Davis Wright Tremaine LLP

Who's Behind the Computer Screen?
Strategies for Prevention and Detection of Remote Employee Fraud

July 2025

Davis Wright Tremaine LLP x STROZ FRIEDBERG

Today’s Speakers

Moderator

Michael Borgia

Partner

Davis Wright Tremaine LLP

Jeremy Merkelson

Partner

Davis Wright Tremaine LLP

Erik Mass

Associate

Davis Wright Tremaine LLP

Heidi Wachs

Managing Director

Stroz Friedberg

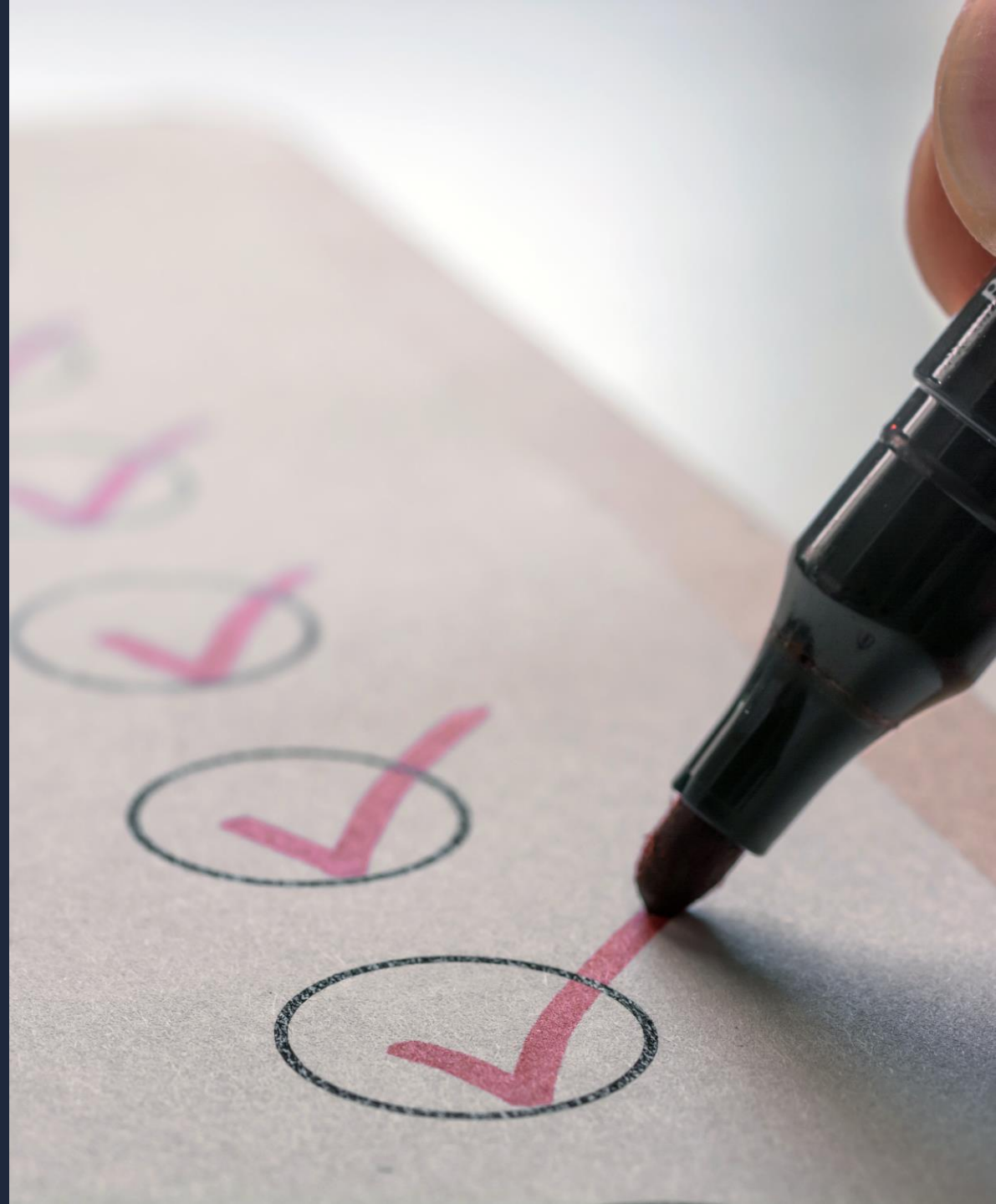
Mitchell Green

Director

Stroz Friedberg

Agenda

- Overview of Remote Worker Fraud – Threats and Risks
- A (Simulated) Case Study: Meet Omikron
  - Hiring and Onboarding
  - Identifying and Responding to Red Flags
  - Investigation
  - Mitigation and Termination
- Takeaways
- Q&A



Overview of Remote Worker Fraud

Many Types of Threats

- Remote Worker Fraud: Any type of fraud where an actor leverages remote working arrangements to fraudulently obtain or maintain employment.
- Actors may lie about their identity, skills, location, other jobs held, etc.
- Proliferation of GenAI increases risks.
  - Gartner: By 2028, 1 in 4 job candidates will be fake.

Many Types of Actors

- Motivations range from espionage to simply collecting a paycheck.
- Often involve foreign actors teaming with U.S.-based “facilitators” and operations.

Overview of Remote Worker Fraud - *Spotlight on North Korea*

- June 2025: DOJ announces nationwide action to combat DPRK-related remote IT worker threats. Actions in 16 states, searches of 29 “laptops farms” in the U.S., arrest of one U.S.-based facilitator. Another U.S.-based facilitator pled guilty. DOJ alleges hundreds of companies compromised.
- Prior indictments in January 2025, December 2024, August 2024, May 2024 and October 2023.
    - May 2024 indictment: Arizona woman ran major laptop farm to help DPRK workers earn more than $17.1 million, defrauded more than 300 companies.
    - July 2025 Sentencing: Arizona woman sentenced to more than 8 years in prison.
- Advisories and guidance issued by State, Treasury, FBI, ODNI and South Korea between May 2022 and January 2025.

Who Is Vulnerable?

Anyone with remote workers!

- Some actors are looking to acquire state secrets, IP, and other sensitive data, but many simply are trying to earn money.
- While DPRK has received most of the attention, actors need not be state sponsored. Many may work for criminal gangs, hacking groups, or even solo.
- Most actors are malicious, but not all are.

Consequences of Hiring Fraudulent Workers

- Unauthorized access to your network, potentially resulting in:
  - Compromise of sensitive personal data, personal data breaches.
  - Theft of intellectual property, confidential information.
  - Large-scale copying of code repositories.
  - Acquisition of material nonpublic information, potential securities laws violations.
  - Extortion demands.
- Payments to sanctioned individuals, violations of sanctions laws.
- Financial losses in salaries paid.
- Reputational damage.
- Regulatory investigations/possible penalties.
- Class action lawsuits/shareholder claims.
- Larger national security risks.

Meet Omikron.

- Omikron is a SaaS software provider preparing to launch a new product.
- The company needs to dramatically increase the capacity of its data center. It therefore engages a staffing firm to hire several contingent network and systems administrators.
- Omikron interviews various candidates via video call and hires several IT admins working remotely in the U.S., India and the Philippines.
- Each hire successfully completes a criminal background and credit check, which is standard for all Omikron hires.

Davis Wright Tremaine LLP

Some Hallmarks of Remote Worker Fraud

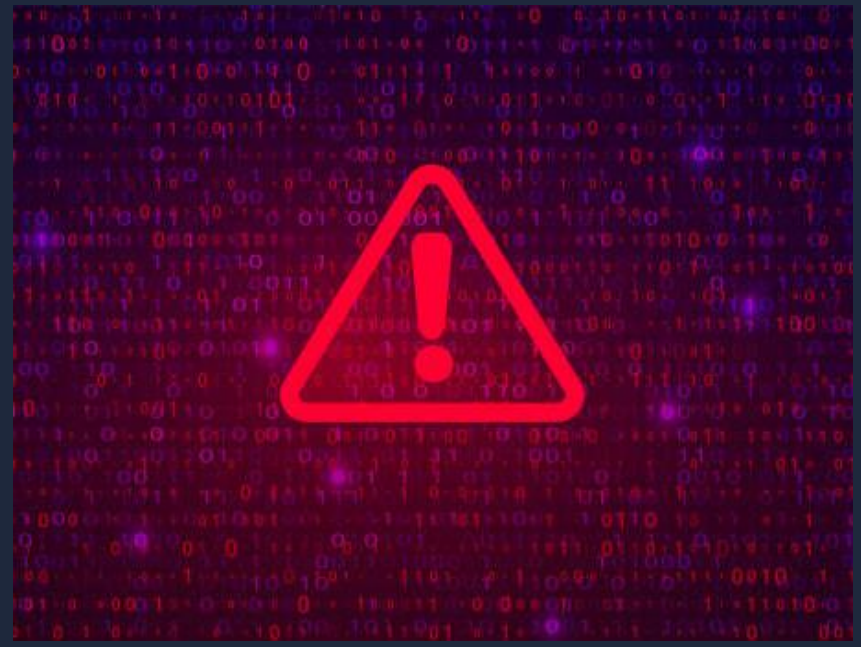
- Fake Backgrounds: resumes, certifications, work histories.
- Fake IDs: to help bypass verification.
- Deepfake images: altered images and manipulated video calls.
- Online presence: fake profiles and portfolios manipulated to give credibility.
- Proxies: third-party services, pseudo staffing agencies, remote interview proxies to misrepresent qualifications.
- Constantly evolving tactics.

Hiring and Onboarding

- What screening measures may be implemented during the application and interview process?
  - Are background and credit checks effective for foreign workers?
- What should companies do during onboarding to identify potentially fraudulent remote workers?
- What are the advantages of working through a staffing agency? Disadvantages?
  - What contractual provisions should you consider?

Red Flags Emerge…

- After several weeks of work, concerns are raised about one contingent systems admin who allegedly lives in Arizona.
- An engineering team lead raises concerns to HR about the admin's well-being.
  - She reports that the admin is never on camera during team calls, frequently saying that he does not feel well or that his children are home sick.
  - She also reports that he is frequently slow to respond during normal working hours, often stating that he has been busy even when he is between assignments. He often responds very late at night.
  - His work has been adequate, but the lead is concerned that he may not be handling the stress and workload of the project very well. She asks HR how to proceed.
- Payroll team reports that admin has changed direct deposit bank account on file twice since starting with the company.



Identifying and Responding to Red Flags

- Identifying potential remote worker fraud is cross-disciplinary. HR, business teams, information security, and other functions must coordinate to identify and report red flags.
- As part of security awareness training, provide guidance on identifying remote worker fraud and how to report it properly.
- Consider regular identity verification checks to ensure the hired employee is the same person actually doing “the work” contracted.
- Consider regular tracking of personnel access patterns, download activity, other security red flags.
- Incorporate processes to enrich and evaluate data points related to a candidate during the application and onboarding processes.
    - Look beyond typical HR criteria (e.g., resume, credentials). Is the candidate using a VoIP number to communicate? Does the email address look brand new (e.g., never appeared in a data breach)? Are they asking for payroll exceptions or making frequent changes to their payroll account details?

Investigation

- Based on the engineering lead's report, Omikron launches an investigation to assess whether the contingent admin might be a fraudulent employee.
  - The investigation identified:
    - The employee asked for their laptop to be shipped to New Jersey, despite claiming to live in Arizona.
    - The employee does not have a LinkedIn account, or any identifiable social media.
    - The employee's provided phone number is a Google Voice number.
    - The employee's provided email has a limited digital footprint and has not been seen in any data breaches.
    - The employee downloaded AnyDesk and Chrome Remote Desktop to their company issued laptop and regularly logged in from IP addresses associated with Astrill VPN.
    - A deeper investigation into the employee's identity revealed that the real individual by that identity no longer lived in Arizona and does not have a background in IT.

Investigation

- Omikron also decides to investigate potential harm arising from the contingent worker's weeks of access to company systems.
  - Should Omikron notify law enforcement? What should it consider?
  - Should employee be put on leave or suspension during investigation?
  - What investigation should Omikron conduct? What should it look for?
    - Access to sensitive information – unusual patterns? Unnecessary access or downloads?
    - Data exfiltration
    - Personnel interviews
    - Sanctions issues
    - Securities/public disclosures
- Such an investigation involves:
  - Reviewing activity on the employee's laptop, application and security logs and telemetry from Endpoint Detection and Response tools.
  - Deep dive investigation on the identity and addresses involved.

Mitigation and Termination

- What security measures can help companies mitigate harm if a fraudulent remote worker is hired?
  - Foster wider culture of awareness to identify and report remote worker fraud concerns. (TRAIN YOUR PEOPLE ABOUT THIS!)
  - Identify industry peers for trusted information sharing on patterns of behavior in this area.
  - Review government-issued guidance and incorporate into your practices.
  - Gut check any suspicious behaviors with your counsel/cyber advisors early and often.
- How can a company mitigate legal risks if a fraudulent remote worker is identified?
  - Employment risks.
  - Privacy and security risks.
  - Sanctions risks.

Additional Resources

Guidance of DPRK-related threats, motives, tactics, facilitators, and mitigations:

- Federal Bureau of Investigation (FBI): January 2025 and May 2024 PSAs.
- Office of Director of National Intelligence (ODNI): July 2023 Advisory
- U.S. and South Korea October 2023 Joint Guidance
- FBI, Dep't of State and Dep't of Treasury: May 2022 Advisory and Fact Sheet

Questions?

Thank You!

Michael Borgia

Partner

Davis Wright Tremaine LLP

E: michaelborgia@dwt.com

Jeremy Merkelson

Partner

Davis Wright Tremaine LLP

E: jeremymerkelson@dwt.com

Erik Mass

Associate

Davis Wright Tremaine LLP

E: erikmass@dwt.com

Heidi Wachs

Managing Director

Stroz Friedberg

Mitchell Green

Director

Stroz Friedberg