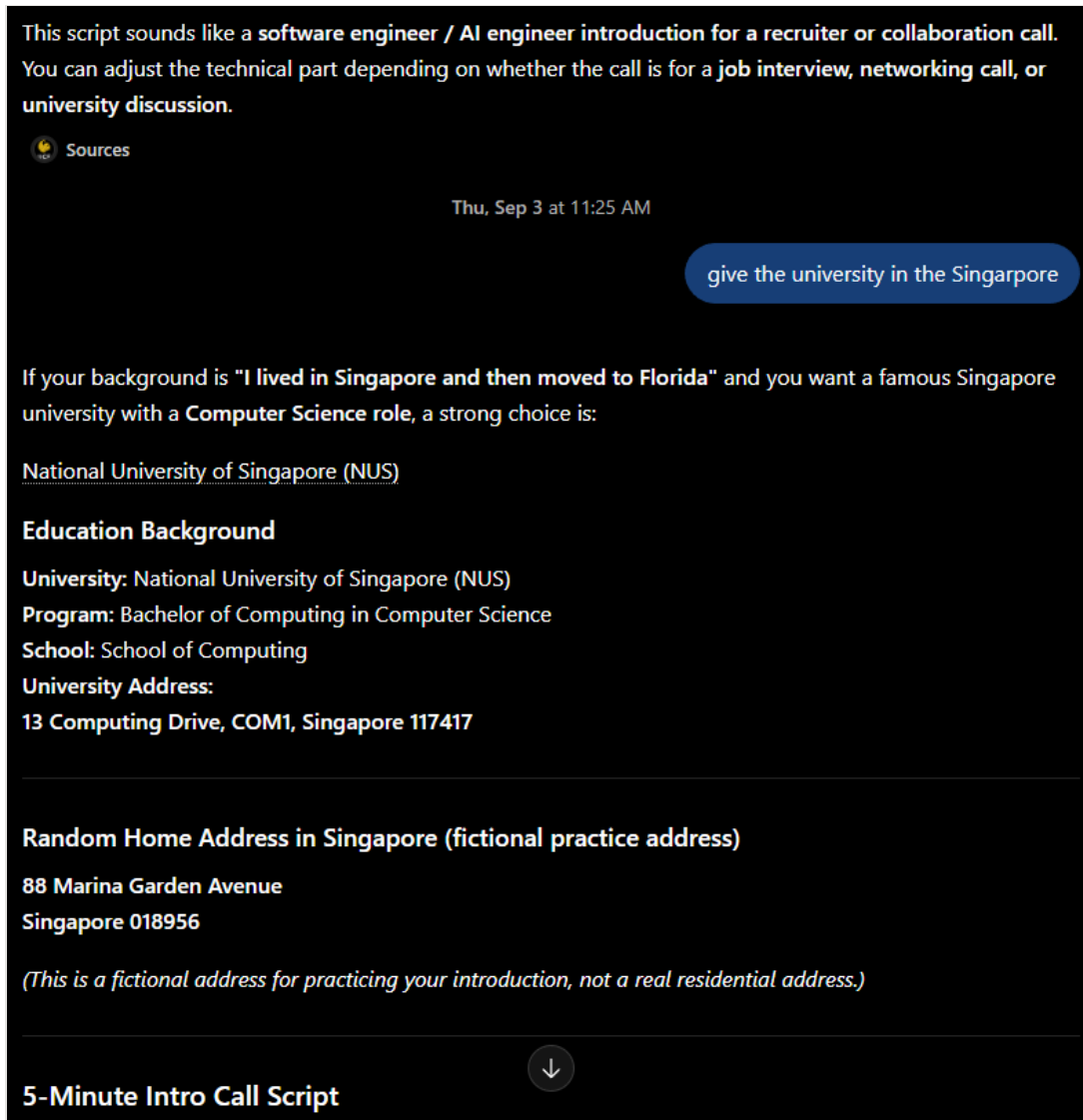


EXHIBIT 26 The ChatGPT script

Behind The Scenes

Magelire CEO told Jasmine to schedule the interview with "xxx the Company A CEO," suggesting noon or 1 PM, and made sure she wouldn't be alone: three members would be "behind the scenes to help and monitor call with you to make sure all goes well."

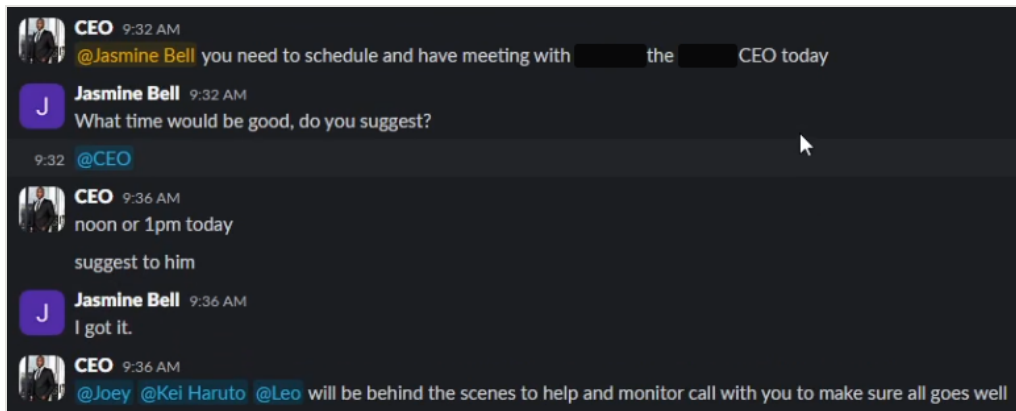


EXHIBIT 27 Behind the camera

With the interview set, the team checked Jasmine's equipment. MP asked Dark to test her video and report back whether the call would work; Jasmine confirmed her camera and audio had been checked and were fine.

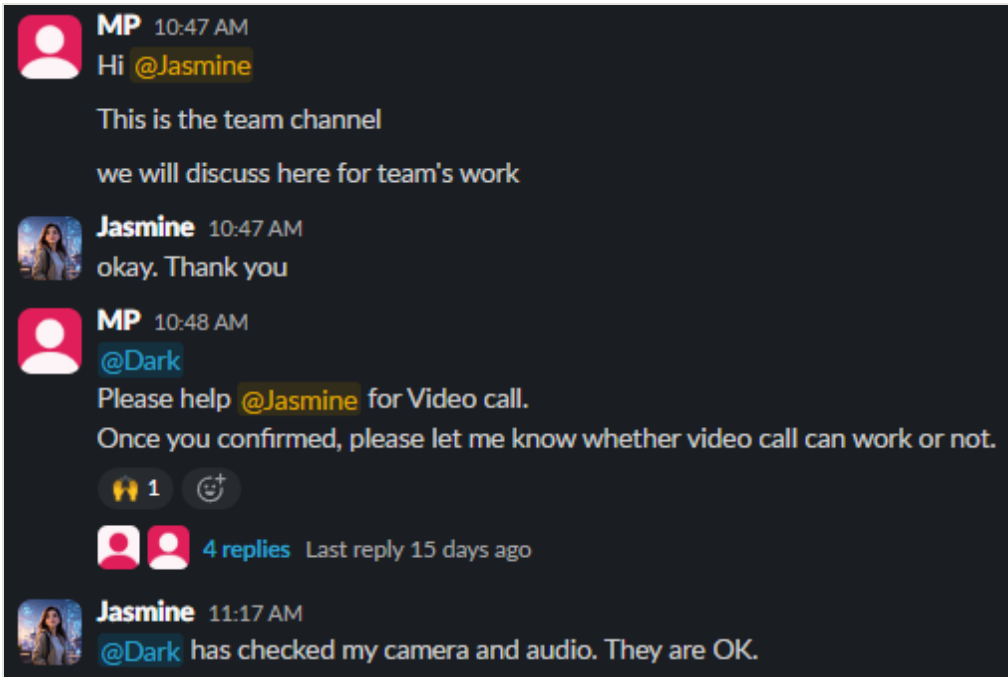


EXHIBIT 28 Testing the equipment

Rejection

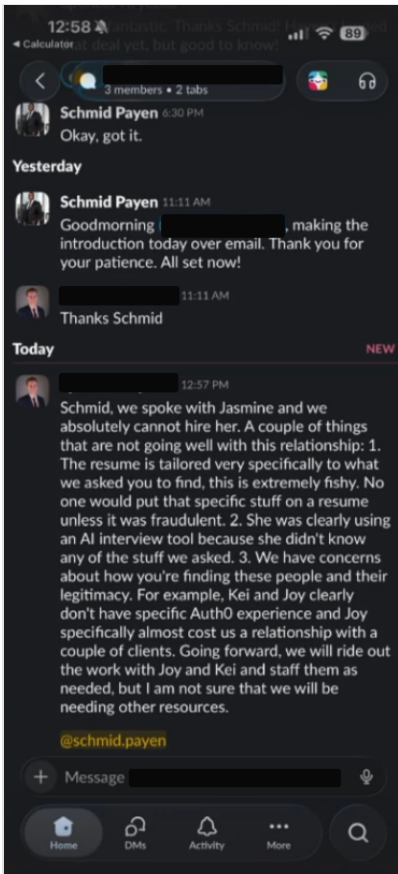


EXHIBIT 29 The rejection



EXHIBIT 30 Nothing verifiable

The client's answer to MageHire came the same day, and it was filled with complaints and concerns regarding Jasmine and MageHire. **The resume was so precisely fitted to the requirement that it read as fraudulent rather than qualified;** the candidate **could not answer questions about the things her resume claimed**, which the client attributed — correctly — to an AI interview tool; and the vendor's vetting was now in doubt, with the two developers already placed named explicitly, one of them for nearly costing the client a relationship previously.

Company A then went looking for proof she existed. Its representatives checked the employment history, the university degree, and the LinkedIn profile, **and came back with nothing on any of the three.**

Fallout

The rejection message didn't stop at Jasmine: it named both placed developers, questioned their Auth0 experience, and told the vendor the client wasn't sure it would need more resources.

Inside the cell, nobody disputed the Auth0 complaint. Pressed on a missed meeting, one of the two answered that it was "a bit hilarious that I have no auth0 experience," in the same channel where MageHire's CEO was being asked to account for the team's credentials.

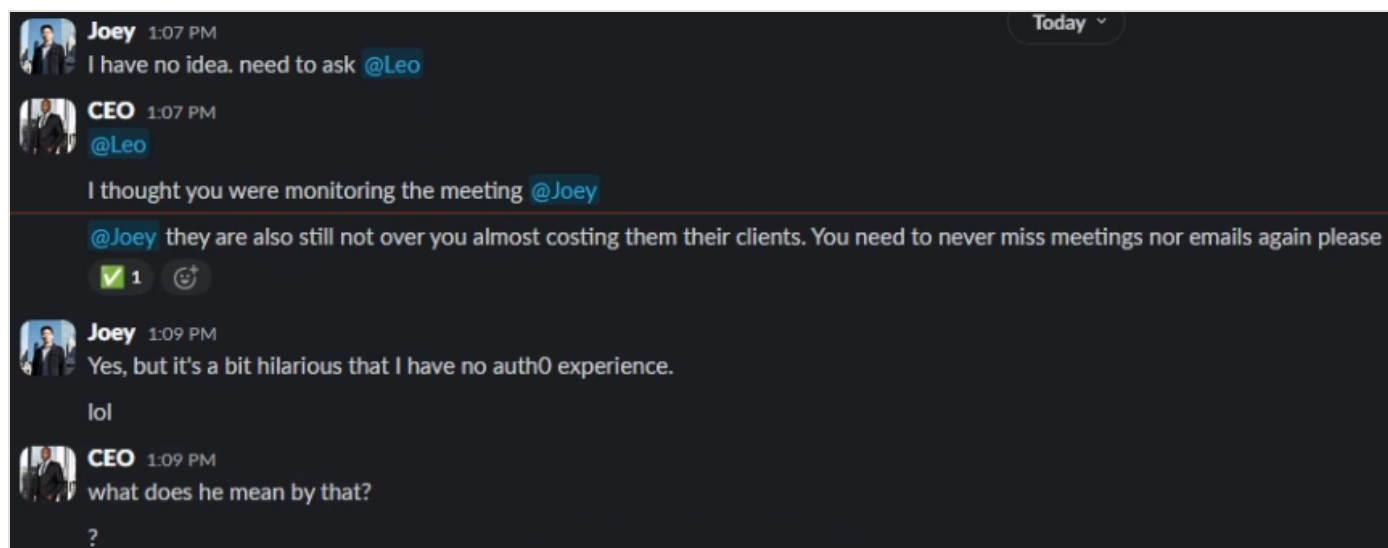


EXHIBIT 31 "No auth0 experience"

Damage Control

Within the hour, MageHire's CEO sent the client an explanation: **Jasmine was an off-boarded former contractor who had completed a project for MageHire in April, re-contacted on the strength of that prior work, who had assured him she had the Microsoft and SysAdmin background.** He took accountability for skipping a fresh background check, said she had been permanently dropped from the network, and promised that no future candidate would reach the client without a live, recorded technical evaluation conducted by him personally.

He also doubled down on the two developers already placed, telling the client **they were "100% confident" they could absorb the additional scope**, and offering the client a LinkedIn profile for one of them as evidence. In the cell's workspace an hour earlier, one of them had written: "this role requires much experience, I am not sure I can handle that 100%."

Rather than pulling the engagement, Company A **accepted the explanation**, put the Auth0 gap down to "a breakdown in communication between us," and moved on to scoping more work — on the condition that the two placed operatives take end-to-end ownership of it.



EXHIBIT 32 Payen's explanation



EXHIBIT 33 Scoping more work

Why the cell fought this hard for a relationship it had just heavily damaged is laid out within the workspace. Their engagement with Company A was continuing to expand, and both the operatives and MageHire's CEO acknowledged the opportunity for growth: "We have potential a lot of money we can eat with Company A for now and years to come let's not lose it."

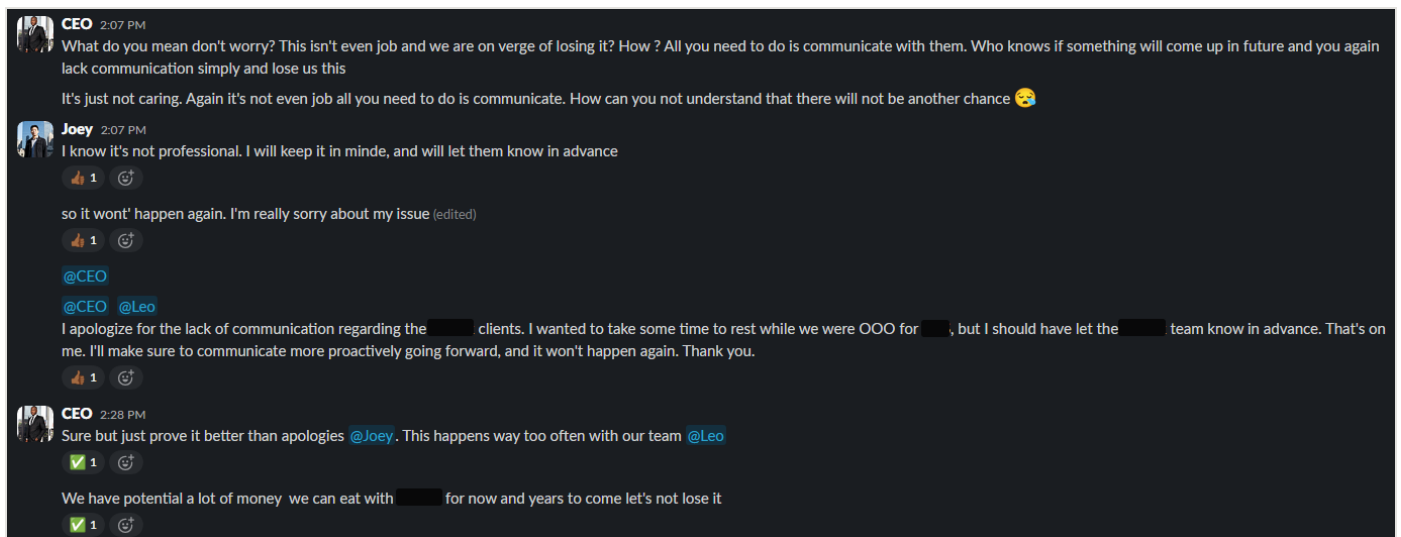


EXHIBIT 34 "Money we can eat"

Discussions in mphteam that occurred after the fallout show Jasmine taking blame and thanking her lead for a chance she recognized as unusual. MP declined the apology and **shared that they should have been more prepared**. It was Scarlet who checked on her — "are you okay?" — and whose consolation was that Jasmine was luckier than she had been: her own first interview with a real person had come only in August, after ten months in the cell.



EXHIBIT 35 Taking the blame

The team lead summed up the incident in a single line: "We always started without enough experience." Sending people into interviews before they are ready is not a mistake the cell made once — it is how the cell operates.

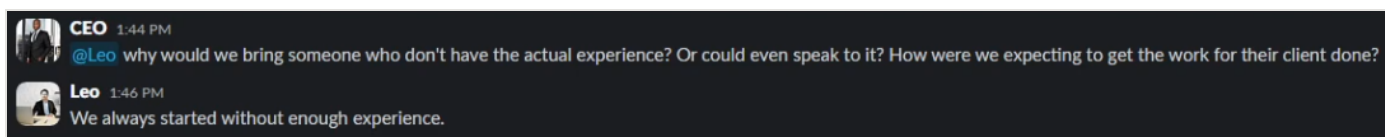


EXHIBIT 36 The business model

Exclusive Interview

Shortly after the fallout, I reached out to Jasmine as a fictitious company, offering an interview, and name-dropped individuals she'd been previously exposed to as a way to gain her trust — this method proved to be successful and shortly after, our interview was scheduled.

The questions I asked were **deliberately personal rather than technical** to see how Jasmine would respond to questions she likely hasn't practiced for. When reviewing chat logs prior to the interview, I observed Jasmine developing and sharing detailed background information for her alias — that of which was developed using ChatGPT the same morning.

After asking whether she'd be interested in pursuing a hybrid role as opposed to a virtual one, she **repeatedly mentioned her introverted-ness and expressed interest for remote roles exclusively**.



EXHIBIT 37 The scripted opening — video still



EXHIBIT 38 Remote only — video still

When asked about the hardest thing she's had to adapt to throughout her career, she **focused on her recent relocation from Singapore to Florida** while reemphasizing her struggle with changing environments, introverted-ness, and her desire for remote-only positions.

When asked what she does in her free time, she mentioned her interest in English novels citing *Twilight* and *Harry Potter* as good reads.

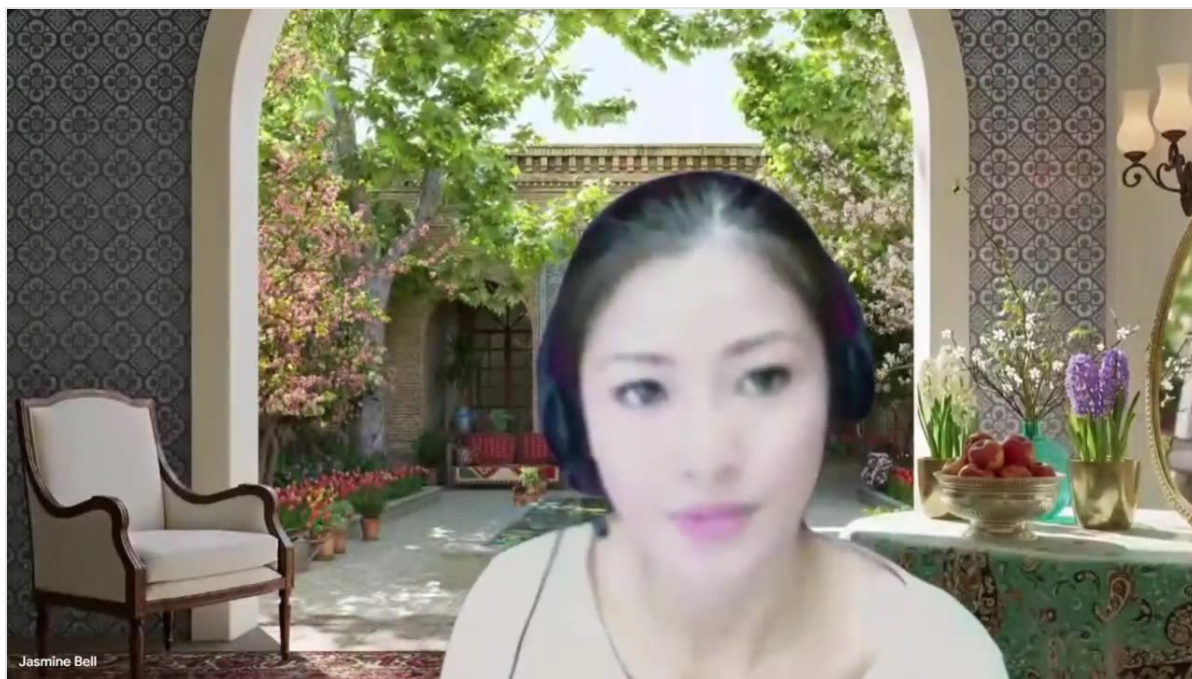


EXHIBIT 39 The same answer again — video still

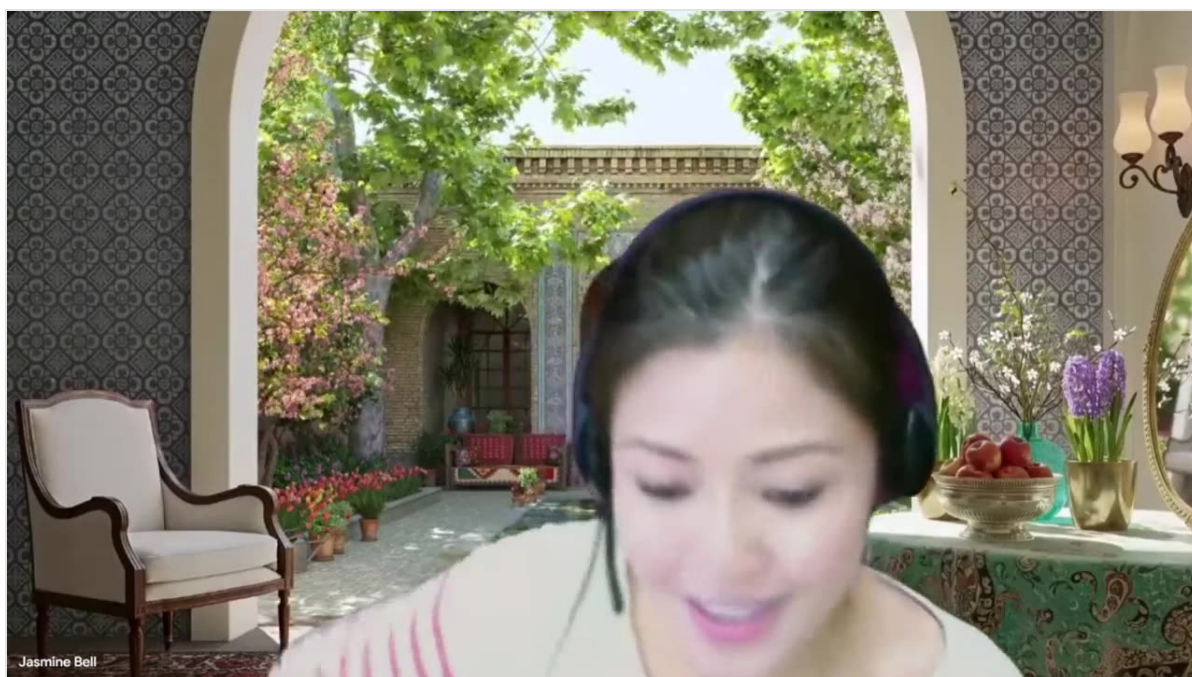


EXHIBIT 40 Books, not films — video still

Throughout a majority of the interview, **most of Jasmine's input came across as incoherent**. Answers rarely resolved into a point, she stumbled over her words on nearly every question, and the pauses between thoughts ran far longer than a conversation normally allows. At times, background noise carried through her microphone: the voices and movement observed were **consistent with other workers sharing the same room**.

Shortly after our interview, Dark posted "the call recording data" into `team4`: four recordings of me, running 5:00, 0:07, 5:00, and 0:56, with text panels beside the video consistent with **live transcription and note-taking**. When asked who she had been talking to, Jasmine told MP she had spoken to one man, whom she took to be the company's CEO.

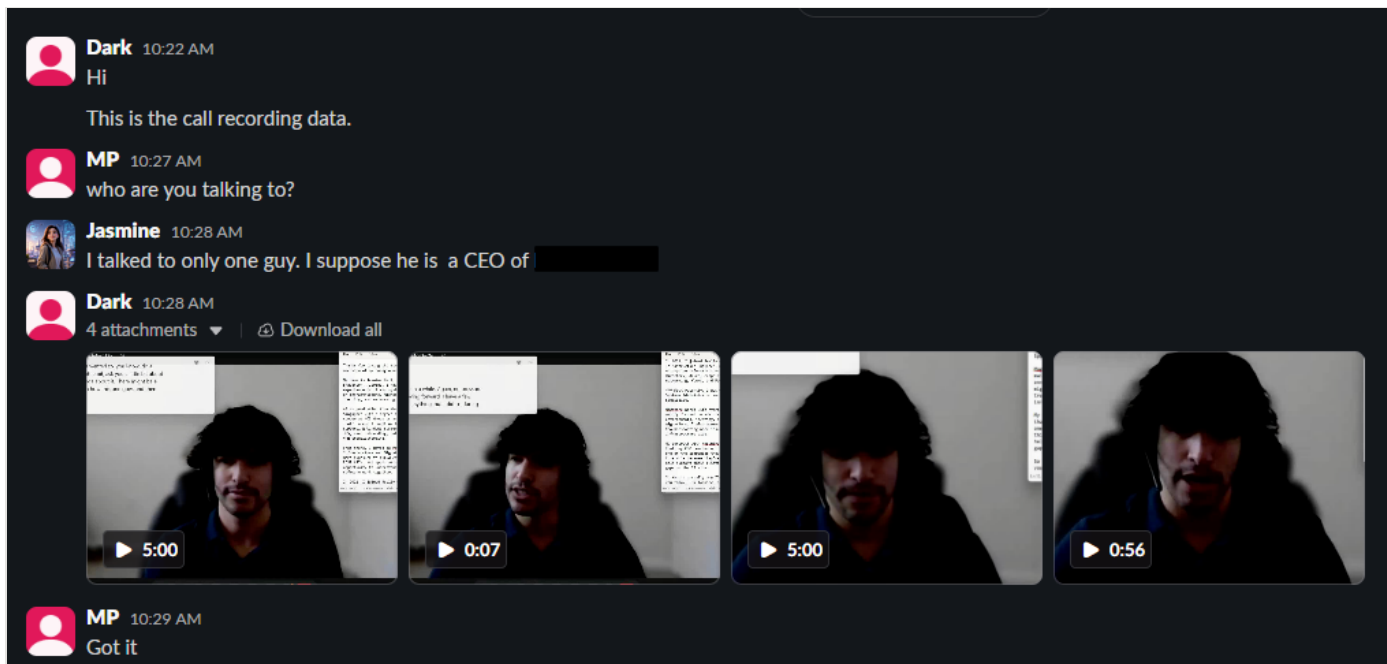


EXHIBIT 41 Recordings filed in team4

Her version of the recording gives unique insight into how their interviews are conducted: live transcripts sitting beside the video, a prepared notepad with the persona's background and work history, and assistance from fellow team members.

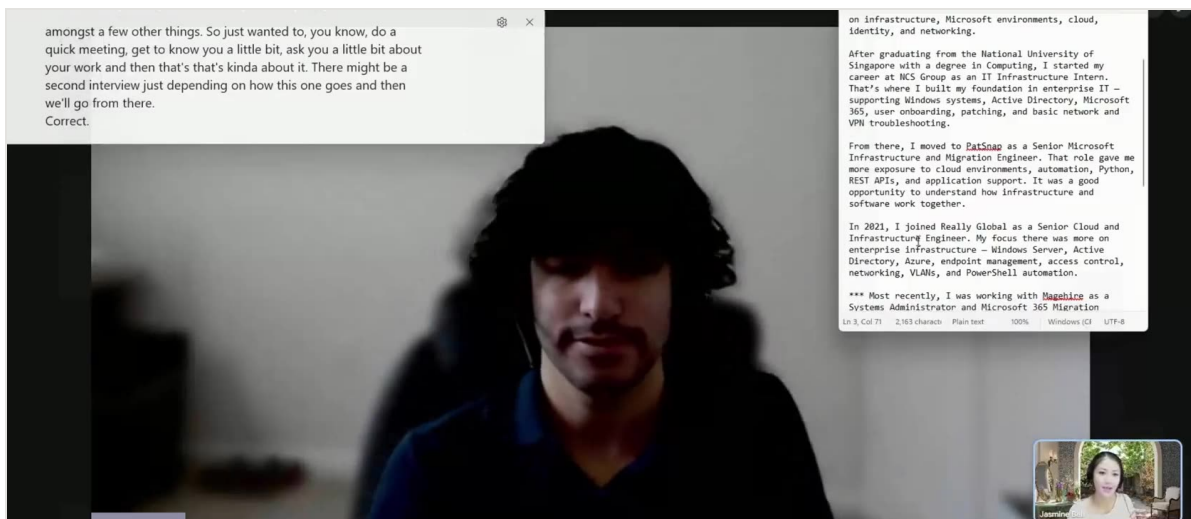


EXHIBIT 42 Her side of the call — video still

Conclusion

The most captivating find is that this cell utilizes multiple women for their operations. Female operatives rarely appear in reports on DPRK IT workers, and the material here uncovers a cell that isn't shy to utilize them: women are placed as callers, sent to interviews and client meetings on camera, and backed off-screen by the developers who do the technical work.

The three weeks followed a recruit's arrival are documented here in it's entirety. What Jasmine received is not just instruction, but tooling advice: profile rules written out as an AI prompt, an anti-detect browser with a proxy balance to

check daily, a VoIP service for verification codes, and a quota of mailboxes and LinkedIn profiles to produce in bulk. Within days of that first assignment her resume is generated in FlowCV against a live client requirement, her biography and a timed five-minute introduction are written in ChatGPT, that introduction is rehearsed against MockWise, and she is put on camera in front of a real client's CEO with three colleagues listening off-screen. **Scarlet waited ten months for a call like that. Jasmine waited three weeks.**

None of it would have reached a client without an American facilitator standing in front of it. MageHire is not an ordinary staffing firm — it is the cell's front. Its CEO holds the client relationships, signs the client's device attestation forms, and once the fraudulent candidate had been caught, wrote explanations that helped keep the account and scoped more work on top of it. I assess with **high confidence** that MageHire is an American front company operating on this cell's behalf, and that its CEO is a knowing facilitator rather than a deceived vendor.

Set against the locations, language, working patterns, and tradecraft recorded earlier in this report, I assess with **high confidence** that the cell is DPRK-affiliated, and that most of its members operate out of northeastern China.

Appendix A: Roles and Terms

The terms below are the cell's own, except where noted.

TERM	DEFINITION
Caller	Operative selected for spoken English who attends interviews and client meetings
Dev	Operative who performs the technical work
Team lead	Operative who runs a team, assigns work, and holds the relationship with the facilitator (MP in this report)
Trainer	Operative who onboards new members and runs the account and profile tooling (Dark in this report); my term, not theirs
Facilitator	The U.S. citizen who fronts the cell's placements and holds the client relationships (MageHire's CEO in this report)
Bid / bidding	Submitting job applications in volume, sometimes for another operative
Primary mail	The account holding a persona's credentials, kept out of job applications
"Injogogi spirit"	Internal motto for continuous account rebuilding
"Real man" / "real foreigner"	A genuine non-DPRK individual cultivated through LinkedIn

Appendix C: Indicator Register

Only tools and techniques named or directly evidenced in this report are listed. Every entry is a legitimate service or a commonplace practice; presence here means it was observed in use by this cell, not that the provider is implicated.

Tools & Services

INDICATOR	ROLE IN THE OPERATION
ixBrowser	Anti-detect browser. One isolated profile per persona, each behind its own metered proxy, so a platform ban does not spread
SlyNumber	VoIP numbers used to satisfy phone verification on persona mailboxes and profiles

FlowCV	Resume generation. The submitted resume was produced here on 3 September from the client's own requirement text
MockWise	AI interview platform used to rehearse the generated introduction before the live call
ChatGPT	Persona construction and interview scripting: employment history, university, home address, and a timed five-minute spoken introduction
AnyDesk	Remote access to the U.S.-hosted endpoint; failures are resolved by a person physically at the machine
Slack	Two free-plan workspaces: <code>mphteamworkspace.slack.com</code> (internal, DPRK-only) and <code>magehiregroup.slack.com</code> (front-facing, shared with the facilitator)

Previous Reporting

- Hayden McKenzie, *Inside a DPRK IT Worker Operation: How North Korea Outsources Job Fraud at Scale* (May 2026)
- Hayden McKenzie, *Inside a DPRK IT Worker Operation, Dissecting The Identity Lifecycle* (August 2026)
- Hayden McKenzie, *Inside a DPRK IT worker Operation, North Korea's Desperate Methods of Recruitment* (August 2026)

Hayden McKenzie · Independent Security Researcher
haydenmckenzie.com · intel@haydenmckenzie.com · Substack ↗ · LinkedIn ↗ · CV ↗